E-MAIL FORENSICS

- İstanbul Şehir Üniversitesi -

Bilgi Güvenliği Mühendisliği Yüksek Lisans Programı Bilgisayar Adli Analizi Dersi

NOT: Eğitmenlerimizden Huzeyfe Önal'ın İstanbul Şehir Üniversitesi 2016 bahar döneminde Yüksek Lisans Programı Adli Bilişim Dersi öğrencileri tarafından hazırlanmıştır.

Hazırlayan: Burak Özdemir & Yalçın Atik

Tarih: 29.05.2016

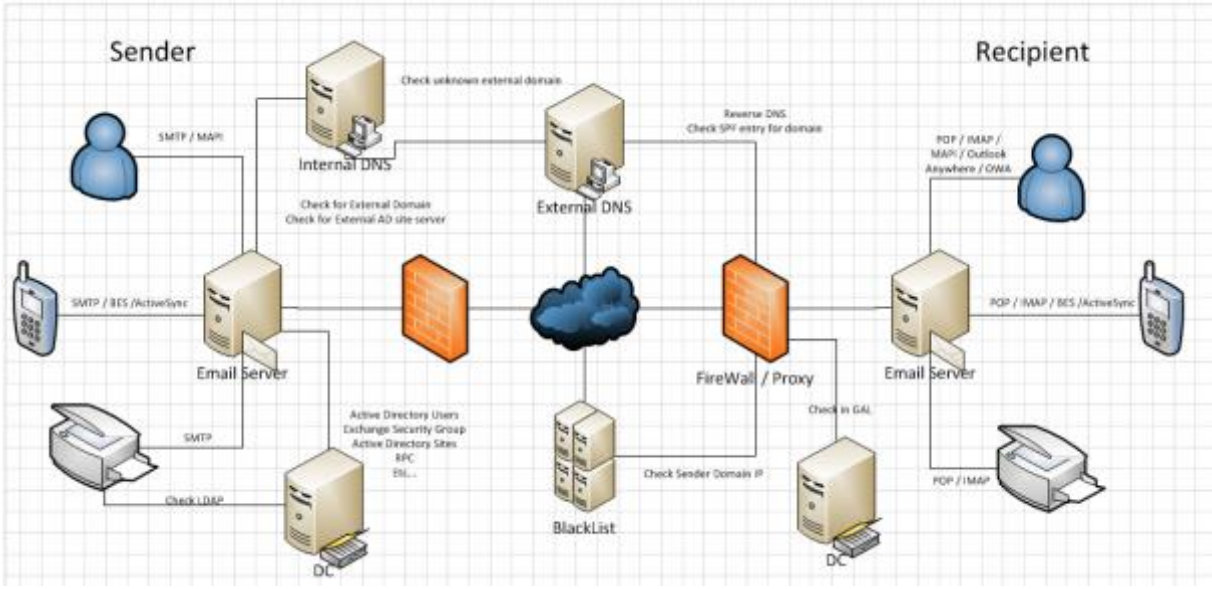
E-Mail Forensics

Adli bilişim incelemesinde elektronik postaların incelenmesi sonucunda önemli deliller elde edilebilir. Sadece elektronik posta ile işlenen suçların bulunmasında değil, veri hırsızlığı ve apt saldırısı gibi olaylarda da elektronik postalar incelenerek olayın çözülmesi için kritik öneme sahip deliller elde edilebilir. Elektronik postalar; elektronik posta sunucularında, kullanıcı bilgisayarında, web mail hizmeti sunan sunucularda ve mobil istemcilerde bulunabilir.

E-Mail Forensics ile neler öğrenilebilir?

Elektronik postayı kimin gönderdiğini öğrenmek için; mail adresine, ip adresine, mailin içeriğine bakılabilir.
Elektronik postanın ne zaman gönderildiğini öğrenmek için; başlık bilgisinde yer alan tarih ve zamana, mail sunucusundaki tarih ve zamana bakılabilir.
Elektronik postanın nereden gönderildiğini öğrenmek için; ip adresine, ISP bilgisine, geo-location bilgisine, mail sunucusu domainine bakılabilir.
Yardımcı başka içerik olup olmadığını öğrenmek için; mesajın kendisine, eklerine, adres defterine, takvim kayıtlarına, görev kayıtlarına bakılabilir.

E-Mail gönderildiğinde izlediği yol nedir?



[E-MAIL FORENSICS]

E-Mail içindeki hangi kısımlar analiz edilebilir?

Bir elektronik posta içindeki üç kısım analiz edilebilir. Bunlar; Mesajın gövdesi, Mesajın ekleri, Mailin başlığı şeklindedir.

