OUTLOOK
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: Fevziye Taş

Tarih: 29.05.2016

Outlook Email Adli Analizi Ödevi

Kullanılan Araçlar

- Outlook 2016 for Windows 64-bit(Home trial version)
- Systools Free Outlook OST File Viewer

Outlook 2016'nın oluşturduğu ve email hesabıyla ilgili bilgileri içeren .ost outlook veri dosyası *drive:\Users\user\AppData\Local\Microsoft\Outlook* dizininde tutulmaktadır. Emaillere ait başlık bilgilerini elde etmek için kullanılan bazı adli analiz yazılımlarına örnek olarak Aid4Mail, MailXaminer, Paraben E-Mail Examiner gibi programlar sayılabilir. Ücretsiz yazılımlardan biri olan Free Outlook OST File Viewer email başlıklarını başarılı bir şekilde çıkarmakta ve silinmiş mailleri de geri getirebilmektedir. Aid4Mail, Outlook 2016'ın 64 bit versiyonunu desteklemediği için hata vermektedir.

Email Başlık(Header) Bilgileri

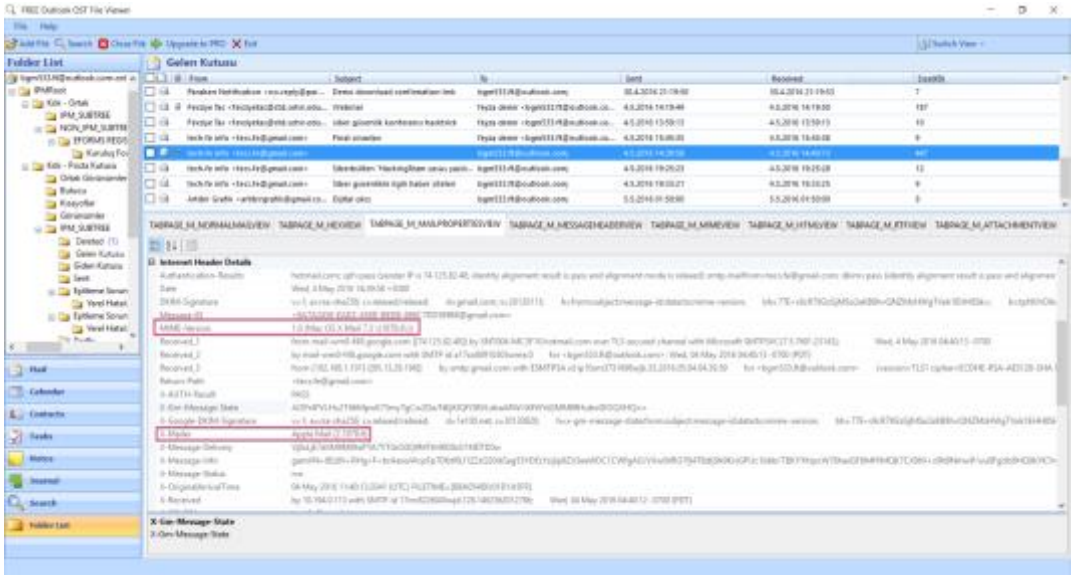
- **From**: Mailin kimden geldiği bilgisini içerir.
- **To**: Mailin kime gönderildiğini belirtir.
- **Received**: Mailin alıcıya ulaşana kadar geçtiği sunucuları belirtir, maili alan cihaz ve mailin hangi cihazdan alındığı gibi bilgileri içerir. Birden fazla Received alanı varsa en alttaki göndericinin cihazı ile ilgili IP bilgilerini verirken üstteki Received etiketleri ise aradaki sunucuların ve alıcı sunucusunun IP bilgilerini tutar.
- **MIME-Version**: Email içeriğinin formatını genişleten bir internet standardı olarak tanımlanmaktadır. Bazı durumlarda göndericinin cihazının işletim sistemi hakkında bilgi sızdırabilmektedir.
- **Message-ID**: Mail ilk oluşturulduğunda sistem tarafından atanan tekil bir karakter dizisidir. Bazı durumlarda gönderici cihazın işletim sistemi hakkında bilgi verir.
- **X-Mailer**: Göndericinin kullandığı mail programı hakkında bilgi verir.
- **X-Originating-IP**: Göndericinin IP adresi ile ilgili bilgi verir.

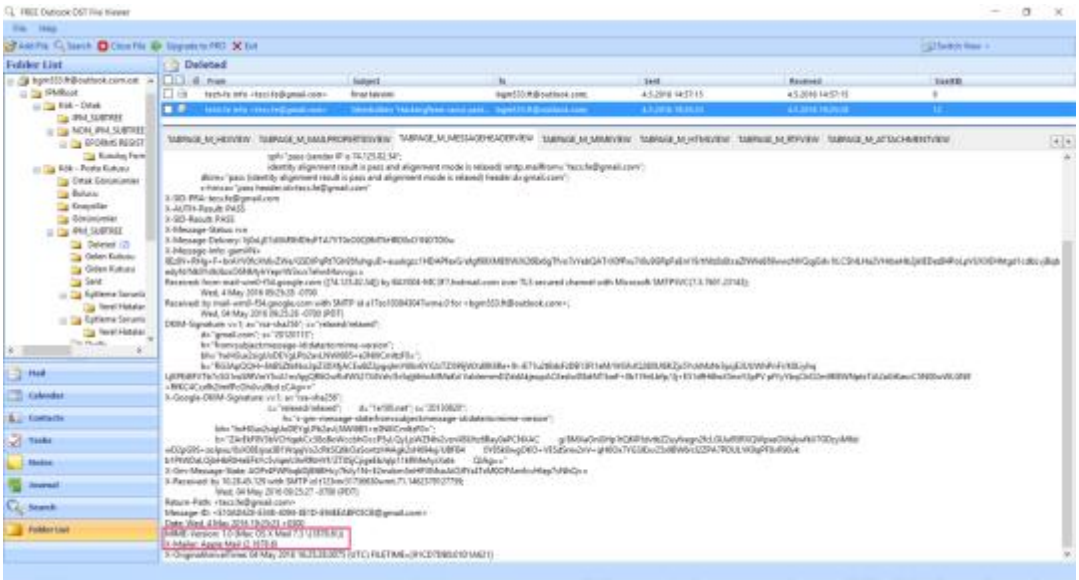
Gönderici IP bilgilerinin veya internet servis sağlayıcılarına ait IP ve şifreleme algoritmaları gibi hassas verilerin email başlıklarından elde edilebilir olması bir zafiyet olarak değerlendirilmektedir. Bu bilgilerle IP adreslerinin ait olduğu cihazlar için port taraması yapılabilir ve ardından siber saldırılar düzenlenebilir.

