E-postalarda Adli Bilişim ve Karşı Adli Bilişim Teknikleri

R. MARAŞ, E. B. CEYHAN, Ş. SAĞIROĞLU

***Özet*—Gelişen teknoloji ile beraber iletişim araçlarının çeşitleri ve sayısı hızla artmaktadır. Günümüzde e-postalar en sık başvurulan iletişim araçlarından birisidir. Bununla birlikte e-postalar işlenen suçlarda araç olarak kullanılmaktadır. Bu nedenle e-postaların adli olarak incelenmesi ve e-postalara ilişkin her kaydın delil olabilecek şekilde elde edilmesi büyük önem arzetmektedir. İyi bir bilirkişi, analizci veya inceleyici personel e-postalardaki işleyişi iyi bilmelidir. Ayrıca suç işleyenlerin kendilerini gizleme ve delilleri saklama/yok etme yöntemlerine de hâkim olmalıdır.**

Bu çalışmada adli bilişim ve karşı adli bilişimin ne olduğu açıklandıktan sonra, e-postaların adli olarak incelenmesi ve karşı adli bilişim teknikleri açıklanmıştır. E-postaların araç olarak kullanıldığı suçlarda, suçluların muhtemel hareket tarzları ortaya konmuş ve adli bilişim uzmanının karşılaştığı olaylarda hangi hususlara dikkat edeceği açıklanmıştır.

***Anahtar Kelimeler*— Adli bilişim, e-posta, karşı adli bilişim, başlık bilgisi, anonim e-posta.**

Abstract—The number and means of communication are rapidly increasing with the deveoping technology. E-mail is one of the means of communication that is mostly used nowadays. However, e-mail is being used as a tool of committing crime. Thus, forensic examination of e mails and getting records of each e-mail to be used as an evidence assume great importance. A qualified expert, analyst or examiner must be aware of how the e-mail system works. Also, they must know the ways of spoliation of evidence that criminals use and their ways of hiding themselves.

ln this study, after computer forensics and antiforensics are described, forensic examination of e-mails and antiforensic techniques are clarified. ln addition, criminals' probable course of action in the crimes, in which e-mail is used as a way of, and the issues forensic experts should pay attention to in the events they come across are explained.

***Keywords*— Forensics, e-mail, antiforensics, headers, remailer.**

I. GİRİŞ

E-posta kelimesi, İngilizce'deki "electronic mail" ifadesinin Türkçe anlamı olan "elektronik posta" kelimelerinin kısaltmasıdır. E-posta hizmeti de, gerçek hayattaki posta Hizmeti model alınarak gerçekleştirilen hizmettir. Gerçek dünyada bir mektup yazılmasına müteakip, zarf içerisine konularak ve zarfın üzerine gönderici, alıcı isimleri ve adresleri gibi bilgiler yazılarak postaneye verilir. Postane görevlileri de zarf üzerindeki bilgilere (başlık bilgileri) bakarak mektubu ilgili adrese gönderirler. E-postalar da bu yapıya benzer şekilde çalışır. Gerçek hayattan farkı ise, aracı olarak insanlar değil bilişim sistemlerinin kullanılmasıdır [1].

İnternetin gelişmesiyle beraber, günümüz iletişim sistemlerinde telefonlardan sonra e-postaların kullanıldığı görülmektedir. Bunun en önemli sebepleri arasında, e-posta hizmetlerinin çoğunlukla ücretsiz ve kullanımının basit olması söylenebilir. GSM servis sağlayıcılarının internet kullanımını artırma yönündeki çalışmalarıyla birlikte e-postaların, kısa mesajın (SMS) yerini alacağı öngörülmektedir [2].

Bununla birlikte e-postalar yalnızca haberleşme için değil, çoğu zaman internet ortamında sanal kimlik olarak da kullanılmaktadır. Ticari internet sitelerinden hizmet almak maksadıyla üye olma ve sanal ödeme yapma gibi işlemler e-postalar kullanılarak yapılmaktadır. Bununla birlikte günümüzde e-posta hizmetini aktif olarak kullanan kişilerin hesap bilgileri, bilgisayar korsanları (hackerlar) ya da kötü niyetli kişilerce ele geçirildiğinde çok üzücü durumlarla karşılaşılmaktadır. Bu da e-postalarda güvenliğin ne kadar önemli olduğunu göstermektedir [2].

E-postaların işlenen suçlarda araç olarak kullanılması gerçeği de önemini artırmaktadır. Bu nedenle işlenen suçların aydınlatılmasında kullanılması ve dijital delil olarak kabul edilmesi göz önüne alındığında, e-postanın gönderilişinden alıcısına ulaşana kadarki yaşam döngüsünün çok iyi incelenmesi gerekmektedir.

Bu çalışmada, adli bilişim ve karşı adli bilişim konuları detaylıca açıklandıktan sonra e-postaların adli bilişim incelemelerindeki yeri ve bu incelemelerde dikkat edilmesi gereken konular tartışılmış ve adli incelemelere karşı koyma teknikleri ele alınmıştır.

II. ADLİ BİLİŞİM VE KARŞI ADLİ BİLİŞİM

A. Adli Bilişim

Adli Bilişim, işlenen bir suçun aydınlatılması ve suçluların tespiti için suç esnasında kullanılan bilişim nesnelerinden

Ş.S., Gazi Üniversitesi Mühendislik Fakültesi, Eti Mh. Yükseliş Sk. No: 5, Maltepe / Ankara. (e-posta: ss@gazi.edu.tr)
E.B.C., Gazi Üniversitesi Mühendislik Fakültesi, Eti Mh. Yükseliş Sk. No: 5, Maltepe / Ankara. (e-posta: eyupburak@gazi.edu.tr)
R.M., Gazi Üniversitesi Mühendislik Fakültesi, Eti Mh. Yükseliş Sk. No: 5, Maltepe / Ankara. (e-posta: rifatmaras@gazi.edu.tr)

ihtiyaç duyulan sayısal delillerin elde edilmesini sağlamaktadır [3].

