DİJİTAL DELİLLERE İLK MÜDEHALE
İMAJ ALMA VE İNCELEME SÜREÇLERİ

YÜKSEK LİSANS TEZİ

İbrahim SARAYDERE

Danışman

Yrd. Doç. Dr. Barış GÖKÇE

İNTERNET VE BİLİŞİM TEKNOLOJİLERİ YÖNETİMİ

ANABİLİM DALI

Ocak, 2018

AFYON KOCATEPE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

DİJİTAL DELİLLERE İLK MÜDAHALE, İMAJ ALMA VE İNCELEME SÜREÇLERİ

İbrahim SARAYDERE

Danışman
Yrd. Doç. Dr. Barış GÖKÇE

İNTERNET VE BİLİŞİM TEKNOLOJİLERİ YÖNETİMİ ANABİLİM DALI

Ocak 2018

TEZ ONAY SAYFASI

İbrahim SARAYDERE tarafından hazırlanan "Dijital Delillere İlk Müdehale, İmaj Alma ve İnceleme Süreçleri" adlı tez çalışması lisansüstü eğitim ve öğretim yönetmeliğinin ilgili maddeleri uyarınca 24/01/2018 tarihinde aşağıdaki jüri tarafından **oy birliği** ile Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü **İnternet ve Bilişim Teknolojileri Anabilim Dalı'nda YÜKSEK LİSANS TEZİ olarak** kabul edilmiştir.

Danışman : Yrd. Doç. Dr. Barış GÖKÇE

İmza

Başkan : Yrd. Doç. Dr. Güray SONUGÜR
Afyon Kocatepe Üniversitesi, Teknoloji Fakültesi

Üye : Yrd. Doç. Dr. Barış GÖKÇE
Afyon Kocatepe Üniversitesi, Teknoloji Fakültesi

Üye : Yrd. Doç. Dr. Serkan CAŞKA

Manisa Celal Bayar Üniversitesi, Hasan Ferdi Turgutlu Teknoloji Fakültesi

Afyon Kocatepe Üniversitesi
Fen Bilimleri Enstitüsü Yönetim Kurulu'nun
...../...../..... tarih ve
……. sayılı kararıyla onaylanmıştır.

……
Prof. Dr. İbrahim EROL
Enstitü Müdürü

BİLİMSEL ETİK BİLDİRİM SAYFASI
Afyon Kocatepe Üniversitesi

Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- Görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- Başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- Atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- Kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- Ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

24.01.2018

İBRAHİM SARAYDERE

ÖZET

Yüksek Lisans Tezi

DİJİTAL DELİLLERE İLK MÜDAHALE, İMAJ ALMA VE İNCELEME SÜREÇLERİ

İbrahim SARAYDERE

Afyon Kocatepe Üniversitesi

Fen Bilimleri Enstitüsü

İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı

Danışman: Yrd. Doç. Dr. Barış GÖKÇE

Bu çalışmada, siber suç soruşturmalarının önemli bir kısmını oluşturan, adli bilişim incelemelerinin ilk bölümü olan dijital delillere ilk müdahale ve imaj almanın gerekliliği incelenmiştir. Dijital materyallerin bulunduğu alanda yapılan işlemlerde yapılan hatalar, delillerin gerçekliğine ve güvenilirliğine gölge düşürebileceği için bu aşamada yapılan hatalar tüm adli bilişim sürecini sekteye uğratabilmektedir. Meydana gelen ve işlenen suçlarda artık cep telefonu, bilgisayar sistemleri veya internet büyük ölçüde yer almaktadır. Bilişim suçunun aydınlatılmasında ve ortaya çıkarılmasında en önemli husus dijital delillerdir. Dijital materyallerin asılları üzerinde inceleme işleminin yapılması delil bütünlüğünü bozacağından ele geçirilen dijital materyallerin her zaman bir adli kopyası alınıp bu adli kopya üzerinde inceleme yapılması gerekmektedir. Dijital materyallerin inceleme aşamasından önceki aşama olan dijital materyalleri ilk müdahale ve imaj alma aşaması önemli bir aşamadır. Dijital Delillerde imaj alma yöntemleri kapalı sistemlerde ve açık sistemlerde imaj alma olarak 2 sınıfa ayrılır. Bu çalışmada siber suç soruşturmalarında delil elde etme yöntemlerinde kullanılan imaj almada kullanılan donanım ve yazılımlar incelenmiş kullanılan yazılımların performansları test edilmiştir. Ayrıca örnek bir senaryo üzerinden analiz yazımlarının delil bulmaz zamanları ve kullanım kolaylıkları da analiz edilmiştir.

2018, xiii + 123 sayfa

Anahtar Kelimeler: Adli Bilişim, Dijital Delillere İlk Müdahale, Adli İmaj, Mobil İnceleme, Adli Bilişim, Dijital Delillerde İnceleme

ABSTRACT

M.Sc. Thesis

INCIDENT RESPONSE TO DIGITAL EVIDENCE, ACQUISITION AND INVESTIGATION PROCESSES

İbrahim SARAYDERE

Afyon Kocatepe University

Graduate School of Natural and Applied Sciences

Department of Internet and Information Technology Management

Supervisor: Assist. Prof. Dr. Barış GÖKÇE

In this study, the necessity of incident response and image acquisition of Digital Evidence which is the first part of forensic investigation and which constitutes a significant part of cybercrime investigations, has been investigated. Errors made in the field where digital materials are located can shadow the authenticity and trustworthiness of the evidence, so errors made at this stage can cause the whole forensic process. Today, mobile phones, computer systems or internet are absolutely involved in crimes that committed. Digital evidence is the most important factor in the elucidation and disclosure of cybercrime. Since the examination of the originals of digital materials will destroy the integrity of the evidence, it is always necessary to take a forensic copy of the digital material that has been captured and examine it on this forensic copy. Digital Materials, the stage prior to the review phase of digital materials, is an important milestone in the initial intervention and image acquisition phase. The methods of image acquisition in Digital Evidence are divided into two classes as image acquisition from closed systems and image acquisition from open systems. In this study, it is informed about hardware and software used in taking image using in getting evidence in cybercrime investigation and the performances of the software that used are tested. Further more evidence finding time of the test software on an example scrip and ease of use are also analyzed.

2018, xiii + 123 pages

Keywords: Cybercrime, Forensic Computing, First Digital Intervention on Forensic Image, Forensic Image, Mobile Review, Forensic Computing, Digitally Inspected.

TEŞEKKÜR

Bu araştırmanın konusu, çalışmaların yönlendirilmesi, sonuçların değerlendirilmesi ve yazımı aşamasında yapmış olduğu büyük katkılarından dolayı tez danışmanım Sayın Yrd. Doç. Dr. Barış GÖKÇE, araştırma ve yazım süresince yardımlarını esirgemeyen aileme, arkadaşım Sibel Arslan ve Cihangir DOĞAN'a her konuda öneri ve eleştirileriyle yardımlarını gördüğüm hocalarıma ve arkadaşlarıma teşekkür ederim.

İbrahim SARAYDERE

AFYONKARAHİSAR, 2018

İÇİNDEKİLER DİZİNİ

Sayfa

KISALTMALAR DİZİNİ

Kısaltmalar	
BIOS	Temel Giriş Çıkış Sistemi (Basic Input Output System)
CD	Kompakt Disk (Compact Disc)
CMK	Ceza Muhakemeleri Kanunu
Cofee	Computer Online Forensic Evidence Extractor
DVD	Dijital Çok Yönlü Disk (Digital Versatile Disc)
DVR	Dijital Video Kaydedici (Digital Video Recorder)
FTK	Forensıc Toolkıt
GPRS	Genel a-Paket Radyo Servisi (General Packet Radio Service)
GPS	Global Konumlandırma Sistemi (Global Positioning System)
IMEI	Uluslararası Mobil Cihaz Tanımlayıcı (International Mobile Equipment Identifier)
IP	İnternet Protokol (İnternet Protocol)
MD5	Message-Digest 5
MMC	Multimedya Kart (Multimedia kart)
MP3	Mpeg Ses Katmanı III (MPEG-1 Audio Layer III)
PDA	Kişisel Asistan Data (Personal Digital Assistant)
RAM	Rasgele Erişim Belleği (Random Access Memory)
SAS	Seri Bağlantı Girişi (Serial Atached SCSI)
SATA	Seri Geliştirme Eki (Serial Advanced Technology Attachment)
SCSI	Küçük Bilgisayar Sistemi (Small Computer System Interface)
SD	Güvenli Dijital Bellek Kartı (Secure Digital Memory Card)
SHA1	Secure Hash Algorithm 1
SIM	Abone Kimlik Modülü (Subscriber Identity Module)
SMS	Kısa Mesaj Servisi (Short Message Service)
USB	Evrensel Seri Veriyolu (Universal Serial Bus)

ŞEKİLLER DİZİNİ

Sayfa

ÇİZELGELER DİZİNİ

Sayfa

1. GİRİŞ

Günümüzde teknolojinin hızlı bir şekilde gelişmesi sürekli olarak kendini yenilemesi, toplumun her kesiminin içinde yer alması bazı hukuki sorunları ortaya çıkarmıştır. Artık internet sayesinde insanlar uzaktan uzağa iletişim kurabilmekte ve mesafeleri yakınlaştırabilmektedir. İnsanlar artık internet üzerinden veya mobil cihazlarından bulundukları yerden mail atabiliyor, alışveriş yapabiliyor ve birçok ihtiyaçlarını halledebilmektedirler. İnternetin bu sağladığı kolaylıklar yanında birde bu teknolojiye paralel olarak meydana gelen suç tipleri mevcuttur. Ortaya çıkan bu suç tipleri insanlar tarafından bilgisayar, mobil cihaz vb. gibi cihazlar tarafından işlendiği için bu cihazların incelenebilmesi için de adli bilişim doğmuştur. Bu cihazların adli bilişim açısından incelenmeden önce yapılması gereken bir takım işlemler vardır. Bu işlemleri kısa olarak anlatmak gerekirse el koyma ve imaj alma aşamasıdır. Ele geçirilen bir dijital materyalin orijinal üzerinde inceleme yapabilmek orijinal olan dijital materyale zarar verebileceği, dijital materyalin delil bütünlüğü bozulacağı ve dijital materyalin içerisinde olan bilgilerde değişiklik yapabileceğinden her zaman dijital materyalin adli bir kopyanın (imajın) alınıp bu alınan adli kopya üzerinde çalışılması gerekmektedir.

Bilişim suçları ve adli bilişimin en önemli konularından biri dijital deliller ve dijital delillere ilk müdahale konusudur. Dijital delil bir suçun nasıl işlendiği, ne şekilde işlendiği, ne zaman işlendiği, bu suçlar işlenirken hangi programlar ve dokümanlar kullanıldığı, bilgisayarı kullanan şahısların kimlik bilgilerini kayıt eden veriler olarak tanımlanabilir.

Siber Suçlar kapsamanda bir suçun aydınlatılabilmesi ve yargı birimlerine iletilmesinde olağan delillerden daha çok elektronik delillere ihtiyaç bulunmaktadır. Dijital/elektronik delil (e-delil), bir dijital materyal üzerinde muhafaza edilen ve bu araçlar ile yürütülen soruşturma aşamasında gerekli olan delilerin bulunduğu araçlar olarak tanımlanabilir. Elektronik delil üzerinde saklanan veya bu araçlar aracılığıyla iletilen soruşturma açısından değeri olan bilgi ve veriler olarak tanımlanabilir. Adli bilişim safhası, olay yerine ilk müdahale işleminden başlayarak, dijital delillerin toplanması, toplanan bu dijital delillerin olay yerinden adli bilişim laboratuvarına sevk edilmesi, adli bilişim laboratuvarında bu dijital materyallerin incelenmesi ve bu inceleme sonunda düzenlenen

raporun adli makamlara sevk edilmesine kadar olan süre olarak özetlenebilir. Elde edilen dijital delillerin gücüne göre, bilişim suçlarını işleyen kişilere verilecek cezalar değişmektedir. Dijital delillerin elde edilmesi, adli kopyasının düzgün alınması, analizi ve incelemesi sürecinde bu tüm adımların doğru olarak atılmasına bağlıdır. Dijital deliller kolaylıkla değiştirebilmesi, yok edilebilmesi ve var gibi gösterilebilmesi adli bilişimin önemini göstermektedir.