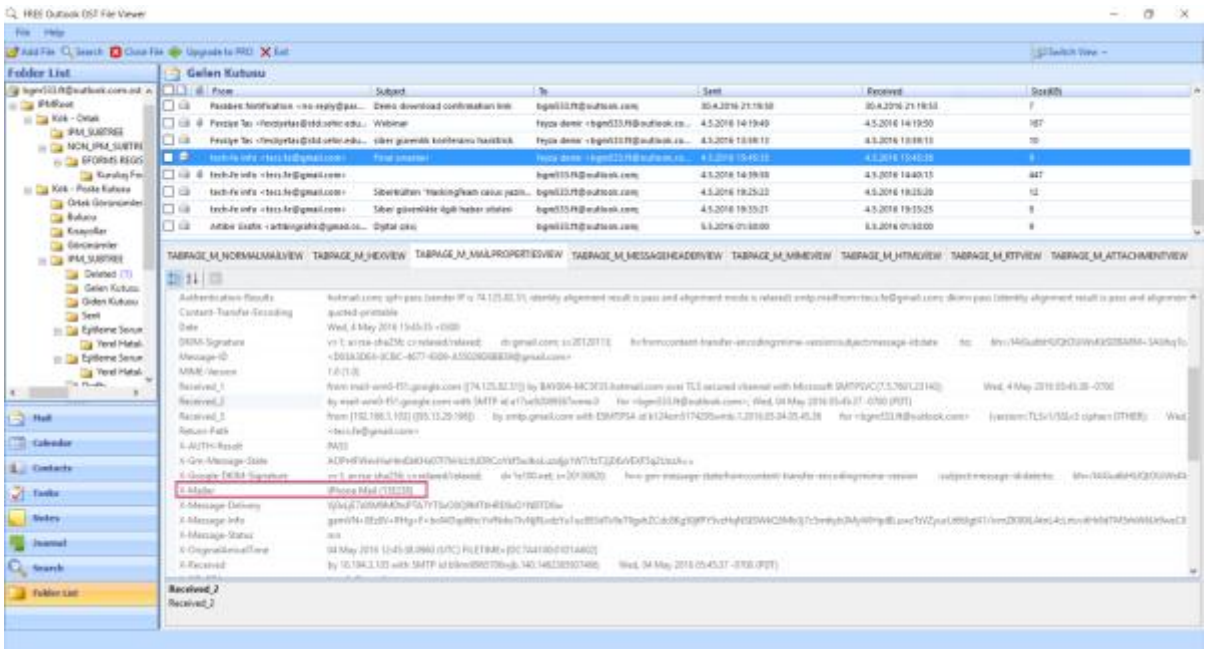
Outlook Email Analizi

- **Göndericinin kullandığı cihazın işletim sistemini ve mail programını belirlemek** (MIME-Version and X-Mailer etiketleri)

X-Mailer, MIME-Version gibi başlıkların göndericinin kullandığı cihazın işletim sistemi ve mail programı hakkında ipuçları verdiğini aşağıdaki ekran alıntıları göstermektedir.