Mesajın Gövdesi

Kullanıcı tarafından yazılan kısımdır.
Karakter arama özelliği, analiz sürecini hızlandırabilir.
İkili formatta saklanıyor olabilir bu sebeple kullanılan yazılım bunu anlayabilmelidir.
En kolay analiz etme yöntemi manuel analizdir.

Mesajın Ekleri

Eklerin incelenmesi sonucunda ciddi delillere ulaşılabilir.
Yapılan araştırmalarda saklanan mesajların %80 ini ekler oluşturmaktadır.
Elektronik posta standartı sadece ASCII karakterlerinin transfer edilmesine imkân tanıyacak şekilde geliştirilmiştir. Bu yüzden bu ekler encode edilip o şekilde gönderilmelidir.
Eklerin görüntülenmesi için uygun şekilde decode edilmesi şarttır.
Analiz edilirken zararlı kodlar göz önünde bulundurulmalı ve dikkat edilmelidir.

Elektronik Posta Başlığı / Detayları

Received: Elektronik postanın hedefine ulaşırken uğradığı MTA'Iarı gösterir. Genellikle bir mail başlığında birden fazla bulunur ve mailin izlediği güzergâhı bulmak için aşağıdan yukarıya doğru okunmalıdır.
Message-ID: Orjinal mail sunucusu tarafından eklenen bir numaradır ve o mail sunucusu içinde tekil bir numaradır. Mail sunucusu üzerinde bu ID ile arama yapılarak detaylara ulaşılabilir. @ işaretinden sonra sunucunun adı yer alır.
X-Originating-IP: Bu alan opsiyonel bir alan olup, özellikle web tabanlı elektronik postaların hangi IP adresi üzerinden gönderildiğini belirtmek için kullanılır Bazı web tabanlı mail hizmeti sunun firmalar bu başlığı eklerken, bazıları eklemezler.
X-Mailer: Elektronik postanın hangi istemci uygulaması ile oluşturulduğunu belirten başlık bilgisidir. Opsiyonel bir alandır ve elektronik postanın bir istemci yazılımı ile mi yoksa web tabanlı bir istemci ile mi oluşturulduğunu göstermesi açısından önemlidir.

E-Mail Başlığında X-Originating-Ip

```
Return-Path: <deekayen@deekayen.net>
Delivered-To: <deekayen@deekayen.net>
Received: from lttleman.deekayen.net
    by lttleman (Dovecot) with LMTP id xAXVMPm1OVKZfwAAgBl5nA
    for <deekayen@deekayen.net>; Wed, 18 Sep 2013 10:17:29 -0400
Received: by lttleman.deekayen.net (Postfix, from userid 33)
    id B702488577; Wed, 18 Sep 2013 10:17:29 -0400 (EDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=deekayen.net;
    s=mail; t=1379513849;
    bh=vyuTUHcafyfYoSEzb8lsThGuPXC3ROLC46MlAZ3LPKM=;
    h=To:Subject:From:Date:From;
    b=b0NoXSs42xUXZDv4DTcH2xT4y7I2/QG/2JG+7PwBlw5+xs4lGpO80eJY8OZ2NbHWG
     5t+L1nm3bqlr5DF4Pl9xYFu6uOaLLFnbSdLXEF693pBJ4cKPn15rAz5Py13CsHUbWw
     atggNzR5leW/uul8QAqwoLDnl+yh09sm5oIS8dsI=
To: deekayen@deekayen.net
Subject: Replacement login information for deekayen at David Norman
X-PHP-Originating-Script: 6226:system.mail.inc
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8; format=flowed; delsp=yes
Content-Transfer-Encoding: 8Bit
X-Mailer: Drupal
Sender: deekayen@deekayen.net
From: deekayen@deekayen.net
X-Originating-IP: [216.119.148.77]
Message-Id: <20130918141729.B702488577@lttleman.deekayen.net>
Date: Wed, 18 Sep 2013 10:17:29 -0400 (EDT)

deekayen,

A request to reset the password for your account has been made at David
Norman.

You may now log in to deekayen.net clicking on this link or copying and
pasting it in your browser:
```