Dijital deliller hassas ve bozulabilir yapıda olduğundan sürecin başındaki bir hata tüm süreci etkileyeceği gibi toplarken muhafaza ederken ve taşınırken özel önlemler almak gerekir.

Adli Bilişim açından imaj alma işlemi, Write Block cihazı ile Encese, Ftk İmager, X Ways Forensic programları ve TD1 diye tabir edilen cihaz ile alınmaktadır. Açık sistemlerde imaj alma Helix Imager programı ile adli imajı alınmakta olup cep telefonlarında ise UFED Cellebrite cihazı ve Mobiledit Forensic programı ile alınmaktadır. İlk müdahalecinin öncelikli amacı dijital delilleri muhafaza etmek, bu delilleri tüm depolanmış veri alanlarının kapsamlı adli kopyalarının (imaj) çıkarabilmektir. Dijital delillere doğru ve düzgün bir müdahalede bulunabilmek için düzgün bir hazırlık yapmak, yeterli ön bilgi toplamak, düzgün ve doğru bir şekilde belgelemek, delilleri doğru tanımlamak, uygun bir biçimde el koymak ve uygun biçimde paketlemek ve inceleneceği yere ulaştırmaktır.

1.1 Çalışmanın Önemi

Bilgisayar ile bilişim teknolojisinin gelişmesi insan hayatında yeni gelişmelere ve değişikliklere neden olmuştur.

İletişim teknolojilerinin hızla gelişmesi, insan hayatında önemli değişikliklere sebep olmuştur. Bu değişikliklerin başında ise insanların alışkanlıkları olmuştur. Artık gelişen teknoloji ile insanlar tabletlerinden, telefonlarından en basit olarak alışveriş yapabilmekte ve faturalarını ödeyebilmektedir. Bu değişim bütün suçlarda olduğu gibi bilişim suçlarında da yeni suç tiplerinin ve yeni suç işleniş biçimlerinin ortaya çıkmasına neden olmuştur.

Bu çalışmada adli bilişimin ilk aşaması olan dijital delillere nasıl müdahale edilmesi gerektiği, genellikle kolluk kuvvetlerinin kullandığı imaj alma (adli kopya) işleminin nasıl yapılması gerektiği ve adli bilişim ile ilgilenenlerin doğru yönlendirilmesi açısından yararlı bir çalışma olması planlanmıştır.

1.2 Çalışmanın Amacı

Kolluk kuvvetlerince yürütülmekte olan bilişim suçları soruşturmalarında bir dijital materyalin sağlıklı olarak adli bilişim uzmanın önüne gelinceye kadar olan aşama dijital delillere ilk müdahale ve imaj alma aşamasıdır. Bu bahsedilen alanlarda yapılan bir hata hem dijital materyal üzerinde oynama yapabilecek ve soruşturmanın güvenirliğini tehlikeye düşebilecektir. Bu çalışmada kolluk kuvvetleri siber suçlar ve adli bilişim ile ilgilenen personel tarafından tam bir soruşturma yürütülmesi için dijital delillere ilk müdahalenin ve imaj almanın nasıl yapılmasının gerektirdiğini, incelemelerde kullanılacak yazılımların özelliklerinin tanınmasını ve bu yazılımlarım delil ortaya çıkarmada performansının test edilmesi ve bir öneri sunulması amaçlanmıştır.

1.3 Çalışmanın Kapsamı

Bu çalışmada verilen bilgiler, yapılan yazılım uygulama örnekleri ve karşılaştırma örnekleri adli bilişim ve siber suçlarla mücadele eden kolluk kuvvetleri olmak üzere Hukuk ve Ceza Mahkemelerinde bilirkişilik yapmak isteyen kişileri kapsar. Adli bilişimde dijital delillere ilk müdahale ve imaj alma genellikle tüm bilişim suçlarında ve bilişim soruşturmalarında yer alacağından yapılan çalışmanın kapsamı daha geniş alanda kullanım alanını kapsamaktadır.

1.4 Bilişim Suçları, Adli Bilişim ve Adli Bilişimin Hukuksal Boyutu

Günümüzde bilgisayarın neredeyse kullanılmadığı bir alanın kalmaması, bilişim suçlarının ortaya çıkmasına ve etki sahasının inanılmaz şekilde artmasına sebep olmuştur (Karagülmez 2011). Bilişim suçları denildiği zaman bilgisayar ile ilgili olan tüm suçlar olarak algılatılmaktadır. Adli bilişim denildiği zaman ise suça konu

bilgisayar içerisinde suç araştırması olarak bilinmektedir. Adli bilişim alanı yeni bir alan olduğundan dolayı kanunlar da yeni düzenleme yapılması gerekmektedir.

1.4.1 Bilişim Nedir?

İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi olarak adlandırabilir (İnt.Kyn.1).

İnsanların teknik, ekonomik, siyasal ve toplumsal alanlardaki iletişiminde kullandığı bilginin, özellikle bilgisayar aracılığıyla düzenli ve akılcı biçimde işlenmesi, her türden düşünsel sürecin yapay olarak yeniden üretilmesi, bilginin bilgisayarlarda depolanması ve kullanıcıların erişimine açık bulundurulması bilimidir şeklinde tanımlanmıştır (Dülger 2013).

1.4.2 Bilişim Suçları Nedir?

Bilişim Suçları; Bilgisayar ve diğer dijital materyaller ve iletişim araçları ile işlenen zarar verici hareketler olarak tanımlanabilir.

Bilgisayarları da kapsayan, ancak sadece bilgisayarlarla kısıtlı olmayıp bu alandaki bütün cihaz ve araçlara karşı veya bunlar marifetiyle işlenen suçlar olarak da tanımlanabilmektedir (Ersoy 1994).

Bir bankayı soymak yerine internetten banka hesaplarına girmek (eğer iyi bir şifre kırıcıdan bahsediyorsak) elbette çok daha kolaydır. Sadece bu bile, neden insanların dijital ortamda yapılan işlemleri kırmayı dolayısıyla da bilişim suçu işlemeyi amaçladığını gösterebilir. Ancak günümüzde tanımlanan bilişim suçları bu kadarla kısıtlı değildir. Bunun dışında kişilerin izni olmadan haklarında bilgi edinme, telefonlarını dinleme, var olan bir sistemi herhangi bir amaçla bozma, farklı düşüncelere sahip olan devlet, kuruluş vs. web sitesini ele geçirip değiştirme veya yapılan çeşitli protestolar da bilişim suçu olarak sayılabilir (Şamlı 2010).

Genel anlamda suçun, bilişim sistemlerine karşı veya bilişim sistemleri ile işlenen suçları ifade eden bilişim suçları kavramı, en basit tabiriyle bilgisayar suçları olarak tanımlayabildiğimiz gibi; siber suçlar, dijital suçlar, internet suçları, bilişim suçları, ileri teknoloji suçları vs. tanımlamaları ile de karşılaşılmaktadır. Diğer ülkelerde yapılan tanımlarda ise; Bilgisayar Suçları (Computer Crimes), Siber Suçlar (Cyber Crimes), Bilgi Teknolojileri Suçları (Crimes of Information Technologies), Ağ Suçları (Crime of Networks) gibi tanımlamalara da rastlanmaktadır. Aslında tüm bunlar ile bu suçların bir kısmının tanımlanması yapılmaktadır. Ancak ülkemizde Bilişim Teknolojileri Suçları olarak geçen (Crimes of Information Technologies) bu suçların alanı açısından tanım olarak daha iyi uymaktadır (Çakır ve Sert 2013).

1.4.3 Adli Bilişim Nedir?

Bilgisayar ve dijital veri bulunduran cihazlarla ilgili adli bilimlerin bir dalıdır. Bilginin belirlenmesi, korunması, kurtarılması, analiz edilmesi ve sunulması amacıyla dijital cihazların adli çerçevede incelenmesidir.

Adli bilişim sürecinde, inceleme ve analiz aşaması; usulüne uygun şekilde alınan imajın adli bilişim inceleme yazılımları ile incelenmesi ve bahse konu suç ile ilgili elektronik verilerin tespiti ve analiz işlemleridir (Kılıç 2013).

Adli Bilişim, veri depolaması yapabilen ve elektronik olarak dijital delil sayılan materyaller üzerinde özel yazılım ve cihazlarla bir suçu ortaya çıkarmak ve yasaklanmış faaliyette bulunup bulunmadığını tespit etmek için kullanılan faaliyetlerin tümü olarak adlandırılabilir. Terim olarak İngilizce ‘Computer Forensic’ deyiminden çevrilerek uyarlanarak Türkçeye kazandırılmıştır. Adli Bilişimin temel amacı dijital veriler ile olay arasındaki bağlantıyı veya fiil ile işlenen veriler ve kullanıcı arasındaki bağlantıyı açığa çıkartmaktır.

Adli Bilişim (Computer Forensics – Bilgisayar Kriminalistiği) bilimi; suçun aydınlatılabilmesi için bilimsel metotlar kullanılarak, çeşitli varyasyonlardaki dijital medyalar üzerinde bulunan, suçla ilgili dijital delillerin bozulmadan ve zarar görmeden anlaşılabilir bir şekilde adalet önüne sunulmaya hazır hale getirilmesini sağlayan ve

başlı başına bilimsel teknik prensiplerin uygulandığı bir delil inceleme sürecinin bütünüdür (İnt.Kyn.2).

Mahkemeye intikal etmiş bir olayla ilgili olarak, olayda ele geçirilmiş ve el konulmuş olan bilişim cihazlarının incelenmesi isteğiyle ilgili olarak bu cihazlara yönelik kriminalistik prensiplerin uygulanmasıdır.

Adli bilişim alanında adli kopya ile ilgili uygulamalarda elektronik delillerin orijinali üzerinde tekrar adli kopya alma işlemleri yapılmakta ve sonucunda hesaplanan hash değeri ilk adli kopya alma işleminde hesaplanmış olan hash değeri ile karşılaştırılarak farklılık görüldüğünde elektronik aygıtın delil niteliği kalmadığı değerlendirilmektedir. Bunun yanında açık olan sistemlerden alınan adli kopyalarla ilgili olarak, RAM'lerden alınan adli kopyalarla ilgili olarak ve cep telefonlarından alınan adli kopyalarla ilgili olarak tekrar adli kopya alınması ve hash değerlerinin kıyaslanması gibi bir uygulama söz konusu değildir. Çünkü açık olan sistemler, RAM'ler ve cep telefonları üzerinde kayıtlı olan verilerin adli kopyaları alınırken sistem çalışmaya devam ettiği için, halen sistem tarafından zararsız ufak değişiklikler yapılmakta olduğu bilindiğinden; tekrar bir adli kopya alındığında aynı hash değeri elde edilemeyeceği bilindiğinden, böyle bir tehdit yoluna başvurulmamaktadır. Bu sistemlerden alınan ve elde olan ilk adli kopyalar üzerinden tüm inceleme ve değerlendirmeler yapılmakta, orijinal elektronik delil üzerinde tekrar hash hesaplatılması gibi bir işlem yapılmadan adli kopya delil olarak olayın aydınlatılmasında kullanılmaktadır (Özbek 2013).