Ayrıca adli bilişim; elektromanyetik ya da elektro optik ortamda saklanan veya bu ortamlarca iletilen; ses, görüntü, metin veya bunların birleşiminden oluşan her türlü bilişim nesnesinin, dijital delil niteliği taşıyacak şekilde elde edilmesi, muhafaza edilmesi, incelenmesi ve sonucun adli makamlara sunulması çalışmalarıdır [4].

B. *Karşı Adli Bilişim*

Dijital deliller üzerinde adli bilişim yöntemlerinin başarılı olamaması için geliştirilen yöntemlerdir. Purdue Üniversitesinden Dr. Marc Rogers'a göre karşı adli bilişim; "olay mahallinde bulunan delillerin varlığını, miktarını ve/veya kalitesini olumsuz yönde etkilemek, incelenmesini ve analizini zorlaştırmak hatta imkânsız hale getirmek için kullanılan her türlü yöntem/aksiyondur" [5].

Diğer bir deyişle karşı adli bilişim; adli delilin ortadan kaldırılması, silinmesi, karartılması ve anlamsızlaştırılması, delil ekleme, adli bilişim alanında personelin veya uygulamalarının etkisiz hale getirilmesi ve bütün bu faaliyetler neticesinde adli makamların etkilenmesinin sağlanmasıdır [3].

Bilişim dünyasındaki gelişmeler ile birlikte gelecekte, ülkelerarası savaşların ve terör olaylarının çoğunun sanal dünyada gerçekleşebileceği değerlendirilmektedir. Buna paralel olarak iletişim, ulaşım, enerji ve e-vatandaşlık gibi birçok hizmetin tamamen bilgisayara bağımlı olarak çalışacak olması nedeniyle, sanal ortamlarda güvenlik kavramının önemi artmıştır. Bununla birlikte adli bilişim alanında standartların henüz belirlenmemesi ve yapılan çalışmaların yeterli seviyeye ulaşmamış olması adli bilişimin akademik bir disiplin haline gelme ihtiyacını ortaya koymaktadır.

Adli bilişim inceleme teknikleri ve karşı teknikler, birbirinin çalışma mantığını anlama temeline dayanmaktadır. Karşı adli bilişim teknikleri; verilerin silinmesi, veri gizleme, karıştırma, yanlış yönlendirme, aldatma, engelleme ve şifreleme olarak sıralanabilir. Metasploit Antiforensics, Linux Kernel Module, ADMutate, Evidence Eliminator, SecureClean, Steganos, StealthDisk, Rootkit FU gibi araçlar, adli bilişim incelemelerini tamamen etkisiz hale getirebilmekte veya delil bulma sürecini oldukça uzatabilmektedir [6].

III. E-POSTALARIN YAPISI VE GÖNDERİM AŞAMALARI

Bu bölümde e-postaların yapısı, e-postayı meydana getiren bölümler, başlık bilgileri ve gönderim aşamaları incelenmiştir.

A. *E-postaların Yapısı*

E-postalar uygulama katmanında kime, konu ve mesaj alanı (body) bölümlerinden oluşur. Ayrıca hizmet alınan e-posta servis sağlayıcı tarafından opsiyonel olarak eklenen CC (Carbon Copy) ve BCC (Blind Carbon Copy) bölümleri de bulunabilir [7]. Genel olarak e-postalar şu bölümlerden oluşur;

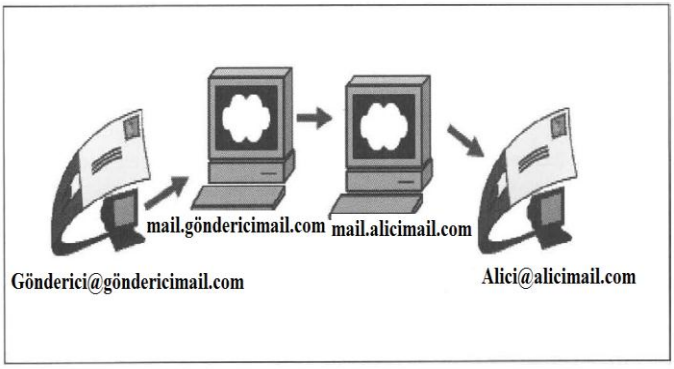
Kime: Mesajın gönderileceği e-posta adresinin yer aldığı bölümdür.
Konu: Mesajın konusu veya başlığının ifade edildiği bölümdür.
Mesaj alanı: Mesajın tam içeriğinin yer aldığı bölümdür.
CC: Mesajın gönderileceği bir başka e-posta adresinin yazılacağı bölümdür.
BCC: Mesajın bir kopyasının gönderileceği ancak diğer alıcılardan gizlenen e-posta adreslerinin yazıldığı bölümdür.

B. *E-posta Gönderim Aşamaları*

E-posta gönderme ve alma işlemi, posta alıcısı ve posta sunucusu olmak üzere iki türlü sistemden oluşmaktadır. E-posta başlık bilgilerini anlamak için öncelikle bir e-postanın A noktasından B noktasına doğrudan gitmeyeceği bilinmelidir. Her e-posta, yaşam döngüsü içerisinde en az dört bilgisayardan geçer. Şekil 1'de görüldüğü gibi e-posta transferinde alıcı ve gönderici arasında, göndericinin ve alıcının mail sunucuları olmak üzere en az iki bilgisayar daha vardır [1].

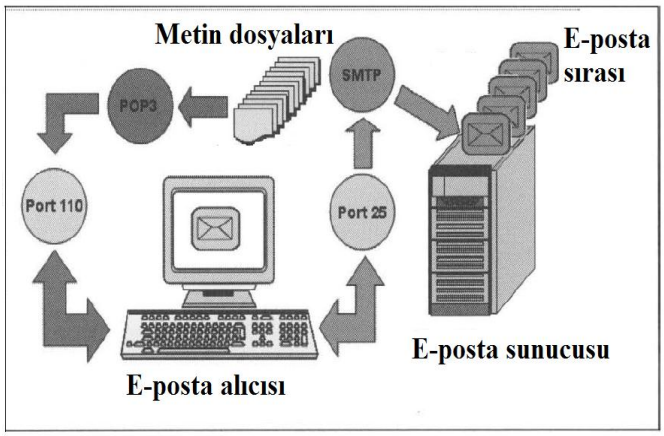
E-posta alışverişine bir örnek şu şekildedir:

Gönderici : gönderici@göndericimail.com
Alıcı : alıcı@alicimail.com
Mail sunucumuz : mail.göndericimail.com
Alıcı sunucusu : mail.alicimail.com



Şekil 1. Örnek e-posta alışverişi [1].