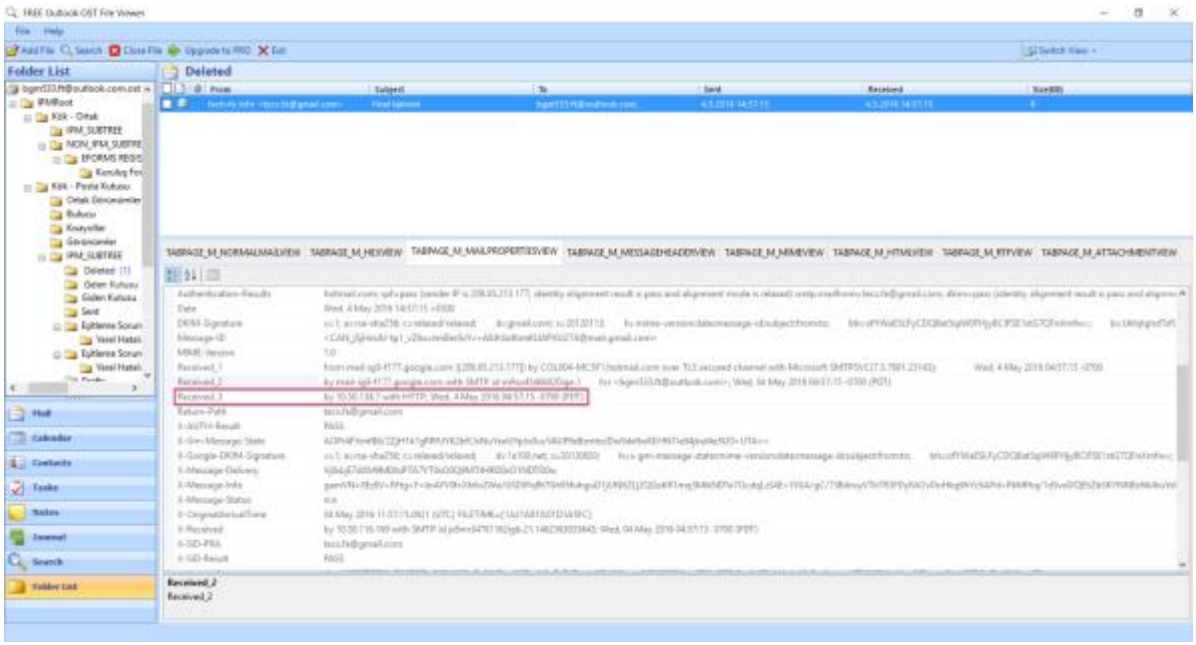




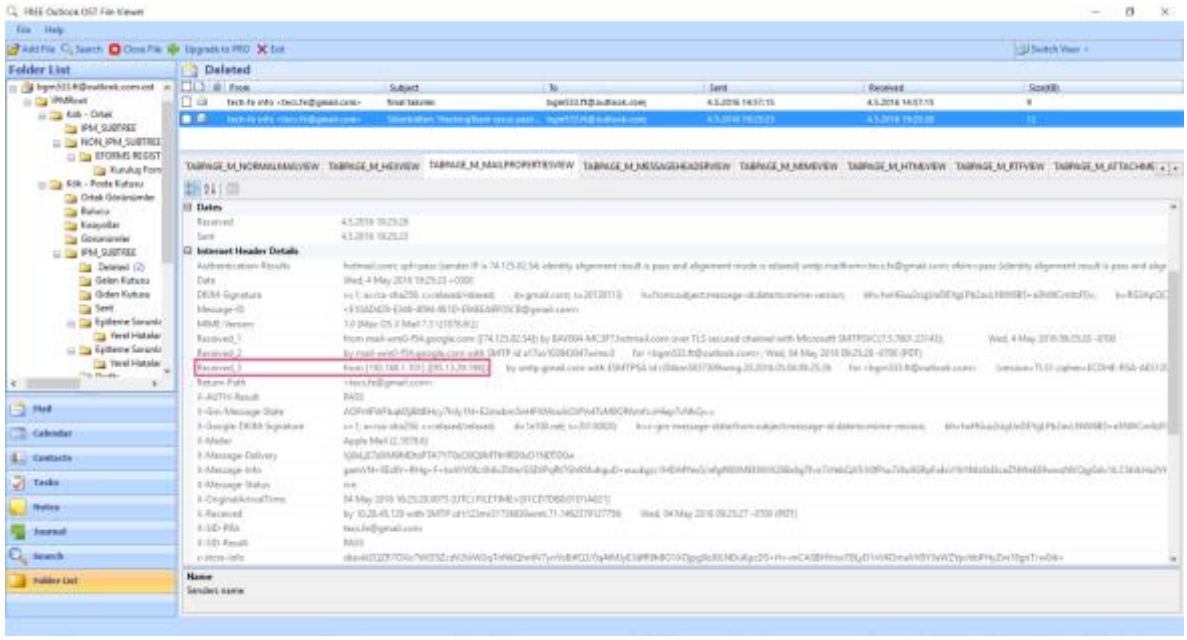


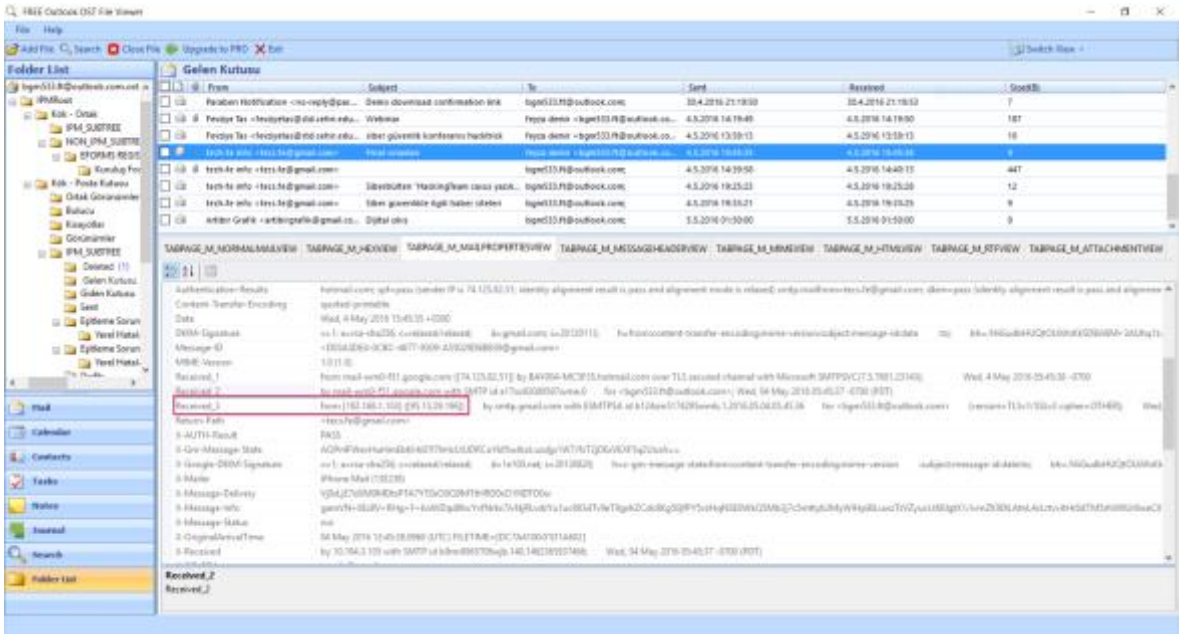
- **Gönderici cihazının IP adresini belirlemek**

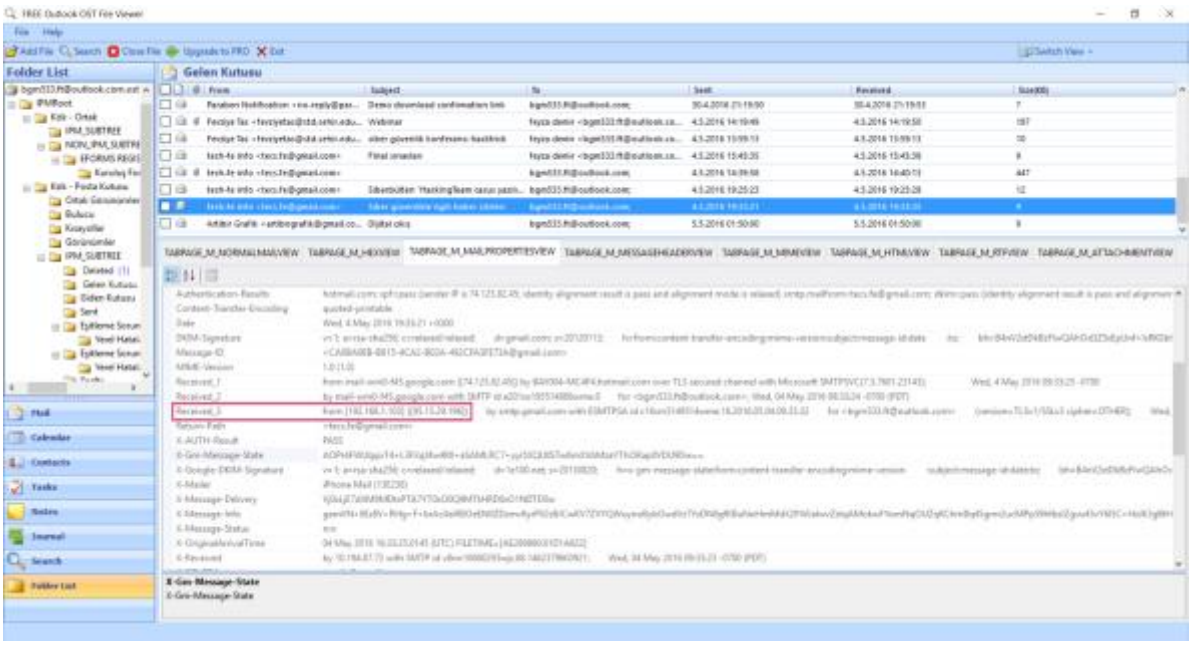
Gönderici cihazının IP adresi Received alanından belirlenebilmektedir. Received satırlarından en alttaki etiket(Received_3) göndericiye ait olan IP bilgilerini içermektedir.