Adli Bilişim (Computer Forensics – Bilgisayar Kriminalistiği) bilimi; suçun aydınlatılabilmesi için bilimsel metotlar kullanılarak çeşitli varyasyonlardaki dijital medyalar üzerinde bulunan, suçla ilgili dijital delillerin bozulmadan ve zarar görmeden anlaşılabilir bir şekilde adalet önüne sunulmaya hazır hale getirilmesini sağlayan ve başlı başına bilimsel teknik prensiplerin uygulandığı bir delil inceleme sürecinin bütünüdür (İnt.Kyn.3).

1.4.4 Neden Adli Bilişime İhtiyaç Vardır?

Teknolojininim gelişimine bağlı olarak el yazısı ve daktilo kullanımı terk edilmiş, tüm dokümanlar bilgisayar üzerinde oluşturulması ve saklanması doğal hale gelmiştir. Siber suç soruşturmalarında ele geçirilen dijital materyaller içerisinde gizlenmiş, silinmiş ve hasar görmüş vaziyette bulunan bilgilerin gün ışığına çıkarmada yardımcı olacaktır.

Adli bilişim dijital deliller üzerinde yapılan incelemeler olduğu için bilgisayar yolu ile bir suç işlenildiği zaman o suç işlenen bilgisayar üzerinde yapılacak olan incelemenin adı adli bilişim incelemesidir. Artık günümüzde teknoloji çok hızla ilerlediği için Adli Bilişim alanında kendisini yenilemesi kaçınılmaz olmuştur.

Bir adli bilişim uzmanı incelemeler esnasında daha önce hiç görmediği bir cihaz ve bu cihazda kendine özgü bir dil ve konfigürasyona sahip bir yazılım ile karşılaşabilir. Bu nedenle bilişim uzmanları farklı işletim sistemi mimarilerinden ve bileşenlerinden haberdar olmalı, farklı yazılım ve donanımlar ile işletim sistemlerini kullanabilmelidir. Kullanılan yazılımların sınırları ve becerileri çok iyi bilinmeli ayrıca sadece tek bir yazılım veya donanıma bağlı kalınmamalıdır. Farklı yazılımlar kullanılarak farklı sonuçlara ulaşılabileceğinden hangi durumda hangi yazılımın kullanılması gerektiği bilgisi de çok önemlidir (Şirikçi ve Cantürk 2012).

1.4.5 Adli Bilişim Türleri

Adli bilişim türleri aşağıda sunulmuştur. Bunlar;

1. Bilgisayar Adli Bilimi (Computer Forensics),
2. Cep Telefonu Adli Bilimi (Mobile Phone Forensics veya GSM Forensics),
3. Ses ve Görüntü Verileri Adli Bilimi (Audio and Video Forensics),
4. Windows İşletim Sistemi Adli Bilimi (Windows Forensics),
5. Linux İşletim Sistemi Adli Bilimi (Linux Forensics),
6. Bilgisayar Ağları Adli Bilimi (Network Forensics),
7. İnternet Adli Bilimi (Internet Forensics),
8. Flash Bellek Adli Bilimi (Flash Memory Forensics) olarak 8 bölüme ayırabiliriz.

Adli Bilişim türlerinin içerisinden en fazla kullanılan alan Bilgisayar Adli Bilimi Adli işlemlerin hemen hepsinde yapılan inceleme çoğu kez şüphelinin bilgisayarında yapılmakta ve istatistiksel olarak bakıldığında, bu incelemelerin hatırı sayılır bir kısmı suç fiiline ilişkin delillerin tespitiyle sonuçlanmaktadır (Daniel 2011).

1.4.6 Adli Bilişim Aşamaları

Adli bilişim aşamaları aşağıda sunulmuştur. Bunlar;

1. İlk Müdahale (Delil Tespit Etme),
2. Toplama ve Muhafaza Etme,
3. Delil Çıkartma,
4. Delil İnceleme,
5. Raporlama aşamalarından meydana gelmektedir.

Yukarıda Belirttiğimiz süreci kısaca açıklayacak olursak, İlk müdahale aşaması arama işlemine giden personelin olay yerinde dijital delil araması, "Delil Toplama ve Muhafaza Etme" aşaması arama sırasında olay yerinde bulunan dijital delilleri toplama ve bu delilleri muhafaza altına alarak adli bilişim laboratuvarına götürünceye kadar olan aşama, "Delil Çıkartma" aşaması muhafaza altına alınan ve adli bilişim laboratuvarına teslim edilen dijital materyaller üzerinde bulunan şifreli ve gizli bilgilerin dışarıya çıkartılması, Delil İnceleme aşaması elde edilen bilgilerin toplanarak bir bütün haline getirilmesi, "Raporlama" ise yukarıda belirtilen olaylar doğrultusunda elde edilen sonuçların metin haline getirilmesidir.

1.4.7 Adli Bilişimin Hukuksal Boyutları

Olay yerinden elde edilen bir nesnenin delil olarak kabul edilebilmesi için bütünlüğünün korunmuş olması gerekmektedir. CMK Md. 217/2 fıkrasında "yüklenen suç, hukuka uygun elde edilmiş her türlü delille ispat edilir" hükmü ile hukuka uygun elde edilen her türlü delilin suçu aydınlatmada kullanılabileceği vurgulanarak, kabul edilme şartı hukuka uygun elde edilmesine bağlanmıştır. Yine CMK 206. maddesi, kanuna aykırı olarak elde edilen delillerin ret edileceği hükmünü içerir. Elektronik delilin geçerli sayılabilmesi için kanuna uygun elde edilmiş olması gerekmektedir(Çatalkaya 2015).

Siber suçlarda yürütülen adli bilişim soruşturmaları ile ilgili Ceza Muhakemesi Kanunu'nun 134 Maddesi, Adli ve Arama Yönetmeliğinin 17. Maddesi Maddeleri ve Suç Eşyası Yönetmeliğinin 9. Maddesinde yer almaktadır.

1.4.7.1 Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El Koyma

Adli Bilişimi ilgilendiren kanunlar aşağıda belirtilmiş ve açıklanmıştır.

Bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma maddeleri CMK Madde 134, Adli ve Önleme Aramaları Yönetmeliği Madde 17 ve Suç Eşyası Yönetmeliği 9. Madde aşağıda sunulmuştur:

(1) Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.

(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, el konulan cihazlar gecikme olmaksızın iade edilir.

(3) Bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır

(4) İstemesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır

(5) Bilgisayar veya bilgisayar kütüklerine el koymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır.

Adli ve Önleme Aramaları Yönetmeliği Madde 17

Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması hâlinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı

bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.

Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması hâlinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için bu araç ve gereçlere el konulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması hâlinde, el konulan cihazlar gecikme olmaksızın iade edilir.

Bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır.

İstemesi hâlinde, bu yedekten elektronik ortamda bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

Bilgisayar veya bilgisayar kütüklerine el koymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan verilerin mahiyeti hakkında tutanak tanzim edilir ve ilgililer tarafından imza altına alınır. Bu tutanağın bir sureti de ilgiliye verilir.

Suç Eşyası Yönetmeliği Madde 9

Mahkeme ve diğer resmî mercilerce incelenmek üzere istenilen suç eşyasının teslimi, emanet bürosuna iadesi, başka yere gönderilmesi işlemleri:
MADDE 9 – (1) Emanet memuru, mahkeme ve diğer resmî daireler tarafından incelenmek üzere UYAP üzerinden veya yazılı olarak istenilen suç eşyasını, üzerindeki etiketlerde yazılı bilgiyi kapsayan bir yazı ile isteyen makama, Cumhuriyet savcısının onayıyla zimmet kaydına görevlinin imzasını almak suretiyle teslim eder ve teslim işlemini suç eşyası kaydına derhâl kaydeder. Mahkemelerin ve Cumhuriyet

başsavcılıklarının isteklerini UYAP üzerinden güvenli elektronik imzalı olarak yapmaları zorunludur.

(2) Zorunluluk bulunmadıkça eşyanın mührü sökülmez. Ancak inceleme sırasında mühür bozulur veya sökülür ise eşya yeniden usulüne uygun olarak ambalajlanıp mühürlenir, bu durumda en az iki nüsha tutanak tutulması zorunlu olup incelenen eşya değişikliğe uğrar ise iade tutanağında bu husus belirtilir. Söz konusu tutanaklarla birlikte eşya emanet bürosuna gönderilir. Emanet memuru, eşyada meydana gelen değişikliği esas kaydının düşünceler sütununa işler.

(3) Emanet memuru, teslim alınmaya engel bir durumu yoksa iade edilen suç eşyasını kabul ederek derhâl suç eşyası esas kaydına işleyip ilgili deposuna yerleştirir. Mühürlü, etiketli, emanet makbuzu olmayan veya açma-kapama-iade tutanağı bulunmayan suç eşyası kabul edilmez. Gönderen makamın tespit edilen eksikliği gidermesinden sonra tekrar emanet bürosuna iade etmesi zorunludur.

(4) İade edilmeyen suç eşyasının iade edilmeme sebebi, ilgili merciden üçer aylık fasılalarla sorulur.

(5) Yetkisizlik, görevsizlik, kamu davasının açılması, dava nakli veya diğer kararlar üzerine görevli mahkeme veya Cumhuriyet başsavcılığı tarafından emanette bulunan eşyasının istenilmesi hâlinde suç eşyası evrakın bulunduğu yere gönderilmek üzere Cumhuriyet başsavcılığına tevdi olunur. Bu hâlde de suç eşyasının sayı veya ebat olarak fazlalığı veyahut da niteliği gereği nakli büyük maliyetler gerektirdiği ya da taşınması sırasında da suç eşyasının zarar görmesi muhakkak ise gönderilmeyerek ilk bulunduğu yerde muhafaza edilir.

1.4.8 Dijital Delilin Problemleri

1-)Dijital Delillerin Bütünlüğü (The Integrity of Digital Evidence): Dijital veriler üzerinde çok kolay bir şekilde değiştirme, silme ve yenisini oluşturma gibi işlemlerin yapılabilmesi bu delillerin bütünlüğünü sağlamayı çok zorlaştırmaktadır.

2-)Dijital Delillerin Doğrulanması (The Authentication of Digital Evidence): Bir kişiyi dijital delillerle birlikte yakaladıktan sonra mahkeme sürecinde o verilerin gerçekten o kişiye ait olduğunun ispatı gerekmektedir. Fakat delil olarak ele geçirilen verilerin aynısı her hangi bir kişi tarafından da oluşturulabilir. Hatta sanık bu verilerin daha sonra, polis tarafından bile oluşturulduğunu iddia edebilir.

3-) Dijital Delillerin İnkar Edilememesi (The Nonrepudiation of Digital Evidence): Dijital delillendirme işlemindeki dijital delilin sahibi, onu ele geçiren şahıslar (Ör: Polis), delilin alındığı medya, delilin ele geçirildiği zaman, delilin içeriği gibi bütün unsurların daha sonradan inkar edilememesi gerekmektedir.

4-) Dijital Delillerin Doğruluğu (The Accuracy of Digital Evidence): Dijital delillerin ele geçirilmesi esnasında kullanılan teknikler ve kullanılan bilgilerin (Örneğin delilin ele geçirilme zamanı) doğruluğunun ispatı gerekir.

5-) Dijital Delillerin Daha Sonradan Ele Alınabilirliği (The Accountability of Digital Evidence):Dijital deliller oluşturulduktan sonra bu delilleri üçüncü bir şahıs inceleyebilmelidir (Hosmer 2002).