Şekil 2'de örnek bir e-posta alışverişi gösterilmektedir. Gönderici ve alıcı arasında e-posta gönderilmesinde kullanılan SMTP (Simple Mail Transfer Protocol) sunucusu ile e-posta alımında kullanılan POP3 (Post Office Protocol) sunucusu vardır. POP3, e-postanın posta sunucusundan alıcının bilgisayarına alınmasını sağlar. SMTP ise, e-postanın göndericinin bilgisayarından posta sunucusuna gönderilmesini sağlar [7]. Aşağıdaki şekilde standart bir e-posta altyapısı gösterilmiştir. E-postanın alım işlemi, POP3 ile 110 numaralı porttan, gönderim işlemi ise SMTP ile 25 numaralı porttan gerçekleşir. Kullanılan bu port numaraları değiştirilebilir.



Şekil 2. Standart bir e-posta altyapısı [1].

IV. E-POSTALARDA ADLİ BİLİŞİM

Genel olarak e-postaların adli olarak incelemesi şu konuları kapsamaktadır;

- E-posların başlık bilgilerinin incelenmesi,
- E-posta servis sunucularının incelenmesi,
- Bilgisayarda kurulu e-posta uygulamalarının (MS Outlook, Thunderbird, vb.) incelenmesi,
- Bilgisayarın bağlı olduğu ağların (network forensics) incelenmesi,
- İşletim sistemlerinde e-postalara yönelik tutulan kayıtların (registry) ile internet tarayıcıların (browser) incelenmesi,
- E-postalarda metin madenciliği [5, 8].

A. E-posta Başlık Bilgilerinin İncelenmesi

İletişimi gerçekleşen her e-posta, başlık bilgisine sahiptir ve bu başlık bilgilerinin incelenmesi adli ve idari soruşturmalarda büyük önem taşımaktadır. E-postalar tıpkı kargo şirketlerinin, kargonun taşınması ve takip bilgilerine benzer şekilde bir gönderim hikâyesini taşır. Bu hikâye başlık bilgilerinde barınır. Başlık bilgileri;

- Göndericinin e-posta adresi,
- Göndericinin IP (Internet Protocol) adresi,
- Göndericinin e-posta sunucusu,
- Alıcı veya alıcılara ait e-posta adresleri ile IP adresi,
- E-postanın gönderildiği tarih ve saat ile zaman dilimi,
- Gönderici ve alıcının hizmet aldığı e-posta servis sağlayıcının sunucularına ait bilgileri barındırır [2, 4].

E-postalara ait başlık bilgileri şu şekilde açıklanabilir [1,2,5,6,7,19];

From: E-postanın kimden geldiğini gösteren başlık alanıdır. İçeriği çok kolay değiştirilebileceği için en az güvenilir başlık alanıdır.

Reply to: E-postaya bir cevap yazılırsa, cevabın hangi adrese gönderileceğini bildirir.

Return-path: Reply-to başlığına benzemektedir. Eğer e-posta gönderiminde bir hata meydana gelirse, hata mesajının hangi adrese gideceğini belirtir.

Received: Bu alanda yer alan bilgi e-posta iletişimi ile ilgili verdiği detaylı ve gerçekçi bilgiden dolayı oldukça önemlidir. Postanın göndericiden alıcıya ulaşana kadarki tüm bilgisayar/sunuculara ait bilgileri barındırır. Received alanı da diğer başlık alanları gibi değiştirilebilir fakat son Received bilgisi mutlak surette gönderici sunucu tarafından ekleneceğinden gerçek bilgi verecektir.

Timestamp: E-postanın alıcıya ait e-posta sunucusuna ulaştığı zamandır. İlk ve son timestamp bilgilerine bakılarak e-posta sunucularının performanslarına dair bilgiler edinilebilir.

For recipient: Alıcı e-posta adresidir. E-postanın kime gönderildiği bilgisini verir.

Date: E-postanın ilk kaynakta oluşturulma zamanını gösterir.

User-agent: E-posta göndericisinin hangi yazılımı kullandığını gösterir.

X-Başlıkları: İstemci ve sunucu dışında özel e-posta yazılımların eklediği başlıklardır. Gerçek başlık değerleri ile karışmaması için X ile başlar. Örneğin bazı webmail uygulamaları gönderdikleri e-postalara X-Originating-IP:[1.2.3.4] şeklinde başlık alanı ekler ve bu başlık bilgisi istemcinin IP adresini gösterir.

E-posta başlık bilgileri çevrim içi (online) siteler ve özel olarak yazılmış bazı yazılım araçları ile de analiz edilebilmektedir. Bununla birlikte içeriğinde kişisel veya gizli olabilecek veriler olduğunda, e-postaları çevrim içi sitelerde analiz etmek uygun değildir. Adli veya idari soruşturmanın da gizliliğine halel getirebilecek işlemlerden kaçınılmalıdır. Google Apps-MessageHeader, MxToolBox, IptackerOnline ve Gaijin e-posta analiz sitelerine verilebilecek örneklerdendir [9-12].

Bu araçlardan en sık kullanılanlardan birisi Google firmasına ait olan Google Apps-MessageHeader'dır. Bu sayfada, bir e-postaya ait başlık bilgisinin analizi ve Gmail, Hotmail, Yahoo, AOL, Excite gibi e-posta servis sağlayıcılar ile Outlook, Mozilla, Apple Mail ve Opera gibi uygulamalardan e-posta başlık bilgilerinin nasıl elde edileceğine dair detaylı bilgiler verilmiştir [13].

Nirsoft firmasına ait IPNetInfo isimli yazılım da e-posta başlık bilgilerinin analizinde oldukça başarılıdır. Bu yazılımı, rekabet ettiği diğer yazılımlardan ayıran en belirgin özelliği ise, e-posta başlığında yer alan IP adresleri hakkında bilgi taraması yaparak, bu IP adreslerinin hangi kurum ya da kişiye ait olduğu, IP adresinin konumu, ait olduğu firma veya kişinin e-postası, telefon numarası, faks numarası ve adresi gibi çok önemli bilgileri toplaması ve sunmasıdır [14].