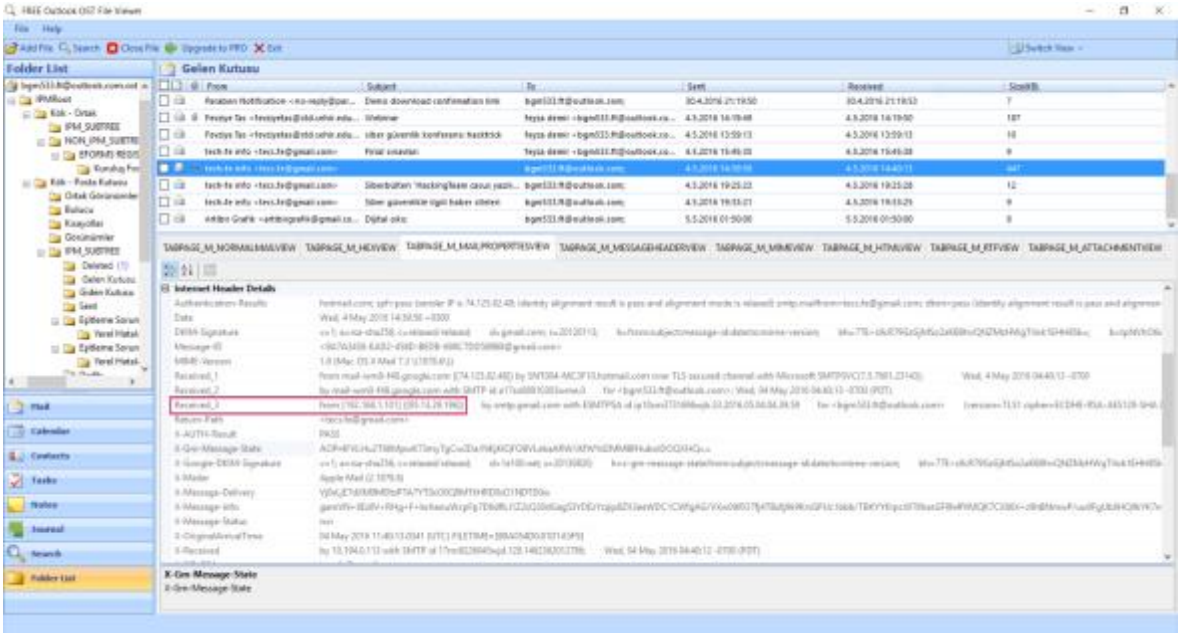


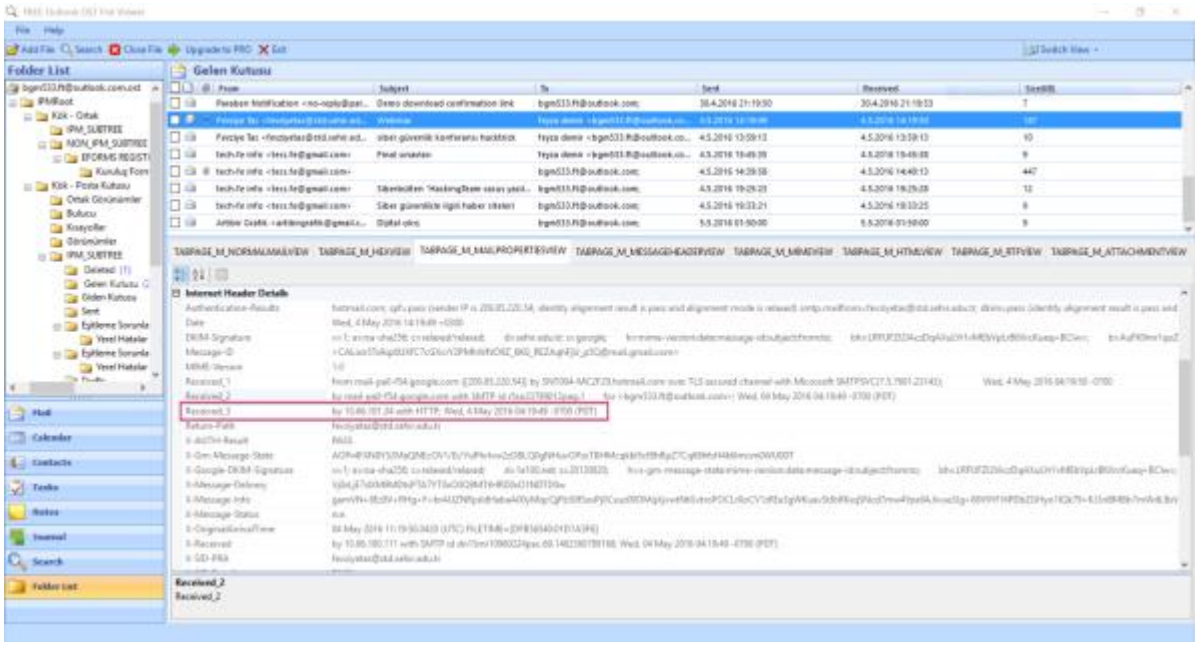
[OUTLOOK E-MAIL FORENSICS]