1.4.9 Dijital Delillerin Hukuki Olarak Sayılabilmesi İçin Gereken Sebepler

Siber Suç soruşturmalarında bir soruşturmanın tam anlamıyla doğru ve kabul edilebilir sayılması için IACIS tarafından belli bir standartlar belirlenmiştir.

1-) Orijinal deliller ilk bulundukları durum ve şartlara benzer şartlarda korunmalıdır.

2-) Orijinal delillerin bütünlüğünü bozmamak için mümkünse bire bir kopyası alınmalıdır.

3-) Kopyanın üzerine alınacağı medya "Adli Tıp yönünden steril – Forensically sterile" olmalıdır. Yani üzerinde daha önceden herhangi bir data bulunmamalıdır ve virüs ve diğer zararlı kodlara karşı kesinlikle temiz olmalıdır.

4-) Deliller mutlak suretle etiketlenmeli, korunmalı ve belgelendirilmelidir.

5-) Adli inceleme esnasındaki bütün basamaklar ve yapılan işlemler yazılı hale getirilmelidir (IACIS 2004).

2. LİTERATÜR BİLGİLERİ

2.1 Dijital Delil Nedir?

Günümüz suç dünyasında artık insan öldürme dahil olmak üzere her suçun bilişim araçlarıyla işlenebilmesi söz konusu olduğundan, ceza muhakemesi hukukunda da kağıt delillerin yerini, başta bilgisayarlar olmak üzere bilişim sistemlerinin içinde yer alan dijital olarak adlandırılan deliller almıştır (Özen 2015).

Dijital/elektronik delil (e-delil), bir elektronik araç üzerinde saklanan veya bu araçlar aracılığıyla iletilen soruşturma açısından değeri olan bilgi ve verilerdir.

2.2 Dijital Delilin Avantajları Nedir?

Dijital deliller sabit ve hassas yapıda olduğu için hem avantajları hem de dezavantajları vardır. Dijital delillerin üzerinde yapılan oynama değişme veya zarar verilip verilmediği adli bilişim programları ile anlaşılabilmektedir. Artık adli bilişim programları sayesinde bir verinin bilgisayarda ne zaman kayıt edildiği ne zaman silindiği anlaşılabilmektedir. Bu durum delillerin tespiti açısında büyük oranda avantaj sağlamaktadır. Ancak dezavantajları ise dijital deliller çok hassas olduğu için en ufak bir yazılımsal, donanımsal ve fiziksel olumsuzluklarda bile zarar görebilir veya dijital delilin bütünlüğü bozulabilir.

2.3 Dijital Delil Olarak Elektronik Aygıtlardan Elde Edilebilecek Ve Delil Oluşturabilecek Bulgular

Dijital delil olarak elektronik aygıtlardan elde edilebilecek ve delil oluşturabilecek bulgular aşağıda gösterilmiştir.

1. Video görüntüleri,
2. Fotoğraflar,
3. Ses dosyaları,
4. Video görüntüleri,
5. Yazı dosyaları (word, excell, open office vb. dosyaları),
6. Çeşitli bilgisayar programları ve bunların ürettiği dosyalar,

7. İletişim kayıtları (SMS, MSN Messenger, GTalk vb. kayıtları),
8. Gizli ve şifreli dosyalar / klasörler,
9. Dosyaların oluşturulma, değiştirilme ve erişim tarih kayıtları,
10. Son girilen ve sık kullanılan internet siteleri,
11. İnternet ortamından indirilen dosyalar,
    a. Sunucu (Server) işlem kayıtları (log kayıtları),
    b. İnternet trafik kayıtları (Gelen – Giden IP),
    c. Ve bu türden olup, silinmiş dosya/klasörler.

Günlük hayatımızda kullandığımız birçok dijital ürün aslında bilmediğimiz bir dijital delil olabilir. Bu sebeple dijital delil olarak sunulan dijital delillerin tanımlanması son derece önemlidir. Dijital deliler aşağıda açıklanmıştır.

2.4 Dijital Deliller

Günlük hayatımızda kullandığımız birçok dijital ürün aslında bilmediğimiz bir dijital delil olabilir. Bu sebeple dijital delil olarak sunulan dijital delillerin tanımlanması son derece önemlidir. Dijital deliler aşağıda açıklanmıştır.

2.4.1 Bilgisayar

Dizüstü bilgisayar, taşınabilir olarak klavye ve ekrandan oluşan bir bilgisayar türüdür. Masa Üstü bilgisayarların tüm özelliklerini barındırır. Masaüstü bilgisayar; sabit kasa, ekran, fare ve klavyeden oluşan bilgisayar türüdür.

2.4.2 Sabit Diskler

Manyetik kayıt ortamlarıdır. Ses, görüntü, programlar, veri tabanları gibi büyük miktarlarda bilgi, gerektiğinde kullanılmak üzere sabit disklerde saklanır. Bilgisayarlarda yardımcı ve kalıcı bellek olarak kullanılırlar. Bir bilgisayar programı işletilmeye başladığında, programın çalışması için gerekli olan bilgiler sabit diskten okunarak çok daha hızlı olan RAM belleğe aktarılır. Gereksinim duyulan kısım RAM'a sığmayacak kadar büyükse, bilgisayar sabit diskin bir bölümünü Ram bellek gibi

kullanır. Sabit disk bilgisayarın kayıt ortamı olduğu için dijital delil olarak gösterilmiştir.

2.4.3 Harici Diskler

Manyetik kayıt ortamları olup USB 1.1, 2.0 veya 3.0 veri aktarım hızı ile bilgisayarlara bağlanabilen taşınabilir veri depolama aygıtlarıdır.

2.4.4 CD/DVD/HD DVD/Blu-Ray Medyalar

CD, 650 ile 900 MB kayıt kapasitesine sahip, veri depolama aygıtlarıdır. 20 derecelik sabit bir oda sıcaklığında ve karanlık bir odada depolanması gerekir. Ömrü 10 ile 50 yıl arasında değişmektedir. İçerisine her türlü bilgi ve belge yüklenebildiği için dijital delil olarak gösterilmiştir.

DVD, plastik kaplı polikarbonattan, iki diskin birleşmesinden ve çok daha ince yansıtıcı bir alüminyum ya da altın tabakadan oluşur. 4.7 GB kayıt kapasitesine sahiptir.
Disk ortamı şunlar olabilir:

- DVD-ROM: salt okunur, kalıpla üretilmiş,
- DVD-R: bir kere yazılır,
- DVD-RW: tekrar yazılabilir,
- DVD-RAM: rastgele erişimle tekrar yazılabilir. DVD+R DL: iki katmanlı bir kez yazılır.

Diskin bir ya da iki tarafı olabilir ve her taraf için bir ya da iki katmanı olabilir; taraf ve katmanlar diskin boyutunu belirler:

- DVD-5: tek taraflı, tek katman 4.7 GB (4.38 GB),
- DVD-9: tek taraflı, çift katman, 8.5 GB (7.92 GB),
- DVD-10: çift taraflı, tek katman iki yüzünde 9.4 GB (8.75 GB),
- DVD-14: çift taraflı, çift katman tek yüzünde, diğerinde tek 13.3 GB (12.3 GB),
- DVD-18: çift taraflı, çift katman iki yüzünde 17.1 GB (15.9 GB).

2.4.5 USB Flash Diskler

USB1.1 ve 2.0 ve 3.0 ara yüzü ile entegre edilmiş, kapasiteleri 256 GB'a kadar ulaşabilen, küçük, hafif, çalışma esnasında sökülüp takılabilir NAND tipinde veri depolama aygıtlarıdır. Flash sürücüler sadece bilgisayarın USB girişine takılı olduğu sürece çalışır durumdadırlar. Harici güç kaynağı veya pil gücüne ihtiyaç duymazlar ve her türlü bilgi saklanabilir. Optik sürücülerden daha hızlı ve kullanımı daha kolaydır. İçerisine her türlü bilgi ve belge yüklenebildiği için dijital delil olarak gösterilmiştir.

Blu-Ray: Sony tarafından 2003 yılında geliştirilmiştir. Yeni nesil yüksek çözünürlüklü (HD) videoların tek bir diskte saklanabilmesi, çok büyük miktarda veri depolama aygıtlarıdır. Tek tabakalı bir Blu-ray disk 25 GB'lık, Çift tabakalı biçimi 50 GB veri depolama kapasitesine sahiptir.

2.4.6 Hafıza SD Kartları

Günlük hayatta kullanılan ve hafıza (SD) kartı örnekleri aşağıda verilmiştir. İçerisine her türlü bilgi ve belge yüklenebildiği için dijital delil olarak gösterilmiştir.

Compact Flash

Flash bellek kart çeşididir. Bilgisayar, dijital fotoğraf makineleri ve Pda'larda kullanılmaktadır. Compact Flash teknolojisi uzun zamandır sahip olduğu pazar liderliğini SD kartlara bırakmıştır. Compact Flash kartların yazma hızı SD kartlara göre daha fazladır.

Mmc Kart

Multimedia kartların kayıt ortamı Flash Belleklerdir. Hafıza kapasiteleri 2 MB ila 4 GB arasındadır. Veri aktarım hızı ise 2,5 MB/s dir. MMC'lerin yaygın kullanım alanları dijital kameralar, MP3 oynatıcılar, cep telefonu ve PDA'lardır. Multimedia kartlar ebat olarak SD kartlar ile uyumludurlar. Genellikle SD hafıza kartı için uyarlanmış aygıtlar ile problemsiz çalışırlar.

Hafıza Kartı

Güvenli sayısal hafıza kartı olarak Türkçeye uyarlanabilir. Güvenlik Dijital Kartları 2001 yılında Sandisk tarafından, daha eski bir standart olan MMC kartının geliştirilmesiyle ortaya çıkmıştır. SD 2.0 veya SDHC olarak bilinen yeni standart ile beraber ise en yüksek kapasite 32 GB'a ulaşmıştır. Kartlar üzerinde bir adet yazım koruma tırnağı mevcuttur. Daha ufak cihazlar için mini SD geliştirilmiştir. Dijital kameralar,mp3 çalıcılar, Pda'larda yaygın olarak kullanılabilmektedir.

2.4.7 Faks ve Fotokopi Makinaları

Telefon hattını kullanarak karşı tarafa yazı, şekil vb. gibi verileri aktaran cihaza Faks makinaları, bir yazı veya resmi çoğaltmaya yarayan cihaza ise fotokopi makinası denilmektedir. Faks ve fotokopi makinaların içerisine hard disk yerleştirilebildiği için dijital delil olarak gösterilmiştir.

2.4.8 GPS Aygıtları

Uydu yöntemi ile çalışan navigasyon sistemidir. GPS aygıtlarının içerisine hafıza kartı gibi kayıt ortamları takıldığı için dijital delil olarak gösterilmiştir.

2.4.9 PDA Cihazları

PDA cihazlarının açılımı Personel Data Assistant'dır. Cep bilgisayarı olarak adlandırılabilir. Bu bilgisayarın içerisine isim adres ve kişisel bilgiler kayıt edilebilen bir cihazdır. Bu cihazların kendi hafızaları olduğu için ve içerisine bilgi kayıt edilebildiği için dijital delil olarak gösterilmiştir.

2.4.10 Cep Telefonları

Cep Telefonları ise adı üstünde olan cebimizde taşıyan küçük boyutlu batarya ve pil ile çalışan görüntülü ve sesli iletişim kurmaya yarayan alettir. Cep telefonların kendi dâhili hafızası veya hafıza kartı giriş birimi olduğundan dolayı dijital delil olarak gösterilmiştir.