B. E-Posta Servis Sunucuları

İnternet dünyasında e-posta servis sağlayıcıları, sağladıkları hizmetleri ücretli veya ücretsiz olarak sunabilirler. Devlet kurumları ve özel şirketler genelde ücretsiz e-posta hizmeti sunmaktadırlar. Kurumlar ve özel şirketler, e-posta sunucularını doğrudan sahip oldukları sunuculardan veya Microsoft Outlook ve Exchange, IBM Lotus Notes, Novell GroupWise gibi e-posta sunucularından da bu hizmeti kiralamak suretiyle sağlayabilirler. Bu sunucular da düzenli

olarak yedekleme yaparlar. Bu sunucuların adli incelemesi yapılarak, sunucular üzerinden transfer edilen tüm e-posta trafikleri içerikleriyle beraber elde edilebilir [15, 16].

C. Bilgisayarda Kurulu E-posta Uygulamaları

Bilgisayarlarda e-postaların otomatik olarak takibinin yapılabildiği uygulamalar vardır. Bunların en sık kullanılanları MS Outlook, Mozilla Thunderbird ve Opera'dır. Bu uygulamalar da bir bilgisayarda yapılan e-posta haberleşmeleri hakkında bilgiler saklar ve e-postaların adli olarak incelenmesinde büyük önem taşırlar.

MS Outlook uygulamasının veri dosyaları olan OST (Offline Storage Table) ve PST (Personal Storage Table) uzantılı dosyalar, bilgisayarda kurulu MS Outlook uygulaması ile yapılan e-posta trafiğinin kaydedildiği dosyalardır. Benzer şekilde Outlook Express DBX, MBX ve IDX uzantılı dosyalarda, Grupwise uygulaması MLM ve DB uzantılı dosyalarda, Lotus NSF ve ID uzantılı dosyalarda, Apple Mac İşletim sistemi ve Thunderbird uygulaması MBOX uzantılı dosyalarda e-posta ile ilgili kayıtlar tutar [7, 15, 16].

MS Outlook Express uygulaması, kullanıcıların isim, telefon numarası, işyeri adı ve adresi gibi bilgilerin yazıldığı "vCards" oluşturmasını istemektedir. vCards incelenerek, e-posta kullanıcısı hakkında ekstra bilgilere de ulaşılabilmektedir [17].

E-postaların adli incelemesini yaparken, bilgisayarda tutulan bu dosyaları anlamlandırarak inceleme yapmaya imkân sunan bazı yazılımlar vardır. Bu yazılımlardan biri de Paraben E-mail Examiner'dir [16].

D. Bilgisayarın Bağlı Olduğu Ağdaki Kayıtlar

MS Exchange uygulamasının EDB (Exchange DataBase) uzantılı dosyası ve Lotus Notes uygulamasının ise NSF (NoteS File) uzantılı dosyası incelenerek e-posta trafiğine ulaşılır. Ayrıca bilgisayarın ağdaki canlı trafiği incelenerek e-posta servisine bağlanma zamanı, e-posta gönderim ve alım aktiviteleri gibi e-posta kayıtları incelenebilir [18].

Bu dosyalar genel adli bilişim yazılımları (X-Ways, Encase, FTK) ile incelenebileceği gibi sadece e-posta sunucuları ve ağdaki e-posta trafiğini incelemede kullanılan Paraben's Network E-mail Examiner yazılımı ile de incelenebilir [19].

E. Bilgisayarda Kurulu İnternet Tarayıcıları

Bilgisayarda kurulu internet tarayıcılar da e-postaların adli olarak incelenmesinde büyük önem taşırlar. Internet Explorer, Google Chrome ve Mozilla Firefox gibi internet tarayıcılarının internet geçmişi ile ilgili tuttuğu kayıt bilgileri, e-postaların gönderilip alındığı zamanlarda e-posta servis sağlayıcılara (Gmail, Outlook, Yahoo Mail, vb.) bir bağlantı kuruyorsa buradan da adli olayların aydınlatılmasında ipuçları elde edilebilir [16, 20].

Ayrıca işletim sistemlerinin tuttuğu kayıtlar (registry) içerisinde de e-postaların gönderim ve alım aşamalarına ait bilgiler bulunur. Örneğin Windows işletim sistemlerinde index.dat isimli dosya internet geçmişi ile ilgili bilgiler tutar. Linux işletim sistemlerinde ise mail isimli e-posta loglarının tutulduğu dosya bulunmaktadır. Bu dosyalar incelendiğinde suçla ilişkili e-postalara ait bilgiler elde edilebilir [17, 20].

F. E-postalarda Metin Madenciliği

E-postaların gönderici tespiti ile ilgili çalışmalar yapılırken, postanın içeriği de mutlaka incelenmelidir. Her e-posta göndericisi, göndericinin seçtiği kelimeler, kısa ya da uzun yazması, kelime sayısı, üslup, şive ve gramer hataları, e-posta metninin şekli, paragraf ve cümle yapısı, başlangıç ve bitişte yer alan ifadeler, kullanılan karakter ve işaretlerle iz bırakır. E-posta metinlerinde metin madenciliği yapılarak göndericiye dair işaretler bulunabilir. Yazarı bilinmeyen ve tahmin edilemeyen e-postaların içeriği ile bilinen kullanıcıların e-posta içerikleri metin madenciliği teknikleri ile kıyaslanarak e-posta yazarı (göndericisi) tespit edilebilir [21, 22].

V. E-POSTALARDA KARŞI ADLİ BİLİŞİM TEKNİKLERİ

E-postaların adli olarak incelenmesinde, incelemeyi sonuçsuz bırakmayı, uzatmayı ve delil olabilecek verileri değiştirerek bozulmasına neden olabilecek karşı adli bilişim teknikleri;

- E-posta başlık bilgilerinin silinmesi ve değiştirilmesi,
- Sahte e-posta gönderimi,
- Geçici e-posta hesabı ile gönderim,
- E-postalara ilişkin tutulan kayıtların silinmesi,
- Vekil sunucu (proxy) ya da VPN (sanal özel ağlar) kullanılarak e-posta gönderimi şeklinde olabilmektedir [5, 8].