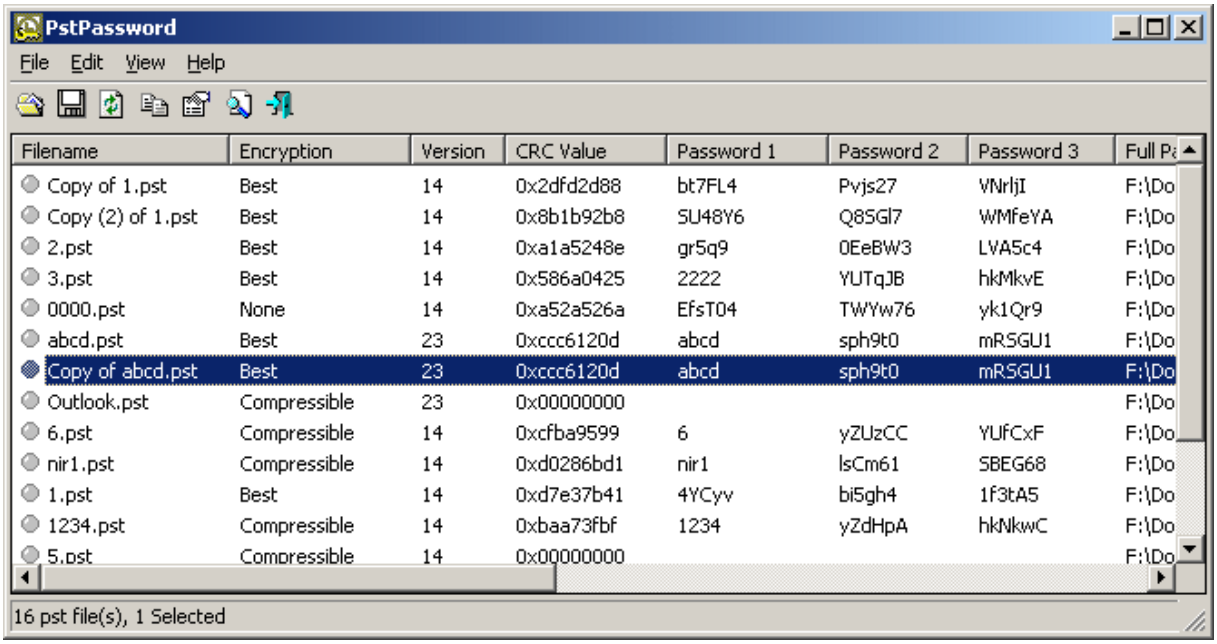
Host Tabanlı E-Mail

Bu tür elektronik postalar mail sunucusunda değil yerelde saklanırlar. Bu dosyaların yerini tespit etmek için; dosya türüne göre arama yapılır, elektronik posta istemcisinin ayarları gözden geçirilir, index ya da mesaj dosyaları aranır. Bu tür dosyalar şifre ile korunuyor olabilir. Gerçekleştirilen adli incelemelerde silinmiş olduklarına sıklıkla rastlamak mümkündür.

Microsoft Outlook

Outlook tarafında kullanılan kişisel klasörün uzantısı genellikle pst' dir. Bu dosya Outlook 2010 ile 50 gb boyutuna ulaşabilmektedir. Bu dosyanın içinde elektronik postalar, postaların ekleri, takvimler, adres defteri toplu halde yer alır. Registry analizi ile bu dosyaların bulunduğu konum öğrenilebilir. Bir bilgisayar üzerinde birden fazla pst dosyası kullanılıyor olabilir. Bu dosyalar sıkıştırılabilir ve içerikleri şifreleme ile korunur, şifrelerini kırmak için PstPassword uygulaması kullanılabilir.

PstPassword



Filename	Encryption	Version	CRC Value	Password 1	Password 2	Password 3	Full P
Copy of 1.pst	Best	14	0x2dfd2d88	bt7FL4	Pvjs27	VNrljI	F:\Do
Copy (2) of 1.pst	Best	14	0x8b1b92b8	SU48Y6	Q8SGl7	WMfeYA	F:\Do
2.pst	Best	14	0xa1a5248e	gr5q9	0EeBW3	LVA5c4	F:\Do
3.pst	Best	14	0x586a0425	2222	YUTqJB	hkMkvE	F:\Do
0000.pst	None	14	0xa52a526a	EfsT04	TWYw76	yk1Qr9	F:\Do
abcd.pst	Best	23	0xccc6120d	abcd	sph9t0	mRSGU1	F:\Do
Copy of abcd.pst	Best	23	0xccc6120d	abcd	sph9t0	mRSGU1	F:\Do
Outlook.pst	Compressible	23	0x00000000				F:\Do
6.pst	Compressible	14	0xcfba9599	6	yZUzCC	YUfCxF	F:\Do
nir1.pst	Compressible	14	0xd0286bd1	nir1	lsCm61	SBEG68	F:\Do
1.pst	Best	14	0xd7e37b41	4YCyv	bi5gh4	1f3tA5	F:\Do
1234.pst	Compressible	14	0xbaa73fbf	1234	yZdHpA	hkNkwC	F:\Do
5.pst	Compressible	14	0x00000000				F:\Do