2.4.11 Dijital Fotoğraf Makinaları ve Video Cihazları

Bir görüntüyü dijital olarak yakalayan ve saklayan cihaza dijital fotoğraf makinası denilmektedir. Bu cihazlara takılı bulunun hafıza veya SD kartlar sayesinde makinada dijital olarak çeken görüntüyü kartlarda depolamaktadır. Dijital video cihazları ise bir görüntüyü video olarak yakalayan ve kaydetme özelliğe sahip cihazlardır. Dijital fotoğraf makinaları ve video cihazlarının kendi dahili hafızası veya hafıza kartı giriş birimi olduğundan dolayı dijital delil olarak gösterilmiştir.

2.4.12 Yazıcılar

Bilgisayarlara bağlanarak bilgisayarı verdiği dijital komutu kâğıt üzerine dökmeye yarayan cihaza yazıcı denilmektedir. Bazı yazıcıların veri saklamak için sabit diskleri olduğundan dolayı dijital delil olarak gösterilmiştir.

2.4.13 Taşınabilir Oynatıcılar (Ipod/Zune/MP3 Player)

Taşınabilir oynatıcılar Mp3 müzik veya dijital sesleri kulaklık veya hoparlör vasıtasıyla dışarı çıkarabilen cihaza denilmektedir. Apple'ın Mp3 Cihazına IPOD denmektedir. Bu Mp3 cihazların kendi hafızaları olabileceği gibi taşınabilir cihazlara dışarıdan harici olarak hafıza kartı takılabildiği gibi bu cihazların kendi hafızaları da olduğundan dolayı dijital delil olarak gösterilmiştir.

2.4.14 DVR Cihazları

Kamera görüntülerini kaydeden ve bu görüntüleri tekrar izlenebilmesi ve bu görüntülerini harici bir yere alınabilmesini yarayan cihazdır. DVR cihazının içerisinde genellikle bir hard disk olur ve bu kayıt edilen video ve görüntüler bu diske kayıt edilir. DVR cihazların içerisinde hard disk kayıt birimi olduğundan dolayı dijital delil olarak gösterilmiştir.

2.4.15 Özellikli TV'ler

Yeni nesil televizyonlarda hard disk televizyona entegre olduğu için televizyonunda bir hafızası olduğu varsayılmaktadır. Bunun için de televizyona entegre olan hard diskin

içerisine dijital veriler yüklemek mümkün hale gelmiştir. Televizyon içerine hard disk olduğundan dolayı dijital delil olarak gösterilmiştir.

2.4.16 Tabletler

Üzerinde sadece ekran olan bu ekran üzerine dokunularak işlem yapılabilen bilgisayarlar olarak tanımlanabilir. Bu tabletler parmak hareketlerine duyarlıdır bir batarya veya pil ile çalışmaktadırlar. Tabletlerin kendi hafızaları olduğu gibi bu cihazlara hafıza kartı yerleştirilerek de harici depolama birimi oluşturulmaktadır. Bu nedenlerden dolayı dijital delil olarak gösterilmiştir.

2.4.17 Telesekreterler

Telefon cihazının içinde yer alan, telefonlara cevap verilmediği zaman arayanların sesini kayıt eden cihaza denir. Cihaz içerisine hard disk veya kayıt depolama ünitesi takıldığından dolayı dijital delil olarak gösterilmiştir.

2.4.18 Sunucular (Server)

Ana Bilgisayar Üzerinde tüm bilgilerin saklandığı daha hızlı işlemcisi ve kapasitesi yüksek olan bilgisayarlardır. Sunucuların çok yüksek miktarda veri depolama kapasiteleri olduğundan dolayı dijital delil olarak gösterilmiştir.

2.4.19 Yardımcı Deliller

Olay yerinde dijital delillerin yanı sıra çeşitli belge ve dokümanlar bulunabilir not, fatura, teslimat fişi, malzeme kutusu, kargo fişi vb. bu belge ve dokümanlar özenle incelenmeli soruşturma konusu ile ilgisi olanlara el konulmalıdır.

2.5 Dijital Delillere İlk Müdahale

Bu bölümde dijital delillerin ne olduğu ve ilk müdahalenin nasıl yapılması ile ilgili bilgiler verilmiştir. İlk olarak dijital delil kavramı, dijital delillerin teknik ve uygulama açısından avantajları, dijital delillerin ne olduğu, dijital delillerde ilk müdahalenin nasıl

yapılması gerektiği, dijital delillere müdahalenin süreçlerinden bahsedilmiştir. Dijital delillerde imaj alma, dijital delillerde imaj alma yazılım ve donanımları, mobil cihazlarda adli bilişim ve inceleme süreçleri bir adli bilişim uzmanı için bilinmesi gereken en önemli bilgilerdir. Buradan yola çıkarak bu kavramların detaylı olarak bilinmesi son derece gereklidir.

2.6. Dijital Delillere İlk Müdahaleye Giriş

Dijital delillere ilk müdahale, bir suç dolayısıyla bir ikamete arama yapılmaya başlanıldığında dikkat edilmesi gereken kuralları içerir.

Delillerin orijinal kalabilmesi için olay yerinin güvenliği sağlanmalıdır. Olay yerinin güvenliğinin asıl amacı dijital delileri muhafaza altına alabilmektir. Olay yerine giriş ve çıkışlar dikkatli bir şekilde yapılmalıdır. Olay yerinde mutlak suretle bir adli bilişim uzmanı bulunmalı ve dijital delil işlemleri adli bilişim uzmanı tarafından yerine getirilmelidir. Olay yerine gitmeden önce kullanılacak olan malzemeler donanım ve yazılımlar hazırlanmalıdır. Olay yerine gelindiğinde fotoğraf makinası ve kamera ile yeteri kadar görüntü alınmalıdır. Olay yerinde hiçbir işlem yapılmadan dijital materyaller sırasıyla etiketlenmelidir. Sonra ilk olarak taşınabilir aygıtlar delil çantalarına konularak el koyma işlemine geçilmelidir. Yapılan tüm bu işlemler bir sıra listesi oluşturularak yapılmalı ve el konulan tüm dijital materyaller seri numaraları birlikte dokümanlara kayıt edilmelidir. Dokümanlarda tarih ve saat bilgisinin olay yerinde bulunan şüpheli veya şüpheli vekili avukatının imzası bulunmasına dikkat edilmelidir.

Bilgisayarlara uzaktan erişim müdahale edilebilecek bağlantılar tespit edilmeli bu cihazlar sökülmeden ilk önce güvenliği sağlanarak el koyma işlemine başlanmalıdır. Olay yerinde bilgisayarlara uzaktan erişim mevcutsa bağlantı hemen iptal edilerek durum yazılı olarak kayıt altına alınmalı yada bilgisayarlar açık ise bilgisayarlar direk fişleri prizden çekerek kontrol altına alınmalıdır. Dijital delil üzerinde olayın mahiyetine göre parmak izi çalışması yapılacaksa dijital materyallere el koymadan önce yapılmalıdır. Dijital materyaller yanında bulunan belgeler varsa notlar kayıt altına

alınmalıdır. Olay yerinde açık bulunan bilgisayarlar üzerindeki çalışan programlar kaydedilmelidir (Henkoğlu 2011).

El konulacak bilgisayarlardan veri alınmasından, bilgisayarın dondurulması, verilerin kopyalanması, klonlanması, bilgisayarın kapatılması ve laboratuvara götürülmesine kadar bütün süreçler çok titiz bir biçimde yerine getirilmeli ve eldeki delillerden hiçbirinin kaybolmaması veya zarar görmemesi sağlanmalıdır (Garfinkel 2010).

En çok aranan nesneler için bir liste oluşturulmalıdır. Tüm hard disk ve diskler için yapılacak delil arama sürecinde, bu anahtar sözcüklerle yeniden arama yapılmalıdır (Ayers 2009).

Olay yerinde dijital materyallere el koyulduktan sonra, olay yerinde imaj almak gerekiyorsa imaj alma donanımları ile birlikte güvenli bir yerde imaj alma işlemine başlanılmalıdır. İmaj alma tutanağı adli bilişim uzmanı oradaki bulunan 1 güvenlik personeli şüpheli veya şüpheli vekilli avukatı tarafından imza altına alınması gerekmektedir. İmaj ama tutanağına imajı alınan dijital materyalin seri numaraları ve özellikleri yazılmasına dikkat edilmelidir. El konulan dijital materyaller etiketlenmesi bittikten sonra ve düzgün bir şekilde paketlemesi yapıldıktan sonra taşıma çantaları konularak adli bilişim laboratuvarına gönderilmelidir.

Dijital delillerde müdahalelerde dikkat edilmesi gereken hususlar aşağıda sıralanmıştır.

1. Şifre, kripto bilgileri?
2. Network bağlantı bilgileri?
3. Çalışan programlar?
4. RAM bilgileri?
5. Aidiyet?
6. Harici bellekler aparatlar?
7. Dijital olmayan ip uçları?
8. Delil zincirinin korunması.

2.7 Adli Arama

Adlî ve Önleme Aramaları Yönetmeliği'nin 5. maddesinde ise adlî arama, bir suç işlemek veya buna iştirak veyahut yataklık etmek makul şüphesi altında bulunan kimsenin, saklananın, şüphelinin, sanığın veya hükümlünün yakalanması ve suçun iz, eser, emare veya delillerinin elde edilmesi için bir kimsenin özel hayatının ve aile hayatının gizliliğinin sınırlandırılarak konutunda, işyerinde, kendisine ait diğer yerlerde, üzerinde, özel kâğıtlarında, eşyasında, aracında 5271 sayılı Ceza Muhakemesi Kanunu ile diğer kanunlara göre yapılan araştırma işlemi olarak tanımlanmıştır (Adlî ve Önleme Aramaları Yönetmeliği 5.Madde).

2.7.1 İlk Müdahalenin Süreci

İlk müdahalenin süreç aşamaları üç bölümden oluşmaktadır. Bunlar:

1. Arama Öncesi Hazırlık,
2. Arama Zamanı,
3. Arama Sonrasıi

2.8 Arama Öncesi Hazırlık

Suçun ne olduğu, suçun görev alanımıza girip girmeği, olay hakkında görevlendirme talep yazısı olup olmadığı, mahkeme kararırım olup olmadığı, CMK 134 gereğince alınmış mı, adres sayısının ne kadar olduğu, olay yeri analizi, potansiyel suç delilleri nelerin olduğu, şüphelinin profilli, teknik cihazların yeterli olup olmadığı, imaj alma cihazlarının yeterli olup olmadığı, boş disk kapasitenin olup olmadığı ve olay yerine adli bilişim personelinin olup olmadığı gibi hususlar kontrol edilmelidir.

Arama öncesi mahkeme kararı fıkraları aşağıda sunulmuştur:

1. Bilgisayarda Arama (CMK 134 birinci Fıkra),
2. Kopya Çıkarma(CMK 134-birinci Fıkra),
3. Çözümleme (CMK 134-birinci Fıkra),
4. El Koyma (CMK 134- ikinci Fıkra),
5. Yedekleme (CMK 134-üçüncü Fıkra),

Şerit, araç kitleri, WS bilgisayar, adaptörler,(USB, SATA, IDE, ESATA, SAS FIREWIRE), kablolar, dönüştürücüler, fotoğraf makinesi ve video kamera, etiket, taşınabilir yazıcı, yazma koruma cihazları (WriteBlokers),imaj alma kitleri, imaj alma yazılımları, boş sabit disk, takım çantası(tornavida seti vb.), eldiven, galoş adli bilişim yazılımları, imaj alma donanımları, imaj kaydetmek için diskler, belgeleme(Silinmez keçe uçlu kalem yapışkan etiketler kablo etiketleri) taşınabilir bilgisayar ve yazıcı tükenmez kalem gibi malzemelerin olup olmadığının kontrol edilmesi gerekmektedir.