A. E-posta Başlık Bilgilerinin Silinmesi veya Değiştirilmesi

E-postalarda başlık bilgilerinde son "Received" başlığı ile son IP adresi ve zaman damgalarını içeren e-posta sunucusu bilgileri değiştirilemez. Onların dışında olan konu, tarih, mesaj-ID, gönderici-alıcı (from, to, CC, BCC), mesaj içeriği, x-mailer, x-message info ve başlangıçtaki "received" başlıkları değiştirilebilir [1].

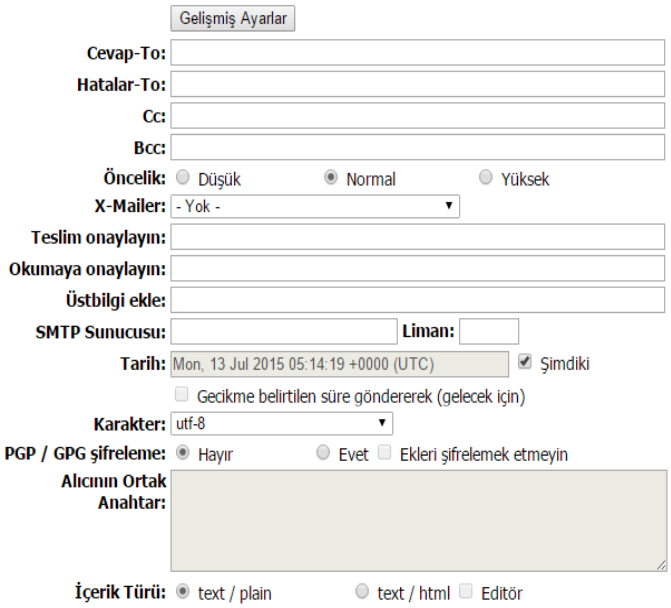
Günümüzde birçok e-posta servis sağlayıcı başlık bilgilerinden Göndericiye ait bilgileri silmektedir. Gmail, Outlook, Yandex gibi en çok kullanılan posta sağlayıcılarından gelen e-postaların başlık bilgilerinde göndericiden alıcıya kadar tüm başlık bilgileri yer almaz. Sadece bu servis sağlayıcılardan alıcıya ulaşana kadarki başlık bilgileri yer alır. Benzer şekilde Dark Mail olarak adlandırılan serviste de e-posta başlık bilgilerinde yer alan göndericiye ait ve diğer posta sunucularına ait bilgiler, başlık bilgilerinden çıkarılmaktadır [23].

E-posta adreslerinin başlık bilgileri bazı uygulamalar kullanılarak değiştirilebilmektedir. Bu değişiklikler de inceleme yapan kişiyi yanıltabilir. Buna örnek olabilecek çevrim içi araçlardan birisi "Emkei's Mailer" sitesidir [24]. Şekil 3'te ekran çıktısı görülen bu araç sayesinde; sahte isim ve sahte e-posta adresi ile posta gönderimi yapılmaktadır.

From satırına yazılan e-posta adresi hiç kullanılmayan adres olabileceği gibi var olan bir e-posta adresi de olabilir.

Şekil 3. E-posta başlık bilgilerinin manipüle edilmesinde kullanılan bir araç [24].

Bu aracın gelişmiş seçenekler bölümünde, mesaja cevap yazılırsa ya da hata mesajı alınırsa hangi adrese gönderileceği, birden fazla kişiye gönderimde kullanılan CC ve BCC alanları, e-postanın öncelik durumu, e-posta gönderiminden sonra ulaşma bilgisi, okundu ise okunma bilgisi, e-posta başlığına herhangi bir ekleme yapılacaksa bu eklemenin girileceği alan, sunucu ismi, tarih değişikliği yapılabilecek alanlar gibi e-postanın başlık bilgilerinin değiştirilmesinde kullanılabilecek birçok alan mevcuttur.



Şekil 4. Gelişmiş seçenekler [24].

Geçmiş dönemde e-posta başlık bilgilerinde sık kullanılan yöntemlerinden biri de tarih ve saat gibi zaman damgalarının değiştirilmesi üzerine olmuştur. 2009 yılının sonuna kadar bu konuda Yahoo Mail, Gmail ve Hotmail gibi servis sağlayıcılar da önlem alamamış ve kişiler ile kurumlar üzerinde birçok mağduriyetler yaşanmıştır [25].

Başlık bilgilerinin değiştirildiği bilgisini tespit işleminde göndericinin e-posta sunucusuna bakılarak uyumlu olup olmadığı incelenmelidir. Örneğin abc@gmail.com e-posta adresinden posta geldiğini varsayalım. Bu e-posta adresinin sunucusu GMail'dir. Gelen mesajın başlık bilgisi de GMail posta sunucusuna uygun olmalıdır. "X-originating IP", "X-originating E-mail" gibi başlık bilgilerinin bölümleri Gmail'in posta formatına uygun olmalıdır. Uygun değilse sahte bir e-posta olduğu çıkarımına varılabilir [2].

E-posta sunucusunun DNS ismi ve makine ismi farklı olması durumunda da başlık bilgilerinin değiştirilmiş olabileceğinden şüphelenilmelidir. From satırında e-postayı gönderen sunucunun smtp2.abc.com.tr olduğu görülür ve aynı adrese DNS sorgulaması yapıldığında farklı bir isim görülürse bu başlığın değiştirilmiş olabileceği sonucuna varılır. Bazen de e-postayı gönderen makinenin DNS ismi ile kendi üzerinde tanımlanmış ismi farklı olur ve Received kısmında iki farklı isim görülür. Örneğin makinenin ismi smtp2.xyz.com.tr olarak tanımlanmasına rağmen DNS kaydı smtp2.abc.com.tr şeklindedir [2].