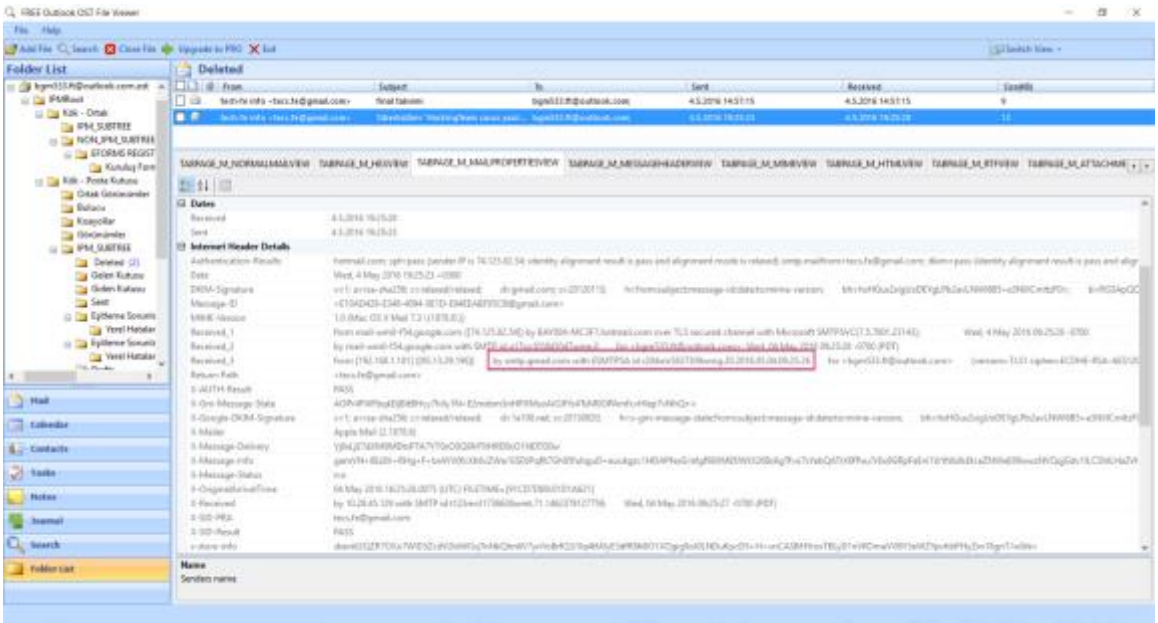


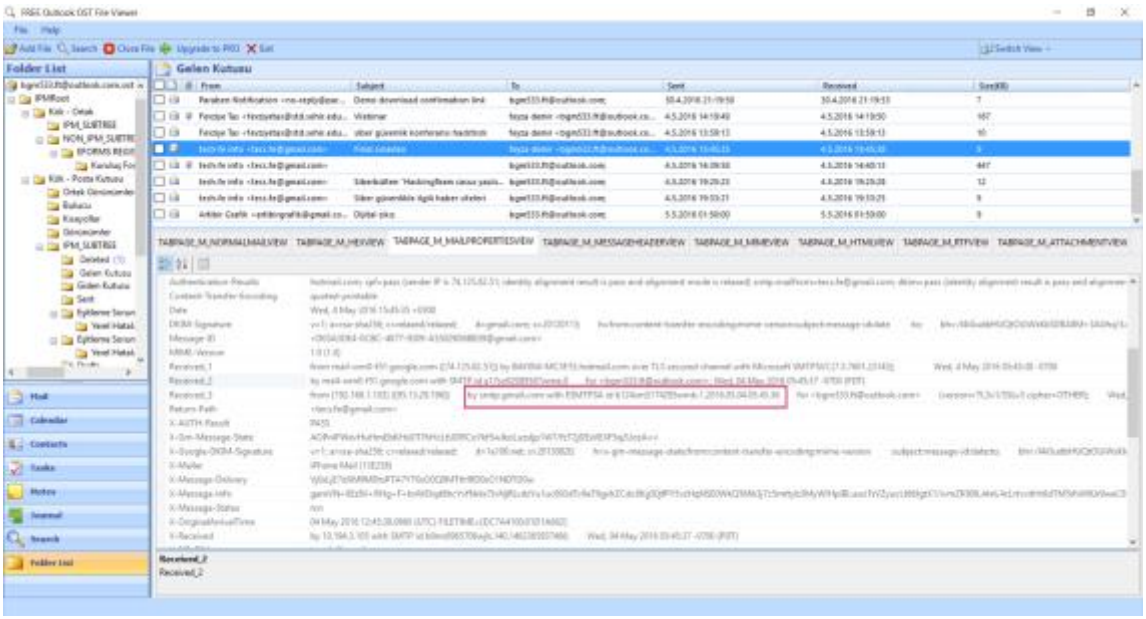




- **Göndericinin email sunucusunu belirlemek (Received etiketi)**

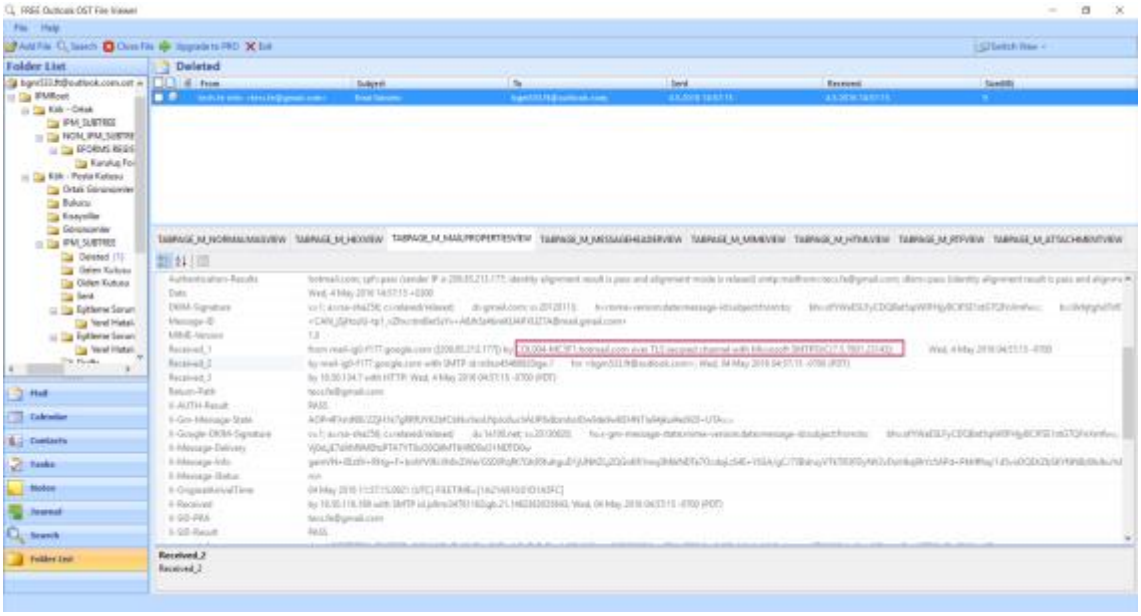
Received_3 etiketi kullanıcının email sunucusunun bilgilerini vermektedir.