Microsoft Outlook Express

Windows işletim sistemlerinde bulunan ücretsiz elektronik posta uygulamasıdır, Outlook gibi gelişmiş özelliklere sahip değildir. İçerik DBX dosyalarında saklanır, kullanıcı tarafından oluşturulan her bir klasör ayrı DBX dosyası altında saklanır. Bu dosyalar sıkıştırma ve şifreleme yapılmadığı için işletim sistemi tarafındaki aramalarda da bu dosya içerisinde arama yapılmış olur. Silinen mesajlar bu dosya compact edilinceye kadar saklanır. Eğer compact edilirse, bu işleme dair bir cleanup.log uzantılı bir log dosyası oluşturulur.

Windows Mail

Outlook Express sonrası onun yerine gelen ücretsiz posta uygulamasıdır. Elektronik postaların her biri ayrı ayrı EML uzantılı dosyalarda depolanır. Klasör ve index bilgileri ise FOL uzantılı dosyalarda tutulur. EML dosyaları sade metin şeklindedir ve başlık bilgileri de içinde yer almaktadır. Silinen elektronik postalar silinen öğeler isimli bir klasör altında EML şeklinde saklanmaktadır.

[E-MAIL FORENSICS]

Mozilla Thunderbird

Açık kaynak kodlu bir posta uygulamasıdır ve Windows, Mac Os ve Android üzerinde çalışabilir. Mesajların saklandığı dosyanın herhangi bir uzantısı yoktur ve mbox formatındadır, her bir klasör içinse MSF uzantılı bir index dosyası tutulur. Silinen mesajlar veri tabanından silinmezler compact işlemi gereklidir ve bu işlem otomatik olarak kapalıdır.

Diğer eposta istemcileri

Kullanıcılar tarafından kullanılabilecek birçok elektronik posta uygulaması bulunabilir. Bu yazılımları ilk bakışta tespit etmek zor olabilir ancak kurulu uygulamaların listesi çıkarılarak elektronik posta istemcisi yazılımları ile karşılaştırılarak bulunabilir.

Takvim, Kişiler ve Görevler

Günümüzde elektronik posta istemcileri sadece posta alıp göndermek için kullanılmıyor. Adli analiz incelemesinde kullanıcının takviminde yer alan bilgiler, kişiler ve tanımlı görevler önemli bilgiler içerebilir. Genellikle takvimle ical standartında ics formatında saklanır. Mozilla Thunderbird takvim kayıtlarını SQlite formatında SDB veri tabanında saklanır. Outlook Express adres defterini WAB uzantılı saklarken, Outlook PAB uzantılı dosyada saklar ikili dosya formatındadır. Geri kalan adres defteri formatları genellikte metin şeklindedir.

Şifreli Elektronik Posta İletimi

Elektronik postalar kullanıcı tarafından aksi belirlenmedikçe clear text olarak iletilir. Spesifik bir elektronik postayı şifrelemek için genelde aşağıdaki iki protokol kullanılır;