B. Sahte E-posta Gönderimi

Sahte e-postalarda kullanılan çevrim içi sayfalara ait bilgiler açık kaynaklarda sıkça yer almaktadır. Örneğin www.spamhaus.org isimli sitede SBL (Spam Block List) bölümü yer almakta olup sahte, reklam veya kötü niyetli gönderildiği düşünülen e-postalardaki IP adresi ve site isimleri bu güncel veri tabanına sahip sayfadan sorgulanabilir [26].

Sahte e-posta gönderim araçlarından biri de www.wetransfer.com isimli sitedir. Bu sitede de e-posta doğrulaması yapılmadan başkası adına e-posta gönderilebilir [27].

Sahte e-posta gönderimi bir yazılım vasıtasıyla da yapılabilir. MS Windows platformunda çalışan "Private Idaho" isimli yazılım ile anonim şekilde e-posta gönderimi yapılabilir [28].

C. Geçici E-posta Hesabı

E-postayı suç işlemek amacıyla kullanan kişilerin sık başvurduğu yollar; geçici e-posta hesabı, tek kullanımlık e-posta hesabı veya günübirlik e-posta hesabı almak şeklinde olabilir. Bu yöntemlerin tercih edilme nedenleri arasında; ücretsiz ve reklamsız olmalarının yanı sıra birçoğunun kullanıcı kimliklerini gizli tutması, IP adresi kaydetmemeleri ve güvenli (şifreli) haberleşme yolunu kullanmalarıdır [23].

Bu şekilde hizmet veren çevrim içi araçlara, Hushmail, Mytrashmail, 10minutemail ve 5ymail gibi sayfalar örnek verilebilir [29-32].

www.hushmail.com sitesini incelediğimizde bu site, OpenPGP standartlarını kullanarak PGP (Pretty Good Privacy) şifreli e-posta imkânı sunmaktadır [28, 29].

Bir diğer örnekte "Remailer" olarak adlandırılan, tek kullanımlık, bir günlük ya da belirli bir süre kıstası ile kendini

imha eden e-postalardır. Buna verilebilecek bir örnek de www.mytrashmail.com sitesidir [30].

D. E-postalara İlişkin Tutulan Kayıtların Silinmesi

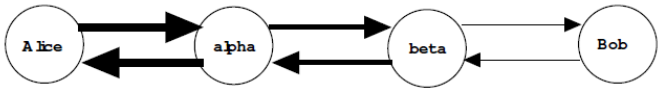
E-postalarda karşı adli bilişim teknikleri kapsamında en önemli ve en basit delil imha yöntemlerinden birisi, e-postalara ilişkin tutulan kayıtların silinmesidir. Bu kayıtların silinmesi; e-posta uygulamalarındaki (MS Outlook, Thunderbird vb.) kayıtların silinmesi, işletim sistemlerinde e-postalara yönelik tutulan kayıtların (internet geçmişi, index.dat ve Linux-mail dosyaları) silinmesi, bilgisayarın bağlı olduğu ağlardaki kayıtların (internet kullanıcı logları, MS Exchange EDB, Lotus NSF dosyaları) silinmesi şeklinde olabilir.

E-posta servis sağlayıcılarda tutulan sunucu kayıtlarında, hizmet veren firmalarca değişiklik veya silme yapılabilir. Bu sunucularda e-posta başlık bilgilerine girecek sunucu isimleri, tarih ve saat gibi zaman damgalarında manipülasyon yapılabilir [23].

Yukarıda bahsedilen bu dosyalar güvenli silme işlemi (wipe) uygulanarak geri getirilemeyecek şekilde silinirse e-posta inceleyicisinin delil tespiti büyük oranda engellenecektir.

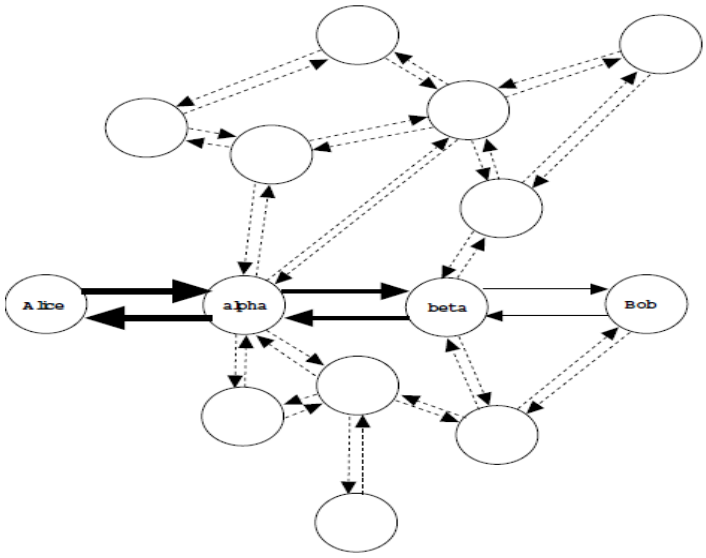
E. Vekil Sunucu veya VPN Kullanımı

E-posta gönderim işleminin bir vekil sunucu üzerinden yapılması durumunda gönderen kişinin tespiti zor olmaktadır. Şekil 5'te gösterildiği gibi Alice'ten Bob'a gönderilen bir e-posta, normal e-posta trafiğine ek olarak Alpha ve Beta isimli iki vekil sunucudan geçmiştir. Vekil sunucu veya VPN hizmeti veren firmaların birçoğu IP adresi değiştirme ve internet trafiğini şifrelemenin yanı sıra kullanıcı loglarını da tutmamaktadır. Bu durumda e-posta göndericisinin kimliğinin tespitini imkânsız kılmakta ya da çok uzatmaktadır [33].



Şekil 5. Alice ve Bob arasında iki vekil sunucu kullanılarak e-posta haberleşmesi [33].

En çok kullanılan ve açık kaynak kodlu VPN'e benzer hizmetleri barındıran TOR Project isimli hizmette, kullanıcılar en az dört farklı sunucudan geçerek internet ortamında dolaşır. Şekil 6'da TOR Project hizmetinde yer alan ve standart e-posta alışverişinin dışında Alpha ve Beta isimli vekil sunucular kullanılmış olup, Alpha ve Beta sunucuları arasında da çok sayıda başka vekil sunucular kullanılabileceği gösterilmiştir. Bu hizmet kullanılarak gönderilen bir e-postanın göndericisine ulaşmak neredeyse imkânsızdır. Teknik olarak mümkün olmasına rağmen uluslararası düzeyde ülkelerin anlaşma yapması gerektiğinden e-posta göndericisine ulaşmak çok zor ve uzun bir süreç gerektirmektedir [23, 33].