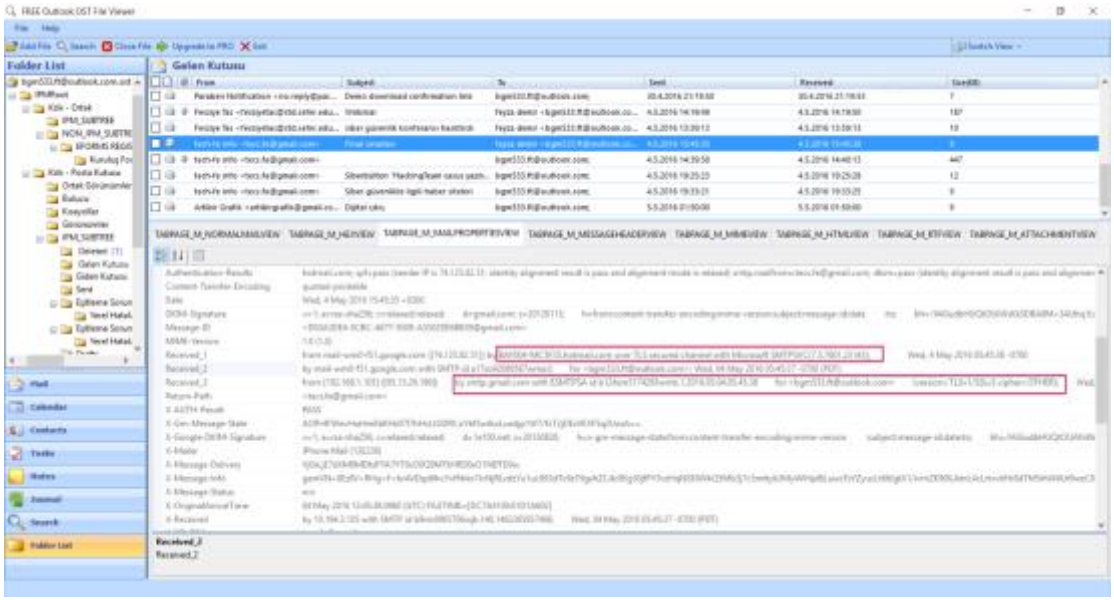


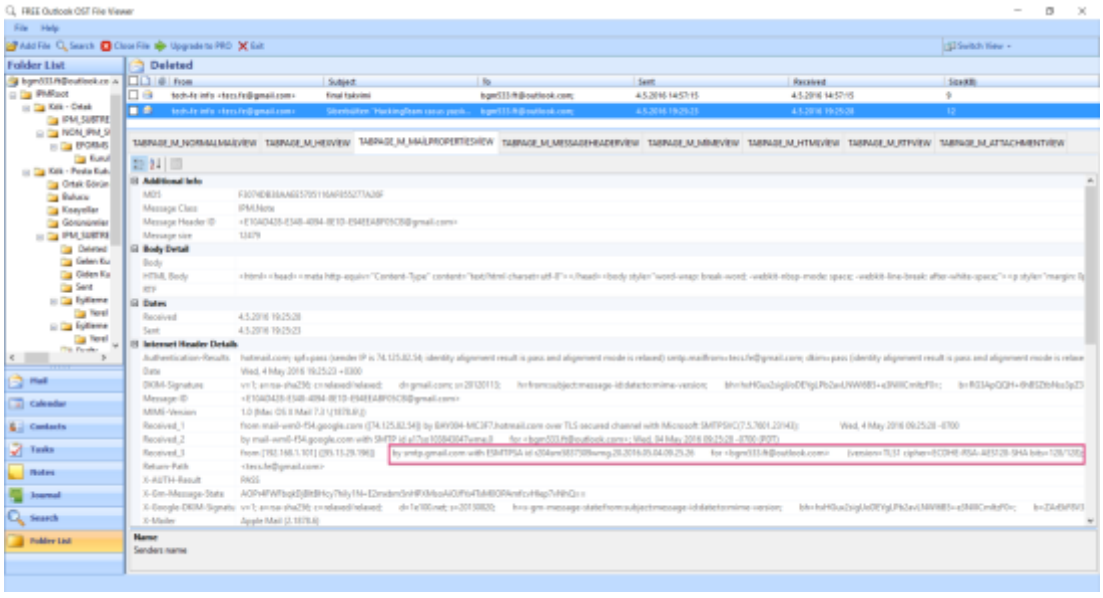
- **Mail sunucularının kullandığı yazılımları, protokolleri ve güvenlik fonksiyonlarını tespit etmek (Received etiketi)**

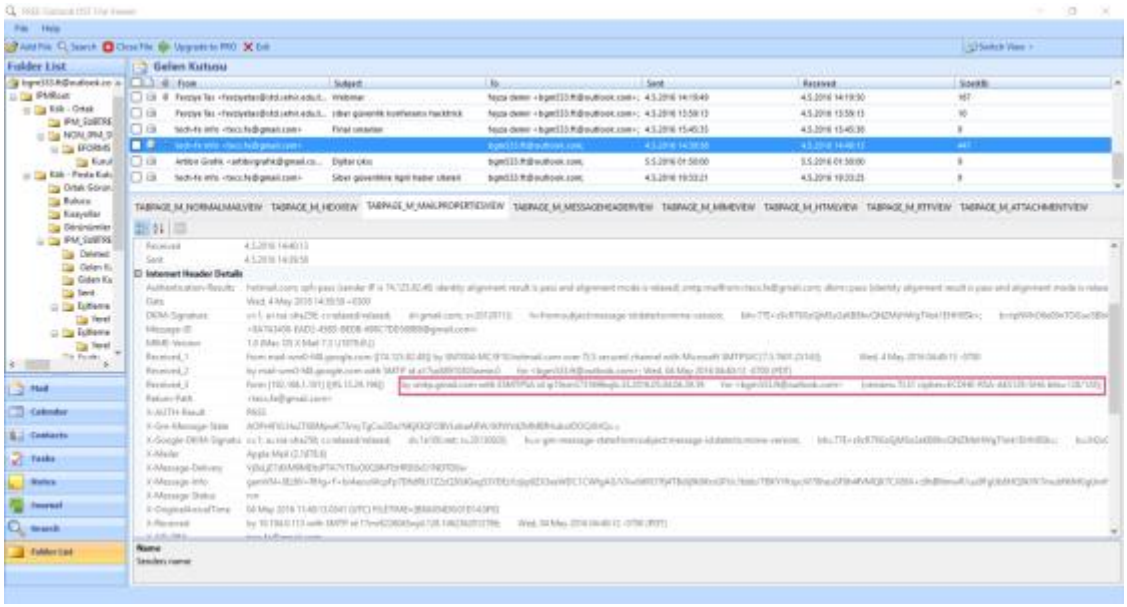
Sunuculara ait Received(Received_1 ve Received_2) etiketleri sunucuların kullandığı Simple Mail Transfer Protocol gibi email protokollerinin versiyonları, TLS/SSL kriptolama protokolleri ve SHA hash fonksiyonlarının versiyonları hakkında bilgiler verir.