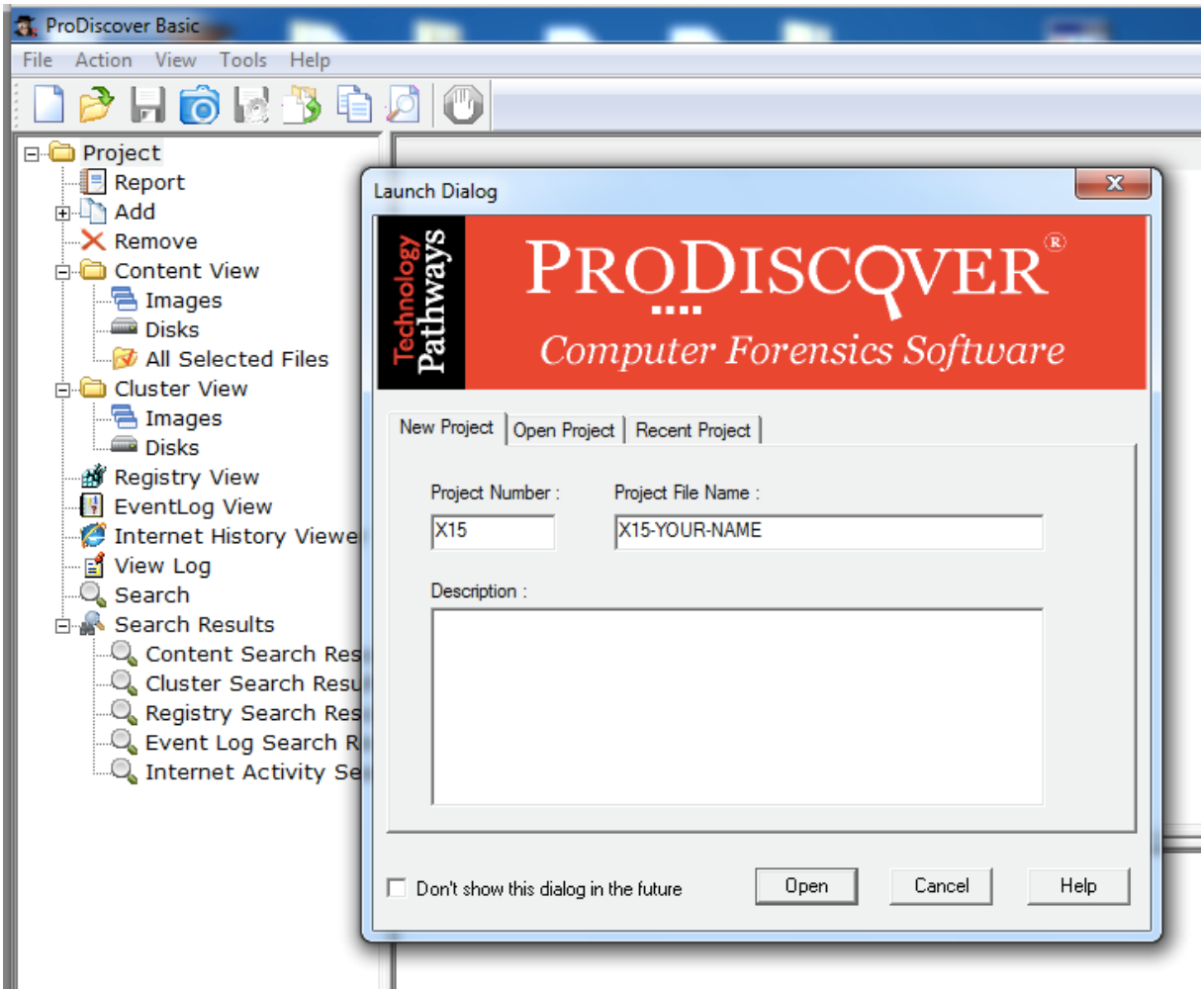
S/MIME
PGP/MIME

Bu elektronik postalar saklanırken de şifrelenmiş şekilde saklanır.

Forensics Yazılımları ile E-mail Analizi

Günümüzde kullanılan bir çok ticari adli bilişim yazılımı, incelenen disk içinde yer alan elektronik postalara ilişkin de analiz yapma yeteneğine sahiptir. Bu yazılımlar ilgili disk imajı içinde yer alan elektronik postaları bulma, indeksleme ve bu elektronik postalar üzerinde arama yapma seçenekleri sunarlar.