Şekil 6. Tor network üzerinde Bob ve Alice'in e-posta haberleşmesi [33].

VI. SONUÇ

Literatürde e-postaların adli incelenmesine yönelik akademik çalışmalar yer alsa da adli incelemeye karşı koyma konusunda yeterli akademik çalışma yer almamaktadır. E-postaların bilişim suçlarında doğrudan kullanılması veya diğer suçlarda da araç olarak kullanılması gerçeğinden yola çıkarak öncelikle e-postaların adli incelenmesi konusuna değinilmiş ve bu alanda kullanılan dünyada kabul görmüş yazılımlardan bahsedilmiştir. Bu yazılımların hangi amaçla kullanıldığı izah edilmiş, okuyucuya rehber olabilecek bir sunum yapılmıştır. Adli incelemenin tüm detaylarına inilmemiş, yol gösterilmiştir.

Çalışmada ayrıca e-postaların adli incelemesinde çalışan kişilerin nelere dikkat etmesi gerektiği vurgulanmış ve bu konuda bireysel ve kurumsal farkındalığı artırma amaçlanmıştır. E-postaların yapısı açıklanmış ve gönderim aşamaları izah edilmiştir. Bununla birlikte e-posta göndericisinin tespitinde en önemli aşamalardan biri olan başlık bilgileri detaylandırılmıştır. E-postaların başlık bilgilerinin ne olduğu, ne gibi bilgiler içerdiği, hangi alanların nasıl değiştirilebileceği ve başkası adına e-posta göndermenin kolaylığı, inceleme yapan kişileri yanıltıcı durumlar örneklerle açıklanmıştır.

E-postaların otomatik takibini yapan uygulamalar, e-postalara ilişkin tutulan kayıtlar ve bu kayıtların hangi araçlarla incelenebileceği detaylandırılmıştır. Kurumsal veya bireysel olarak e-posta ile ilişkili konuları inceleme konusunda hangi detaylara dikkat edilmesi gerektiği vurgulanmıştır. Başlık bilgilerinin değiştirilmesi, e-postalara ilişkin tutulan kayıtların silinmesi, sahte e-posta gönderimi, şifreli ve geçici hesapla yapılan e-posta gönderimleri ve vekil sunucu veya VPN kullanımı gibi karşı adli bilişim teknikleri ortaya konmuştur. Profesyonel olarak bir e-posta incelenmek isteniyorsa, tek bir yöntem değil, birden fazla yöntem uygulanmalıdır. İnceleme yapılmasını kolaylaştıran

uygulamaların mutlaka alternatifleri de olmalıdır. Tüm dünyada ve ülkemizde adli inceleme konusu yeni ve hızla gelişen bir alan olduğu için araştırma iyi yapılmalıdır.

Adli incelemeyi zorlaştıran, engellemeye çalışan ya da imkânsız hale getirmeyi amaçlayan karşı adli bilişim tekniklerinin bilinmesi de çok önemlidir. Bir araştırmacı veya bilirkişi, e-posta kullanılarak işlenen suçlarda, suçu işleyen hedef kişinin kendini gizleme yönünde attığı adımların neler olabileceğini iyi bilmelidir. Bu nedenle karşı adli bilişim teknikleri de çok önemlidir. İnceleyicinin herhangi bir hususu unutmasını önlemek, sistemli çalışmasını ve adım adım inceleme yapmasını sağlamak amacıyla hazırlanan kontrol listesi Tablo 1'de verilmiştir.

TABLO 1. E-POSTALARIN ADLİ OLARAK İNCELENMESİNDE KONTROL LİSTESİ

1	Gelen e-postanın hangi e-posta adresinden geldiği tespit edildi mi?	
2	Gönderici e-posta adresinin doğrulaması ve halen kullanımda olup olmadığı tespit edildi mi?	
3	Gönderici e-posta adresinin servis sağlayıcısından kime ait olduğu ve hangi bilgilerle kayıt olunduğu bilgileri talep edildi mi?	
4	Gelen e-postanın başlık bilgileri incelendi mi?	
5	Başlık bilgilerinden gönderici IP adresi tespit edildi mi?	
6	Gönderici IP adresi tespit edildi ise, tarih ve saat bilgisi ile kime ait olduğuna ilişkin internet servis sağlayıcısı ile irtibata geçildi mi?	
7	Gönderici IP adresinin vekil sunucu veya VPN kullanıldığına dair bir tespit mevcut mu? Mevcut ise vekil sunucu veya VPN sisteminin yöneticileri ile şüpheli IP adresinden kimlik tespitine yönelik irtibata geçildi mi?	
8	Başlık bilgilerinde yer alan Received alanlarındaki IP adresi, sunucu ismi ve tarih-saat bilgilerinde herhangi bir uyumsuzluk var mı?	
9	Başlık bilgilerinde yer alan DNS ismi ile DNS sorgulamasındaki isim aynı mı?	
10	Başlık bilgileri gönderici e-posta sunucusunun formatına uygun mu?	
11	Başlık bilgilerinin manipüle edildiğine dair bir şüphe var mı?	
12	Tespit edilen IP adresini kullanan bilgisayarda suça ilişkin e-postayla ilgili kayıtlar (registry, browser, internet kayıtları) incelendi mi?	
13	Suçla ilişkili bilgisayarda herhangi bir e-posta uygulaması mevcut mu? Mevcut ise incelendi mi?	
14	Suçla ilişkili bilgisayarın bağlı olduğu ağdaki kayıtları incelendi mi?	
15	Gönderici e-posta sunucusundaki kayıtlar incelendi mi?	
16	Alıcı e-posta sunucusundaki kayıtlar incelendi mi?	
17	E-posta göndericisinin kimliği belli değilse, kimliği bilinen e-postalar ile kıyaslanarak metin madenciliği uygulandı mı?	