Dijital delillerin delil bütünlüğü korunarak imajının alınabilmesini ve fezleke için gereken acil ve basit incelemelerin yapılmasını sağlayan cihazdır.

Şekil 2.1'de Tableu Marka Yazma Koruma Kiti (writeblockers) gösterilmiştir.

Şekil 2.1 Tableu Marka Yazma Koruma Kiti (Writeblockers)

İmaj alma cihazı, adreste ya da şube müdürlüğünde, el koyulan dijital materyallerin sağlıklı bir şekilde birebir kopyasının (clone) veya imajının almasını sağlayan cihazdır. Şekil 2.2'de Tableu marka TD1 Duplicator cihazı gösterilmiştir. Tableu marka TD1 duplicator cihazının sag tarafına imajı alınmak istenilen hard diski sol tarafına ise boş olan hard diski takılır ve istenirse hard diskin imajı istenilirse hard diskin kopyası alınabilir.

Şekil 2.2 Tableu Marka TD1 Duplicator Cihazı

Yapılan arama sonucu adreste el konulan hard disklerin güveni bir şekilde adli bilişim laboratuvarına götürülmesinde kullanılan alettir. Şekil 2.3'de taşıma çantaları verilmiştir.

Şekil 2.3 Taşıma Çantaları

Arama öncesi imaj almaya yarayan programların isimleri aşağıda liste olarak verilmiştir. Bunlar;

1. Helix3,
2. FTK (FORENSIC TOOLKIT),
3. EnCase,
4. Tableau Imager,
5. XWays programlarıdır.

2.9 Arama Zamanı

Aramaya başlanılmadan önce aranacak adresin muhafaza altına alınması gerekir. Daha sonra dijital delillerin karartılması veya fiziksel olarak zarar verilmesini engellenmenin sağlaması, çalışan sistemlere dikkat edilmesi, adli bilişim personeli haricindeki görevlilerin dijital delillere müdahalesini engellenmesi, parmak izi çalışması yapılması gereken aygıtlara el koyma/imaj alma işlemi yapılmadan olay yeri inceleme uzman personel tarafından çalışma yapılması, şüpheliler şok halindeyken sorular sorarak şifre gibi hayati bilgiler şüphelilerden alınmaya çalışılmalı, delillerin tamamı tespit edilmeli ve ilk iş olarak dokümantasyonu, etiketlenmesi çok iyi ve ayrıntılı yapılmalı, deliller öncelikler bulundukları yerlerle fotoğraflanmalı veya video kaydı yapılmalı, odalara isimlendirme yapılması için kroki çizilebilmeli, suç ve delillerin listelenmesi listeleme yapıldıktan sonra imajı adreste alınacak materyaller belirlenmeli, dijital delillerin orijinalinde çalışma yapılmamalı, imaj alma işlemleri adli bilişim ilk müdahale kursu almış uzmanlar tarafından yapılmalı, yasal olarak el koyma değil, adreste imaj alma işlemi tercih edilmelidir. Cumhuriyet Savcısı operasyon ekibi tarafından her aşamada bilgilendirilmeli, tarafların kopya istemesi durumunda bir kopyası taraflara verilmelidir.

El koyma veya imaj alma sırasında; En az 2 hazirun (tanık), şüpheli veya gerekirse vekilinin nezareti, fotoğraflama ve kameraya alınması gerekir. Şifrelerin çözümlememesi gizlenmiş bilgilere ulaşılamaması durumunda dijital materyallere el konulmalıdır.

El koyulacak materyalin tüm bağlantı kabloları, güç kabloları ile birlikte el koyulması gerekir. Dijital delillerin adli makamlarca delil olarak kabul edilebilmesi süreci ilk müdahaleden başlamaktadır. Bu aşamada yapılacak bir hata tüm dava sürecini ve taraflarını etkileyecektir. Adli makamlara sunulacak en sağlıklı dijital deliller ilk müdahale süreçlerinin eksiksiz olarak yerine getirildiği ve adli bilişim süreçlerini tamamlamış delillerdir. Teknolojinin sürekli olarak değişmesi tartışmasız bir gerçek olsa da dijital delillerin toplanmasına yönelik prensipler ve teknikler bu değişmeler karşısında etkili olmaya devam edecektir.

2.10 Dijital Delillerin Avantajı ve Dezavantajı

Dijital delillerin imajının alınabilmesi ve kopyalanabilmesi delilin üzerinde oynanıp oynanmadığı tespit edilmesi dijital delillerin avantajını göstermektedir. Dijital delil hassas yapıda olduğu için delilin çabuk deforme olması dezavantajı olarak gösterebilir. Toplarken, muhafaza ederken ve taşınırken özel önlemler alınması gerekir. Şekil 2.4'de dijital delillerin bulunduğu bir ortamdan bir örnek gösterilmiştir.

Şekil 2.4 Örnek Dijital Deliller

2.11 Dijital Delillerin Elde Edilmesi

Dijital delillere mümkün olduğunca elle dokunmamaya özen gösterilmelidir. Çünkü el konulan cihazda statik elektrik olabileceği ve çıplak elle cihaza dokunulduğunda el konulan cihaza zarar verilebilmektedir. Bunu önlemek için statik önleyici bileklikler kullanılmalıdır. Elektronik cihaz ve veri depolama üniteleri üzerinde parmak izi araştırması gibi kriminal işlemlerde ilk aşamada dijital delillerin toplanması işlemi ile birlikte yürütülmelidir. Delillerin elde edilmesi ve arama işlemi esnasında bir denetleme/gözetleme zinciri oluşturulmalı, tüm yapılan işlemler kamera kayıtlara altına alınmalı ve grup halinde hareket ederek kameranın görme alanı dışınca hareket edilmemelidir. Olay yeri incelemesinde uyulması gereken genel kurallar çerçevesinde öncellikle çalışan sistemler tespit edilmeli, uçucu bilgilerin analizi ile ilgili nasıl bir yöntem izleneceğine karar verilmelidir.

Uzaktan erişim ile ilgili bir problem tespit edilmemiş, delil bozacak bir program çalıştırılmamış ve çevre güvenliği de alınmış ise, çalışma programlarını gösteren bir ekran görüntüsü alınmalı ve ilk olarak şifre sorma ihtimali olan ekran koruyucu vb. program çalışmasına son verilmelidir. Laboratuvar ve bilirkişi incelemelerinde büyük zorluklar yaşatılabilecek programlar (PGP TrueCryp vb.) varlığı araştırılmalı ve bu tür programların kurulu olması halinde, durumu açıklayan bir tutanak hazırlanmalı ve kamera kaydı altında canlı inceleme yapılmalıdır. Canlı inceleme konunun uzmanı tarafından yapılmalı, yapılan tüm işlemler ayrıca dokümana kayıt edilmelidir. Olay yerindeki açık bilgisayarların kapatma işlemi esnasında işlemin sisteminin durumu mutlaka göz önünde bulundurulmalıdır. Windows işletim sistemleri bilgisayarın fişini çekmek suretiyle kapatılırken, Linux ve Macintosh bilgisayaralar normal bilgisayar kapatma işlemi kapatarak yapılmalıdır. Diz üstü bilgisayarlar kapatılırken, işletim sistemine bağlı olarak aynı işlemler uygulanmalı, bataryanın da çıkartılması gerekmektedir. Olay yerindeki bilgisayarların imajı alınırken adli bilişim standartlarına uygun programlar (FTK, ENCASE,) gibi programlar kullanılmalı ve orijinal delilin birebir kopyası alınmalıdır.

2.12 Açık Sistemlerde Dijital Delillere İlk Müdahale

Açık sistemlerde dijital delillere ilk müdahalede karşılaşılan sorunlar ve çözümleri aşağıda sunulmuştur.

Uçucu veri, bilgisayar kapatıldığında çoğunlukla değişen ve sıkça kaybolabilen verilerdir. Bu verilerin kaybolmaması için monitörün fotoğrafını çekilmeli ve görüntülenen bilgileri belgelenmeli, sistemin bir ağa bağlı olup olmadığını kontrol edilmesi gerekmektedir. Uçucu verinin diğer tanımı ise uçucu veriler, bilgisayar sistemleri üzerinde, geçici kayıt bölgelerinde tutulan ve elektrik gücü kesildiğinde içeriği sıfırlanan verilerdir (Shinder 2002).

Raid yapı sistemleri ise sistemi kapatmadan imajını alın ve tutanakla belgelenmelidir. Normal işletim sistemi ise Cofee, Helix, irtools, Encase Portable yazılımları ile açık sistemlerde imajının alınması gerekmektedir.

İlk olarak en çok kaybolma (uçma) ihtimali olan delilleri toplamalıdır:

1. Fiziksel hafıza (RAM) verilerini,
2. İlişkili veri (METADATA)'leri,
3. Kullanıcı verilerini,
4. Yedeklenmiş verileri toplanmalıdır.

Uçucu Verinin İçerisinde Tespit Edilebilecek Veriler;

1. Unix, OS X: /dev/mem, /var/vm,
2. Unix, Linux, OS X: swap file,
3. Linux: /proc/kcore,
4. Sanal hafıza,
5. Microsoft Windows: pagefile.sys, hiberfil.sys.

Uçucu Verinin İçeriği;

1. İşletim Sistemi (OS) bilgisi,
2. Uygulama bilgileri,
3. Kötü niyetli yazılım (malware) tespiti,
4. Microsoft Windows: pagefile.sys, hiberfil.sys,
5. Register (Kayıt defteri), cache ve çevresel hafıza,
6. Ana / fiziksel hafıza (RAM),
7. Network (Ağ durumu),
8. Çalışan uygulamalar,
9. Sürücüler,
10. Yedekleme üniteleri vs.

Microsoft Windows;

İşletim Sistemi (OS) bilgisi;

1. Çalışan uygulamalar ve işler,
2. Açık dosyalar,
3. Ağ bağlantısı bilgileri,
4. Kaybolma ihtimali olan kayıt defteri verileri,
5. Psinfo (Sistem bilgileri Win7, ghz, Ram),

6. Psloggeon (Oturum açılan pc listesi),
7. Psloglist (Olay günlüğü),
8. Autoruns (Çalışan Programları listeler),
9. Pslist (Çalışan işlemler, tasklist),
10. Handle (Verilerin hangi işlemle açıldığı, ilişkili olduğu),
11. Listdlls (Dll sürücülerin hangi işlemlerle bağlantılı olduğu),
12. Psservice (Sistem üzerinde çalışan hizmetler, sc query),
13. Procexp (Arka planda çalışan işlemler),
14. Procmon (Şuanda çalışan işlemler),
15. Psfile (Uzaktan erişim ile açılan dosyalar),
16. Tcpview (Ağ bağlantısı ile bağlı programların ne ile bağlı olduğu),
17. Shareenum (Kullanıcıların ağda hangi dosyaya bağlandıkları),
18. Fport (Açık portları gösterir)

gibi bilgilere ulaşılabilmektedir.