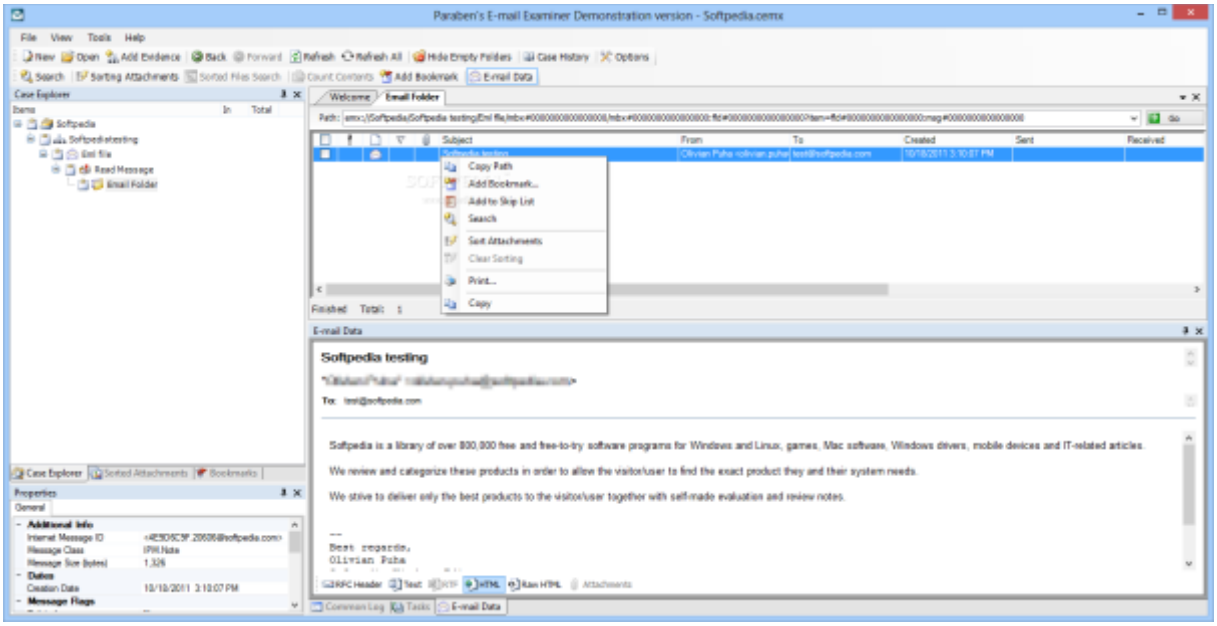
ProDiscover



[E-MAIL FORENSICS]

Paraben's E-mail Examiner

Paraben E-mail Examiner, sadece elektronik posta analizi gerçekleştirmek için kullanılabilecek ticari bir uygulamadır ve aşağıda listesi verilen elektronik posta formatlarının tamamını destekler.
America On-line (AOL)
Microsoft Outlook (PST)
Microsoft Outlook Offline Storage (OST)
The Bat! (sürüm 3.x ve daha yukarısı)
Thunderbird
Outlook Express
Eudora
EML dosyaları
Windows Mail veri tabanları
75o'den fazla MIM E tipi ve dosya uzantısı desteği
Plain Text mail
Paraben E-mail Examiner, analiz edilecek elektronik postalar üzerinde gelişmiş arama yapmaya imkân tanıyan bir Search ara yüzüne sahiptir.



Elektronik posta sunucuları

Birçok kurumsal yapı içinde elektronik posta sunucuları yer almaktadır. Bazı elektronik postalar istemciye hiç indirilmeden sunucu üzerinde tutulabilir. Günümüzde genellikle hem istemci de hem de sunucuda aynı elektronik postaların tutulduğuna şahit oluyoruz. (Offline kullanım vb.) Bu sunucular şirket içinde barındırabileceği gibi uzak bir lokasyonda da yer alabilir. Bu durum, elektronik postaların yer aldığı dosyalara erişimi zorlaştırabilir ya da imkânsızlaştırabilir. Bu sunucuların kapatılıp ardından imajlarının alınması her zaman mümkün olmayabilir.
Bir Adli Bilişim Uzmanı aşağıdaki dört seçeneğe sahiptir;

[E-MAIL FORENSICS]

Mail sunucusunun full disk imajını almak
Mantıksal ya da volume bazında imaj almak
E-mail veri tabanı dosyaların: export etmek
E-mail sunucusunun yedekleri üzerinde çalışmak

Microsoft Exchange Server

Günümüzde en çok kullanılan kurumsal mail sunucu sistemidir.
Exchange Server tarafından kullanılan dosyalar şunlardır;
Her bir storage grup iki ana dosyadan oluşur. Bu dosyalardan birisi mailleri, kontakları, görevleri, notları tutan. EDB uzantılı veri tabanı dosyası iken, bu mailler içinde yer alan multimedya içerikleri saklamak için .STM uzantılı ikinci bir dosya kullanılır.
Örneğin, priv1.edb ve priv1.stm gibi.
Exchange server üzerinde işlem yapan uygulamaların neredeyse tamamı bu iki dosyanın da olmasını zorunlu koşar.
Bir Exchange sunucusunda birden fazla storage grup olabilir ve bu durumda doğru veri tabanları üzerinde çalışıldığından emin olmak için ilgili sistemin yöneticisi ile çalışmakta fayda vardır.

Microsoft Exchange İçinden Silinmiş Öğeler

Kullanıcı tarafından silinen mailleri kullanıcının posta kutusu içinde yer alan silinmiş öğeler klasörüne taşınır. Bu tür silme işlemine soft silme denir. Eğer kullanıcı silme sırasında shift tuşuna basarsa hard bir silme işlemi gerçekleşir ve obje direk çöp sepetine gider. Bir kullanıcı tarafından silinen elektronik postaların ve mail sunucusundan silinen posta kutusunun ne kadar süre daha sistemde saklanacağını ilgili storage group ayarlarından silme ayaları ile belirlenir. Varsayılan olarak silinen postalar 14 gün silinen posta kutuları da 30 gün süreyle veri tabanında kalırlar.