Tablo 1'deki kontrol listesinde yer alan soruların tamamı e-postaların adli incelenmesinde kullanılabileceği gibi, birkaç tanesi de kullanılabilir. Her olay, kendine özgü çalışma gerektirir ve farklı soruları içerebilir.

Gelişen teknoloji ile beraber karşı adli bilişim teknikleri de hızla artmakta ve suç işleyen kişilerin tespiti zor olmaktadır. Ancak her zorluğu aşmak için yeni yöntemler araştırılmakta ve ortaya çıkarılmaktadır. Unutulmamalıdır ki, bilişim ortamında yapılan her işlemin kaydedildiği kaçınılmaz bir gerçektir.

KAYNAKÇA

[1] L. James, "E-Mail: The Weapon of Mass Delivery", *Syngress Force Emerging Threat Analysis*, Canada: Springer, Bölüm 10, 289-334, 2006.

[2] H. Önal, "E-posta Başlıklarından Bilgi Toplama", *Bilgi Güvenliği Akademisi*, 2009.

[3] S. Sağıroğlu, "Karşı Adli Bilişim ve Siber Güvenlik", 1. Uluslararası *Adli Bilişim Sempozyumu*, Ankara, 2014.

[4] H. Önal, "Bilişim Sistemlerinde Adli Bilişim Analizi ve Bilgisayar Olayları İnceleme"**,** *Bilgi Güvenliği Akademisi*, 2013.

[5] H. Öztürkçi, "Bilişim Suçları ve Takibi", *Adeo Bilişim Teknolojileri Eğitim Merkezi,* 2010.

[6] M. Dalyanda, "Adli Bilişim Sistem Analizi", *Beyaz Şapka Dergisi*, 4, 16-17, 2006.

[7] A. Schroader, *Alternate Data Storage Forensics*, USA: Syngress, Bölüm 5, 147-169, 2007.

[8] J.Gn.K.lığı, "Bilişim Suçları ve Bilişim Güvenliği Kursu". *Kurs Notları*, 2015.

[9] İnternet: https://toolbox.googleapps.com/apps/messageheader, (Erişim Tarihi: 7 Nisan 2015).

[10] İnternet: http://mxtoolbox.com/EmailHeaders.aspx , (Erişim Tarihi: 7 Nisan 2015).

[11] İnternet: http://www.iptrackeronline.com/email-header-analysis.php, (Erişim Tarihi: 7 Nisan 2015).

[12] İnternet: http://www.gaijin.at/en/olsmailheader.php, (Erişim Tarihi: 7 Nisan 2015).

[13] İnternet: https://support.google.com/mail/answer/22454?hl=en, (Erişim Tarihi: 7 Nisan 2015).

[14] İnternet: http://www.nirsoft.net/utils/ipnetinfo.html, (Erişim Tarihi: 7 Nisan 2015).

[15] L Daniel ve L. Daniel, "E-mail Evidence" *Digital Forensics for Legal Professionals*, USA: Syngress, Bölüm 34, 239-244, 2012.

[16] C. Albrecht, Email Analysis, İnternet: http://www.gsaig.gov/assets/File/other-documents/Forensics-EmailAnalysis.pptx.pdf, (Erişim Tarihi: 10 Nisan 2015).

[17] H. Çakır ve M.S. Kılıç, "Bilişim Suçlarına İlişkin Delil Elde Etme Yöntemlerine Genel Bir Bakış", *Polis Bilimleri Dergisi*, 15 (3), 23-44, 2013.

[18] T. Fair, M. Nordfelt, S. Ring ve E. Coler, "Spying on E-mail", *Cyber Spying*, USA:Syngress, Bölüm 8, 291-316, 2005.

[19] V.K. Devendran, H. Shahriar ve V. Clincy, "A Comparative Study of Email Forensic Tools", *Journal of Information Security*, 6 (2), 111-117, 2015.

[20] J. Sammons, "Internet and E-Mail" *The Basics of Digital Forensics*, USA: Syngress, Bölüm 8, 119-131, 2015.

[21] F. Iqbal, H. Binsalleeh, B.C.M. Fung ve M. Debbabi, "Mining writeprints from anonymous e-mails for forensic investigation", *Digital Investigation*, 7 (1-2), 56-64, 2010.

[22] F. Iqbal, R. Hadjidj, B.C.M. Fung ve M. Debbabi, "A novel approach of mining write-prints for authorship attribution in e-mail forensics", *Digital Investigation*, 5, 42-51, 2008.

[23] D. Bradbury, "Can we make e-mail secure?", *Network Security*, 3, 13-16, 2014.

[24] İnternet: https://emkei.cz/. (Erişim Tarihi: 10 Nisan 2015).

[25] M.T. Banday, F.A. Mir, J.A. Qadri ve N.A. Shah, "Analyzing Internet E-mail Date-Spoofing", *Digital Investigation*, 7 (3-4), 145-153, 2011.

[26] İnternet: http://www.spamhaus.org/sbl/ (Erişim Tarihi: 25 Nisan 2015).

[27] İnternet: https://www.wetransfer.com/ (Erişim Tarihi: 25 Nisan 2015).

[28] P. Loshin, "E-mail Security and Anonymity Practices", *Practical Anonymity*, USA:Syngress, Bölüm 7, 103-112, 2013.

[29] İnternet: https://www.hushmail.com/ (Erişim Tarihi: 1 Mayıs 2015).

[30] İnternet: http://www.mytrashmail.com/ (Erişim Tarihi: 1 Mayıs 2015).

[31] İnternet: https://www.5ymail.com/ (Erişim Tarihi: 1 Mayıs 2015).

[32] İnternet: http://www.10minutemail.com/ (ErişimTarihi: 1 Mayıs 2015).

[33] P. Wayner, "Anonymous Remailers", *Dissappearing Cryptography*, USA: Morgan Kaufmann, Bölüm 10, Sayfa 193-230, 2009.

Şeref SAĞIROĞLU, Gazi Üniversitesi Fen Bilimleri Enstitüsü Müdürü ve Bilgisayar Mühendisliği Bölüm Başkanıdır.

Eyüp Burak CEYHAN, Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümünde araştırma görevlisidir.

Rıfat MARAŞ, Gazi Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği ABD'da Yüksek Lisans öğrenimine devam etmektedir.