Uygulama Bilgileri;

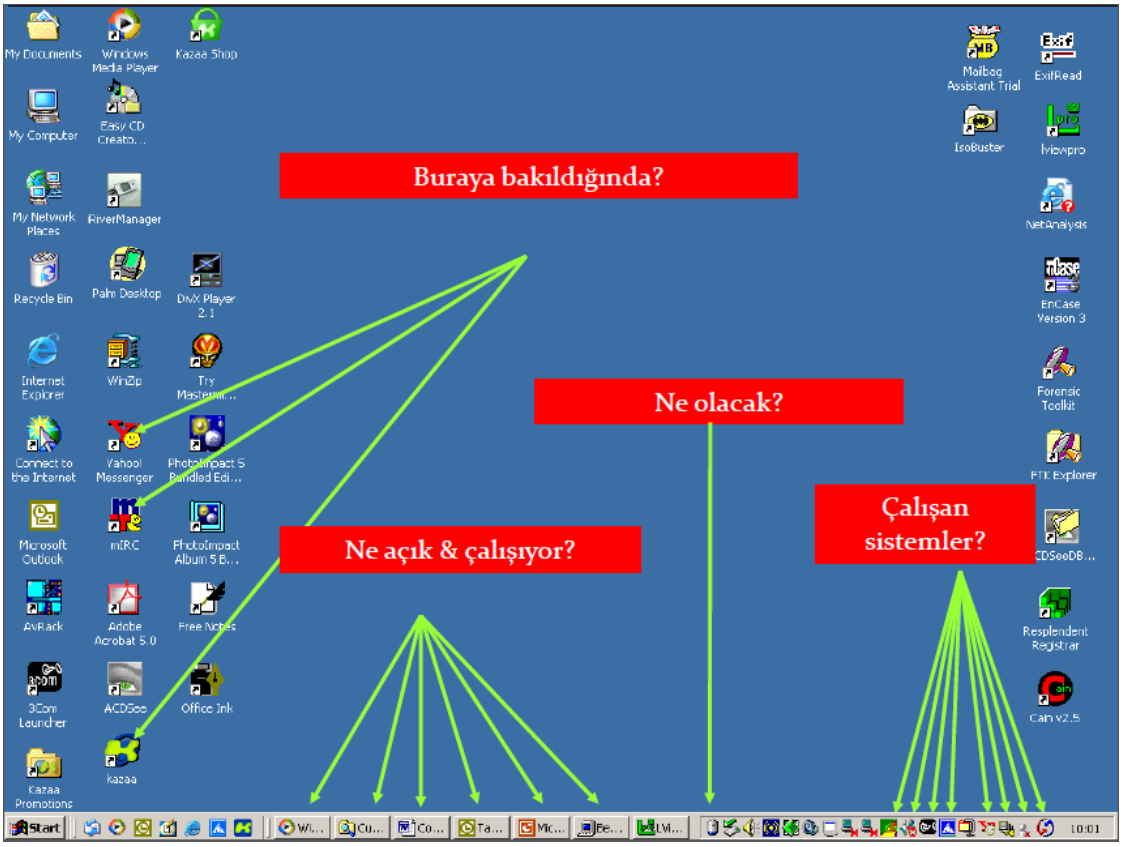
1. Şifreler (okunabilir şekilde),
2. Henüz şifrelenmemiş halde bulunan veriler,
3. Anlık mesajlaşma oturumları,
4. Açık web e-posta ekranları,

gibi bilgilere ulaşılabilmektedir.

Kötü niyetli yazılım (malware) tespiti;

1. Rootkitler,
2. Trojan yazılımları,
3. Botnet aktiviteleri,

gibi bilgilere ve zararlı yazılımlar bulunduğu bilgisayarın dosya sistemi içerisinde bir takım izler bırakırlar. Bu izler de sıklıkla fiziksel hafıza (RAM) içerisinde bulunur. Şekil 2.5'de açık sistem olan bir masa üstü örnek gösterilmiştir.



Şekil 2.5 Açık Sistem Olan Bir Masaüstü

2.13 Açık Sistemlere Müdahalede Oluşabilecek Sistem Değişiklikleri

Açık sistemlerde müdahalede oluşabilecek sistem değişikleri aşağıda belirtilmiştir.

1. Harici USB disk bağlanması,
   a-) USB ilişkili kayıt defteri girdisi (kaydı) oluşur.
   b-) Mount edilmiş aygıtlar alanına girdi eklenir.
2. Bir uygulama çalıştırmak,
   a-) Son kullanılanlar alanlarına ekleme yapabilir
   b-) UserAssist veri değeri ekleyebilir.
3. Klasör açmak ve kapatmak, kayıt defterinde bulunan ShellBag kayıtlarında değişlik olur.
4. Firewall yazılımları başlatılan uygulamalar için yeni kurallar oluşturabilir,
5. Anti virüs yazılımları takılan USB disk içerisinde otomatik tarama başlatabilir. Bir indeksleme yazılımı mevcut ise takılan disk içeriğini delil niteliğindeki diskte bulunan kendi veri tabanında güncelleyebilir,
6. Şifreli verileri yalnızca yetkili olan kişiler analiz etmesi gerekmektedir.Bu yetkili

kişiler bilgisayar sahibinin özel bilgilerini okuyabilirlerler. Yetkili kişi bilgisayarın şifresini çözmeye çalışmamalıdır (Srinivasan 2007).

2.14 Kapalı Sistemlere Müdahale Ederken Dikkat Edilmesi Gerekenler

Güç kaynağını elektrik ile bağlantısını kesilmeli, güvenli taşıma için mevcut diskleri çıkarın ve ayırıcı özellikleriyle belgelenmeli, fotoğraflama ve parmak izi çalışması yapılmalı, el koyma işlemi sırasında şüpheliler netleştirilmeli, CD Rom kontrol edilmeli, sürücü yuvaları ve güç bağlantılarına bant çekilmeli, sistemin tipini, modelini ve seri numarası kaydedilmelidir.

Kapalı sistemlerdeki güç (Power) hariç veri taşıyan bütün medyalar sökülmeli sistem sürücüleri söküldükten sonra BIOS (BasicInputOutSystem) temel giriş çıkış sistemi çalıştırılarak doğru sistem tarihi ve zamanı ve ayrıca sistemde yüklü çevre birimlerin önyükleme sırasını tanımlamasında yardımcı olabilecek bilgiler alınmalı, BIOS önyükleme için sistemiz de giriş (f5, f2 veya delete) tuşları değişkenlik gösterebilir.

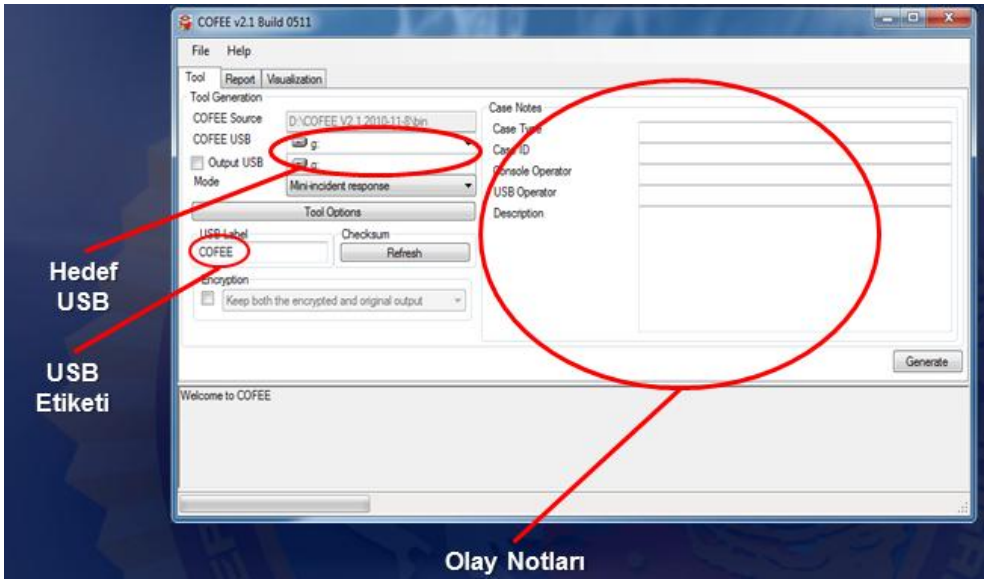
2.15 Sistem Bilgilerinin Toplanması

Cofee programı bir ilk müdahale programıdır. Flash bellek vasıtasıyla bilgisayara takılarak çalıştırılır. Cofee programı ile bilgisayarın tarih ve saat ram bilgileri ve bilgisayarın kullanıcı adı gibi verilere ulaşılabilmektedir.

2.15.1 Cofee Programı

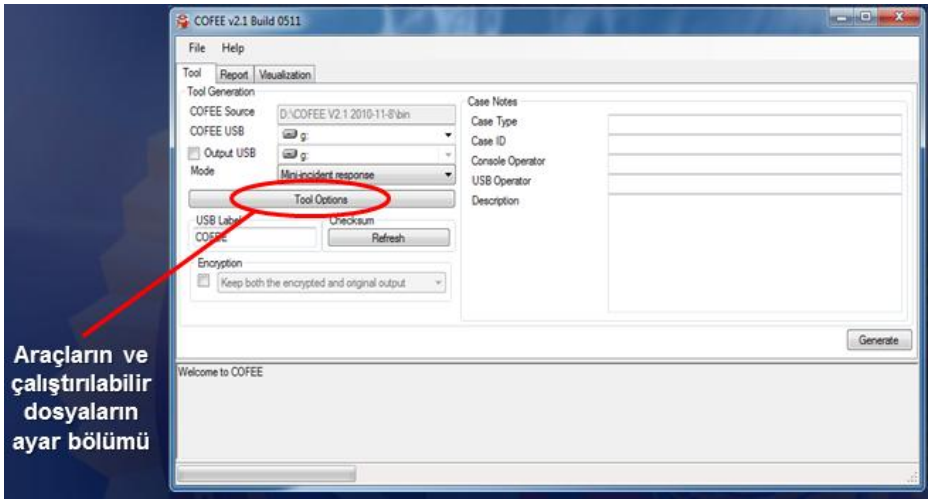
Cofee (Computer Online Forensic Evidence Extractor) Microsoft tarafından hazırlanmış bir ilk müdahale aracıdır. Daha önce bir USB sürücüsüne yüklenen ve açık sistemlerden bilgi toplamak için kullanılan bir dizi (100-150 kadar) uygulama, inceleme yapılacak sisteme USB'nin takılarak başlatılması ile otomatik olarak sırayla çalışır ve gerekli bilgileri toplar. Topladığı bilgileri aynı USB içinde depolar. Şekil 2.6'da Cofee programına ait örnekler gösterilmiştir.

Cofee programını flash belleğe yükleyip bilgisayara takılır ve Usb içerisinde yüklü bulunan Cofee Programını çalıştırılır. Programı çalıştırdıktan sonra Cofee Source kısmında olması gerekmekte, Cofee Usb ve bilgilerin dışarı çıkarılacağı alan seçilir. Sol tarafa ise olay hakkında not alınacak ise buralar doldurulmalıdır. Şekil 2.6'de Cofee Ekran Ara yüzü 1 gösterilmiştir.