Microsoft Exchange Serverdaki Verilere Erişim

Online
Exchange server üzerinde tutulan verilere iki farklı yöntemle ulaşılabilir. Bunlardan birincisi Exchange Server çalışır durumdayken gerçekleştirilen erişim yöntemidir ve buna online erişim denir. Bu yöntemde Exchange Server kullanıcılara hizmet verirken, diğer taraftan NT Backup veya Exchange Server uyumlu başka bir yedekleme yazılımı ile ilgili Exchange sunucusundaki veri tabanlarına bağlantı gerçekleştirilir ve ilgili veri tabanlarının bir yedeği alınır. Bu yöntem en güvenli yöntemdir fakat bu yedeklerin inceleme amaçlı başka bir sunucuya restore edilme işlemi ciddi şekilde zaman alacaktır.

Offline
Exchange veri tabanlarının unmount edilmesi ve ardından dosya seviyesinde EDB ve STM dosyalarının kopyalanması esasına dayanan ikinci yönteme ise offline erişim yöntemi denir. Bu işlen sırasında veri tabanları offline moda alındığı için ilgili veri tabanlarında posta kutuları bulunan kullanıcıların bu işlem sırasında posta alış verişleri kesintiye uğrar. Bir çok Forensics yazılımı bu iki dosya üzerinde direkt çalışabildikleri için online erişimde olduğu gibi ekstradan

bir geri dönme işlemine gerek yoktur. EDB ve STM dosyalarının kopyalarını almadan önce bu dosyaların tutarlılıklarını eseutil yardımı ile kontrol etmek ve sağlıklı olduklarından emin olduktan sonra dosyaları kopyalamak en doğru yaklaşım olacaktır.

DumpsterAlwaysOn Kayıt Defteri Değeri

Normalde sadece «Deleted Items» klasörü üzerinde iken aktif olan «Recover Deleted Items» seçeneğini diğer klasörlerden silinen objeleri kurtarmak için de kullanmak istiyorsak aşağıdaki kayıt defteri değerini 1 olarak girmemiz gerekiyor.

• HKEY_LOCAL_MACHINE\Software\Microsoft\Exchange\Client\Optıons\DumpsterAwaysOn

Outlook 2007 den önceki versiyonlar için bu zorunludur. Outlook 2007 ve sonrasında varsayılan olarak bu değer 1 olarak gelir ve bütün klasörler üzerinde silinmiş öğe kurtarma işlemi yapılabilir.

Silinmiş Elektronik Postaların Kurtarılması

Kullanıcı tarafından silinen elektronik postaların Exchange üzerinden geri getirilmesi noktasında Exchange 2010 gelişmiş özellikler sunmaktadır. Dumpster 2 olarak da adlandırılan özellik sayesinde kullanıcı tarafından silinen mesajlara ait çok daha detaylı bilgilere ulaşmak ve bu mesajları kurtarmak mümkündür.

OST dosyaları

Son kullanıcının bilgisayarında bulunabilecek ve içerisinde elektronik posta bulunan bir diğer dosya türü ise Offline Folder olarak isimlendirilen ve Exchange Server'ın Cached Mode'da kullanılması durumunda bilgisayarda oluşturulan OST uzantılı dosyalardır. OST dosyaları sayesinde kullanıcı Exchange Server'a bağlı olmadan da kendi posta kutusundaki postalara ulaşabilir ve o postaları okuyabilir. Adli bilişim açısından bu dosyanın diğer bir avantajı, sunucu üzerinden silinen elektronik postalara OST dosyası içinde rastlamanın mümkün olma ihtimalidir. Özellikle Exchange Server'da meydana gelen bir sorundan ötürü (Exchange Server'ın yeniden kurulması veya mailbox store'un bozulması vb gibi) kullanıcının yeniden Exchange Server ile bağlantı kurmasının ardından bilgisayar üzerinde yetim (orphan) OST'ler oluşur ve adli bilişim incelemeleri açısından bu dosyaların analiz edilmesi de oldukça önemlidir.

Lotus Notes

Lotus Notes, iş dünyasında en çok karşılaşılan ikinci elektronik posta istemcisi olarak karşımıza çıkmaktadır ve Lotus Domino üzerinde tutulan veri tabanlarına erişim için kullanılır. Notes tarafından kullanıcıya gösterilen her şey Domino üzerindeki veri tabanlarında tutulurlar ve E-mail bu veri tabanlarından sadece biridir. Bunun yanında takvim, to-do listeleri, dokümanlar, kontaklar hepsi birer veri tabanıdır. Veri tabanları .NSF uzantılıdırlar ve hem sunucuda hem de istemcide NSF uzantılı veri tabanı dosyalarına rastlamak mümkündür.