[OUTLOOK E-MAIL FORENSICS]

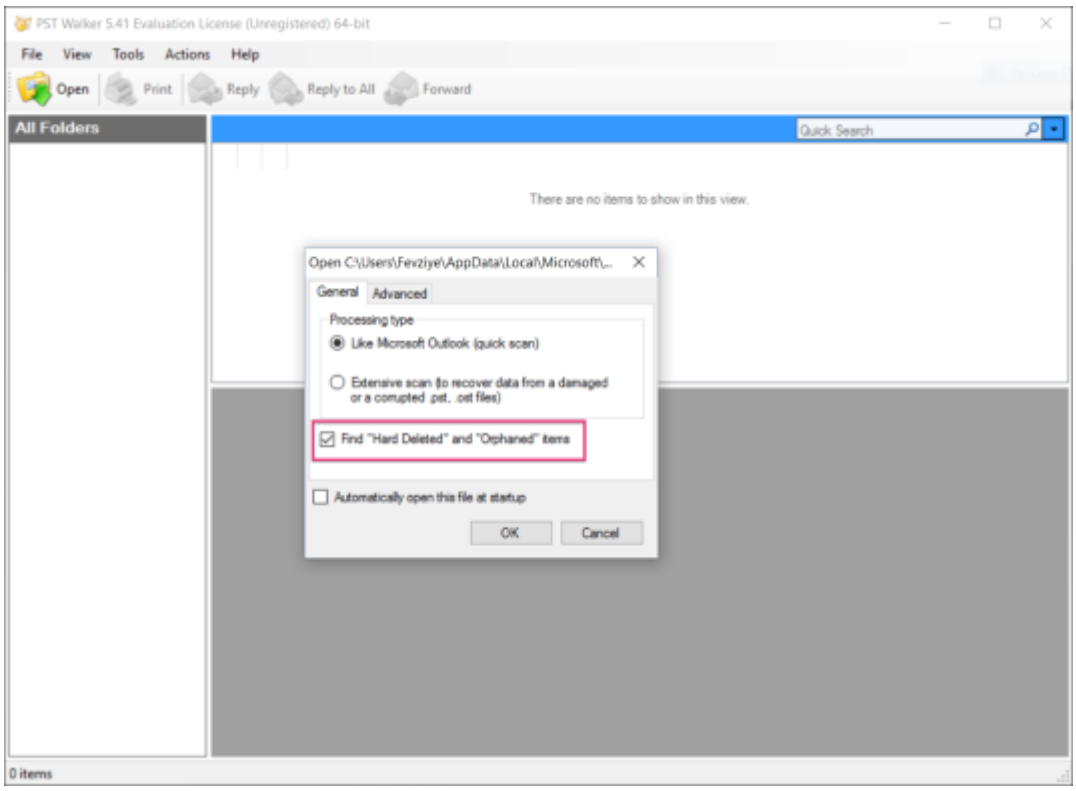


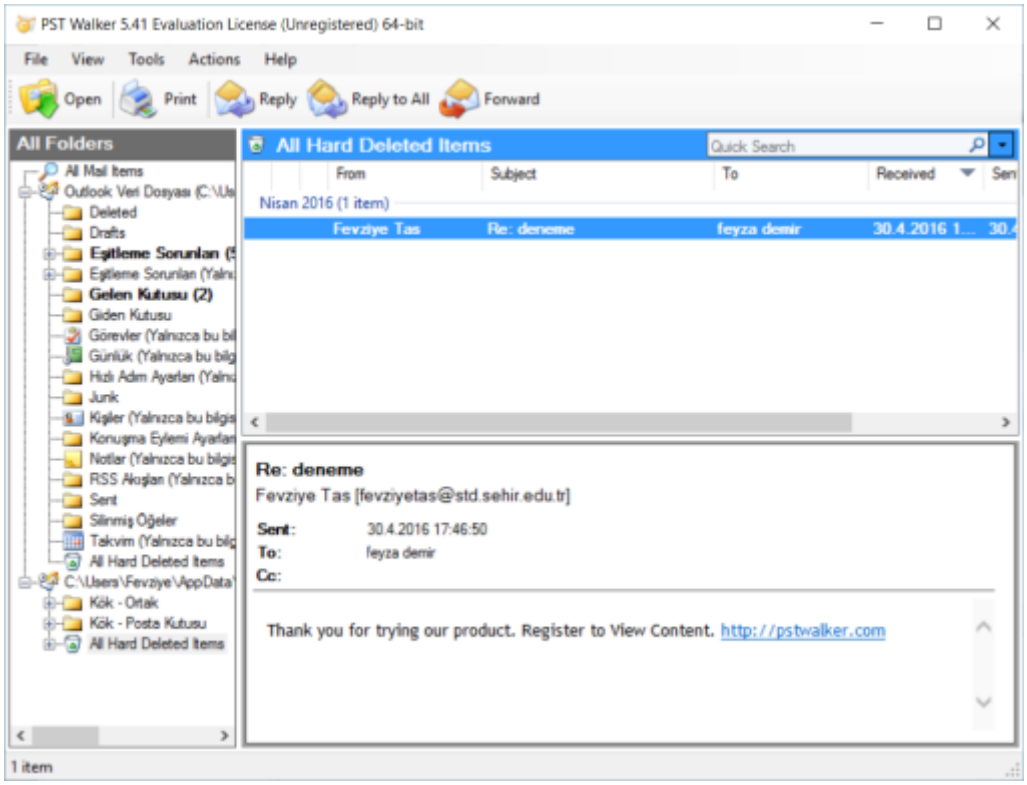




- **Silinmiş emailleri geri getirmek**

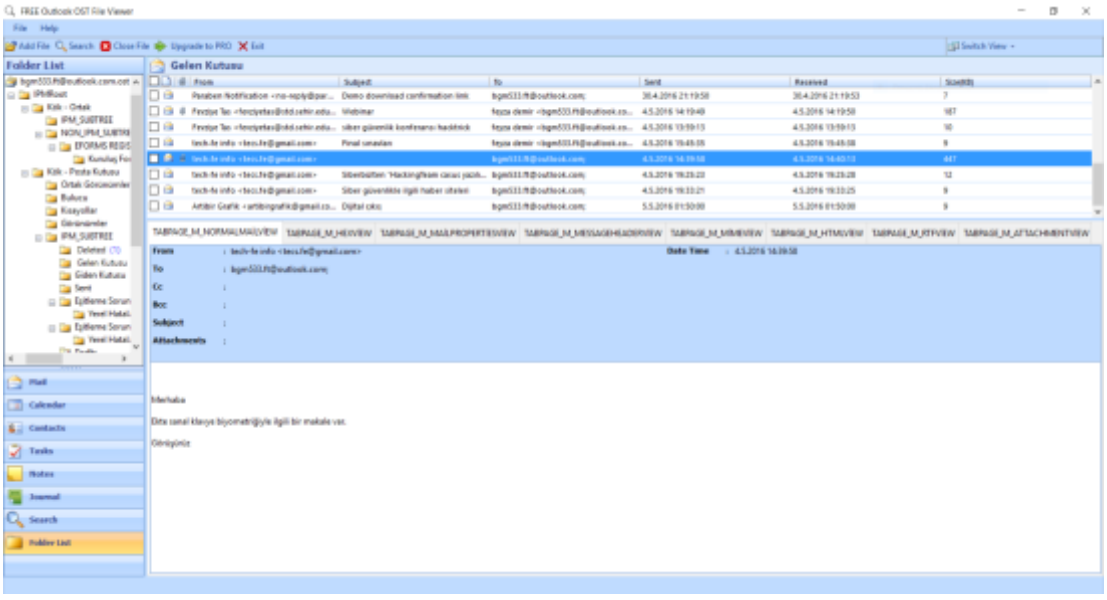
PST Walker gibi bazı email kurtarma programları *Deleted* dosyasından da kalıcı olarak silinen emailleri geri getirebilmektedir. Kalıcı olarak silinmiş ancak program tarafından kurtarılan emailler *All Hard Deleted Items* sekmesinde görüntülenebilmektedir. Bunun için .pst dosyası seçilirken *Find "Hard Deleted" and "Orphaned" items* alanının seçilmesi gerekmektedir.

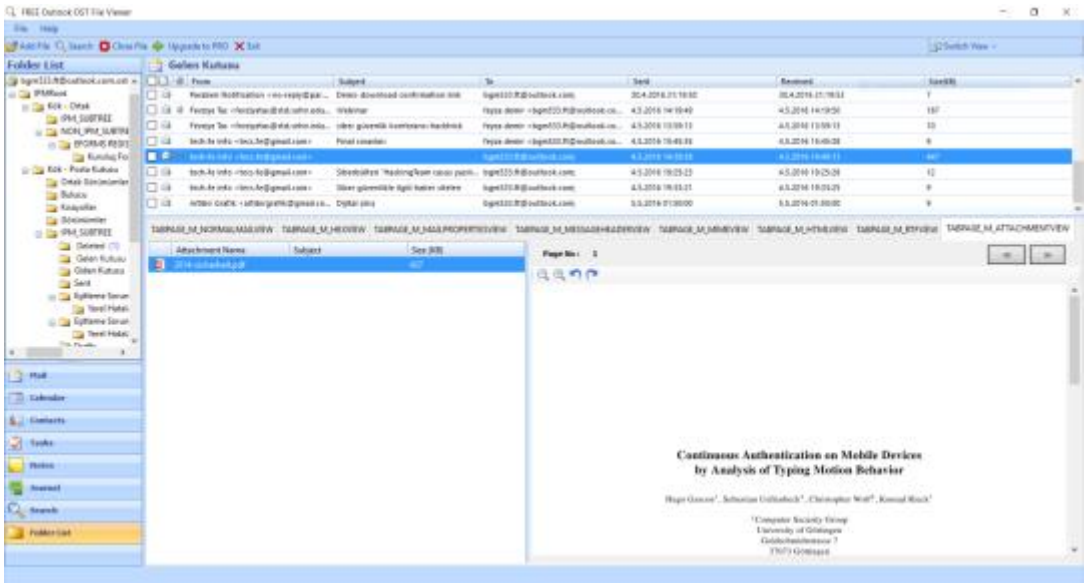