Web Tabanlı Elektronik Postalarda Adli İnceleme

Web tabanlı elektronik postalar, gerçekleştirilen adli bilişim incelemesini zorlaştırırlar. Bunun başlıca sebebi genellikle bu türden postalar kullanıcıların bilgisayarında offline bir şekilde tutulmazlar ve kullanıcı web tabanlı elektronik posta servislerine bir browser aracılığı ile bağlanır ve bu servisi kullanır. Bazı durumlarda kullanıcıların web tabanlı eposta servislerini POP veya IMAP üzerinden bir istemci vasıtasıyla kullanırlar ve bu durumda gerçekleştirilecek inceleme yukarıda anlatılan eposta istemcileri üzerinden yapılan analizle aynı şekilde ilerler. Fakat genellikle kullanıcının bilgisayarında web tabanlı elektronik posta servisi üzerinden eriştiği, okuduğu, yolladığı postalara ilişkin izlere ulaşmak için geleneksel adli bilişim teknikleri kullanılır. Örneğin disk imajı üzerinden karakter arama veya carving ile veri kurtarma gibi.

Web tabanlı elektronik posta servisleri üzerinden gerçekleştirilecek incelemede genellikle ISP veya mail servisini veren şirkete yasal başvuru yapılır ve buralardan gelecek yanıtlar üzerinden dava devam eder. Bu başvuru sırasında şüpheli tarafından hangi elektronik posta adreslerinin kullanıldığının tespiti için incelenen sabit diskteki browser geçmişi, auto-complate ve protected storage alanlarından elde edilen bilgilere başvurulabilir. Bu bilgiler ışığında yapılacak başvuru ile ilgili eposta adresine hangi IP adresleri üzerinden bağlantı gerçekleştirildiği gibi ekstra bilgiler de servis sağlayıcıdan istenebilir ve akabinde soruşturma bu bilgilerle genişletilebilir.

BGA Bilgi Güvenliği A.Ş. Hakkında

BGA Bilgi Güvenliği A.Ş. 2008 yılından bu yana siber güvenlik alanında faaliyet göstermektedir. Ülkemizdeki bilgi güvenliği sektörüne profesyonel anlamda destek olmak amacı ile kurulan BGA Bilgi Güvenliği, stratejik siber güvenlik danışmanlığı ve güvenlik eğitimleri konularında kurumlara hizmet vermektedir.

Uluslararası geçerliliğe sahip sertifikalı 50 kişilik teknik ekibi ile, faaliyetlerini Ankara ve İstanbul ve USA'da sürdüren BGA Bilgi Güvenliği'nin ilgi alanlarını "*Sızma Testleri, Güvenlik Denetimi, SOME, SOC Danışmanlığı, Açık Kaynak Siber Güvenlik Çözümleri, Büyük Veri Güvenlik Analizi ve Yeni Nesil Güvenlik Çözümleri*" oluşturmaktadır.

Gerçekleştirdiği başarılı danışmanlık projeleri ve eğitimlerle sektörde saygın bir yer edinen BGA Bilgi Güvenliği, kurulduğu günden bugüne alanında lider finans, enerji, telekom ve kamu kuruluşlarına 1.000'den fazla eğitim ve danışmanlık projeleri gerçekleştirmiştir.

BGA Bilgi Güvenliği, kurulduğu 2008 yılından beri ülkemizde bilgi güvenliği konusundaki bilgi ve paylaşımların artması amacı ile güvenlik e-posta listeleri oluşturulması, seminerler, güvenlik etkinlikleri düzenlenmesi, üniversite öğrencilerine kariyer ve bilgi sağlamak için siber güvenlik kampları düzenlenmesi ve sosyal sorumluluk projeleri gibi birçok konuda gönüllü faaliyetlerde bulunmuştur.

BGA Bilgi Güvenliği AKADEMİSİ Hakkında

BGA Bilgi Güvenliği A.Ş.'nin eğitim ve sosyal sorumluluk markası olarak çalışan Bilgi Güvenliği AKADEMİSİ, siber güvenlik konusunda ticari, gönüllü eğitimlerin düzenlenmesi ve siber güvenlik farkındalığını arttırıcı gönüllü faaliyetleri yürütülmesinden sorumludur. Bilgi Güvenliği AKADEMİSİ markasıyla bugüne kadar "Siber Güvenlik Kampları", "Siber Güvenlik Staj Okulu", "Siber Güvenlik Ar-Ge Destek Bursu" , "Ethical Hacking yarışmaları" ve "Siber Güvenlik Kütüphanesi" gibi birçok gönüllü faaliyetin destekleyici olmuştur.