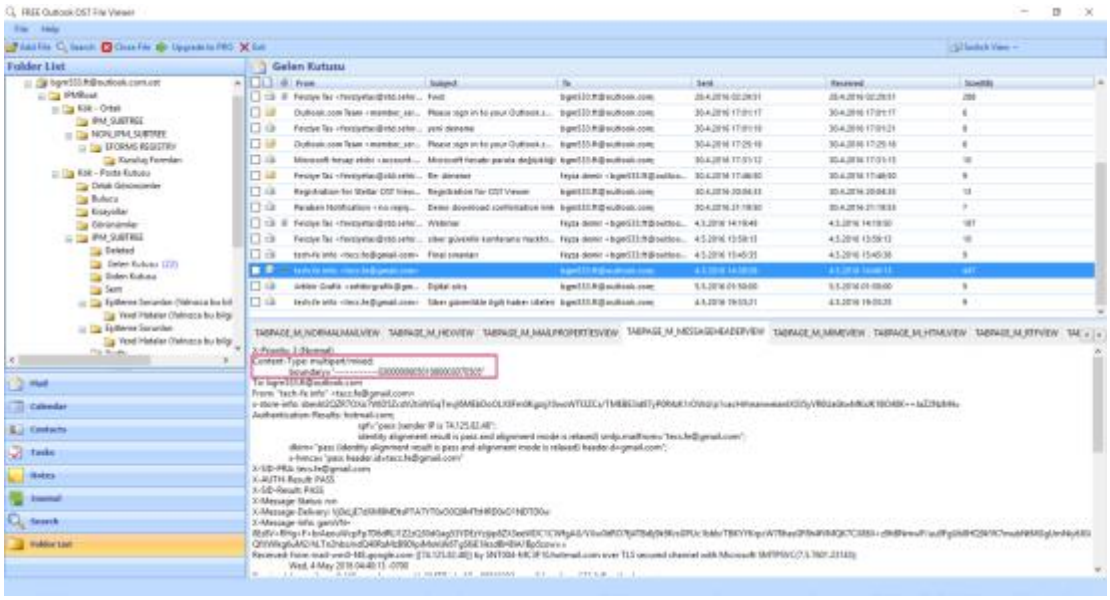
- **Bir emailin orijinal halini ve ilintili dosyalarını(attached files) görüntülemek**

Free Outlook OST File Viewer programında TABPAGE_M_NORMALMAILVIEW sekmesi emaillerin normal görünümüne ulaşmayı sağlarken, TABPAGE_M_ATTACHMENTVIEW ise eklenti dosyalarını görüntülemek için kullanılmaktadır.





Dosya ilintili maillerde eklenti barındırmayan maillerden farklı olarak Content-Type alanının değeri *text/plain* yerine *multipart/mixed* olarak değişmiştir.



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 kurul uşlarına 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.