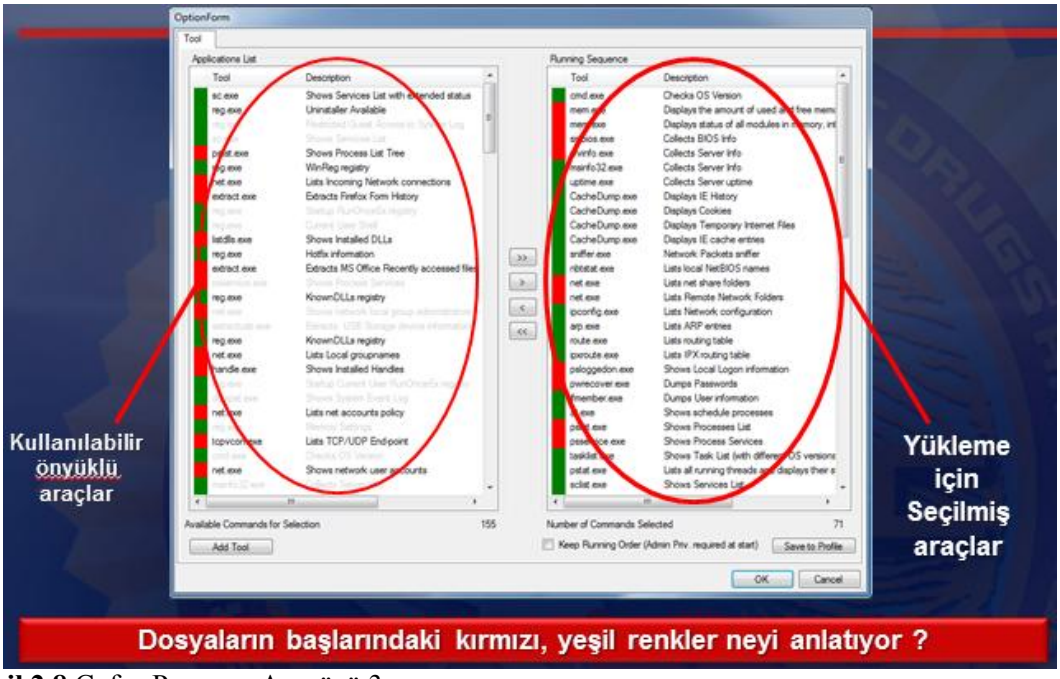
Şekil 2.6 Cofee Program Arayüzü 1

İşareti olan bölümde araçların ve çalıştırabilir dosyaların ayar bölümü bulunarak ayarlanmalıdır. Şekil 2.7'de Cofee Ekran Ara yüzü 2 gösterilmiştir.



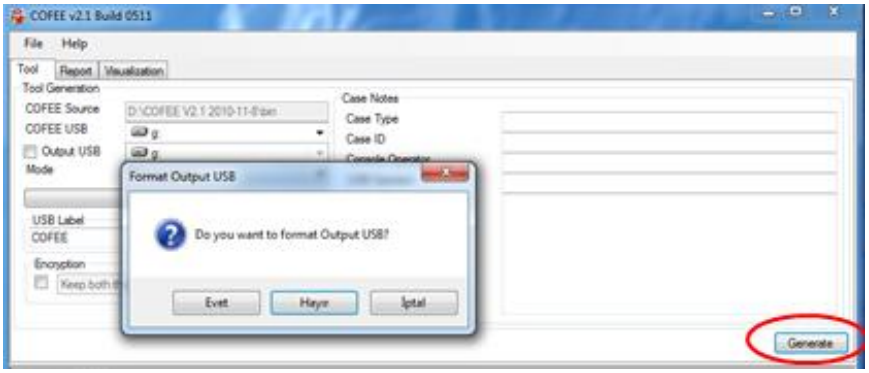
Şekil 2.7 Cofee Program Arayüzü 2

1. KIRMIZI: Medya ve ‘registry’ içerisindeki kullanıcı verilerinde değişiklik olabilir veya ‘unallocated space’ üzerinde dosya oluşturabilir.
2. SARI: Medya ve ‘registry’ üzerindeki sistem verilerinde değişiklik oluşturur.
3. YEŞİL: Sistem ve kullanıcı verileri üzerinde hiçbir değişiklik yapmaz. Şekil 2.8’de Cofee Ekran Ara yüzü 3 gösterilmiştir.



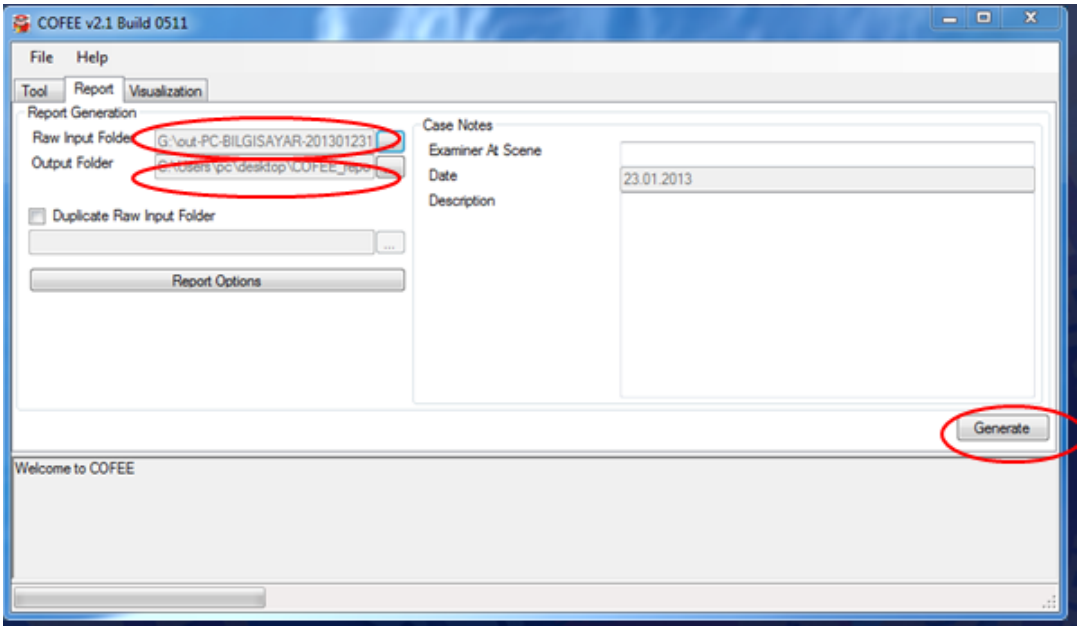
Şekil 2.8 Cofee Program Arayüzü 3

Sol altta bulunan Generate sekmesine tıklayarak sistem bilgilerini almaya başlanır. Şekil 2.9’de Cofee Ekran Ara yüzü 4 gösterilmiştir.



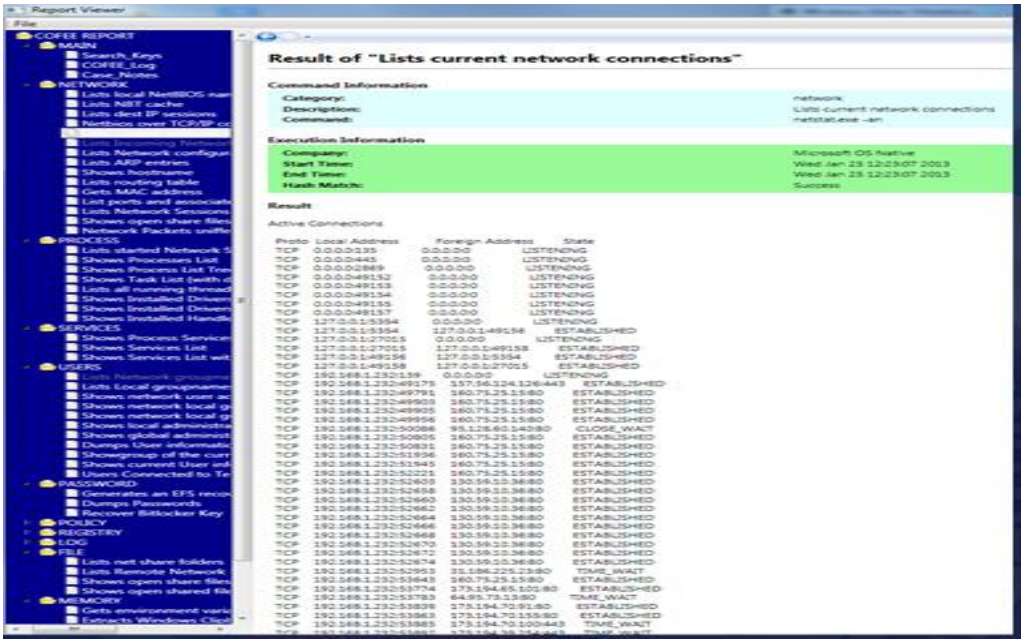
Şekil 2.9 Cofee Program Arayüzü 4

Cofee programında alınan sistem bilgilerinin rapor bilgilerinin alınması için Report kısmına tıklayarak alınmaktadır. Şekil 2.10'de Cofee Ekran Ara yüzü 5 gösterilmiştir.



Şekil 2.10 Cofee Program Arayüzü 5

Alınan Örnek rapor ekranı aşağıya çıkartılmıştır. Şekil 2.11'de Cofee Ekran Ara yüzü 6 gösterilmiştir.



Şekil 2.11 Cofee Program Arayüzü 6

2.15.2 Cofee İle Elde Edilebilen Bilgiler

1-) Tarih ve saat,
2-) Uçucu hafıza,
    a-) Fiziksel hafıza imajı
    b-) Swap file (pagefile.sys vs)
3-) Network bağlantıları,
    a-) Açık TCP ve UDP portları
    b-) NetBIOS, komşu ağ bağlantıları
    c-) ARP cache
    d-) IPConfig ayarları
4-) Kullanıcı hesapları,
    a-) Giriş yapmış kullanıcılar

2.16 Arama Sonrası Yapılması Gereken İşlemler

Arama sonrası arama yapılan adreste dijital materyallere düzenli bir şekilde imaj alma işlemine başlanır. Eğer imaj alma işlemi olay yerinde yapılmıyorsa el koyma işlemine geçilir. Toplanan her delil paketlenmeden önce mutlaka etiketlendirilmeli ve dokümanlara kayıt edilmelidir. Bu işlemler mümkün olduğunca kamera eşliğinde yapılmalıdır. Elde edilen delillerin yerleştirildiği kutu ve paketler ayrıca etiketlendirilmeli ve ihtiyaç duyulması halinde açıklayıcı notlar alınmalıdır. Birden fazla bilgisayara el konulması halinde, sistem bütünlüğünün bozulmamasına ve etiketlendirilmeye özen gösterilmelidir. Her bilgisayar birimlerinin sahip olduğu yardımcı donanım birimleri kendi gruba içerisinde paketlenmelidir. Veri depolama ünitelerinden alınan imajların MD5 VE SHA1 hash değerleri alınmalı ve bu değerler tutanak kayıtlarına geçirilmelidir. CD ve DVD yedekleme ünitelerinin hassa veri depolama birimi olduğu unutulmamalı, çizilmesi, bükülmesi ve kırılmamasına özen gösterilmelidir. Dijital delillerin taşınma işlemi uygun şekilde yapılmalıdır. Dijital deliller yapısı gereği (statik elektrik ve bazı cihazların oluşturduğu manyetik akımdan etkilenme olanağı yüksek olduğu için) özel toplama ve paketleme poşetlerinin kullanılmasına özen gösterilmelidir. Delillerin yerleştirildiği paketler aşırı ısı veya sıvı

temasından uzak tutulmalıdır. Delillerin araç içerisindeki yerleşimi fiziki darbelerden korunacak şekilde yapılmalıdır.

2.17 Dijital Delil Zarfları

Zarfların üzerindeki bölümler detaylı ile birlikte doldurulmalı, delil zarfını ele alındığında içerisine konan malzeme hakkında yeteri kadar bilgiye ulaşılabilmelidir.

Delil torbalarının üzerine ise;
1.Soruşturmayı yapan birim,
2.İlgili birime ait suç numarası,
3.İşlemin yapıldığı tarih,
4.İşlemin yapıldığı Cumhuriyet Savcılığı adı,
5.Savcılık soruşturma numarası,
6.El konulan eşyanın cinsi, miktarı, modeli, seri numarası, kapasitesi, el konulduğu yer,
7.El konulan eşyanın maliki olan şüphelinin kimlik bilgileri, adres ve telefonları,
8.El konulan dijital deliller üzerine el koyma işlemi sırasında şüpheli veya huzurunda el koyma işlemi yapılan şahsa adı soyadı yazdırılıp imza ettirilmedir.

Daha sonra laboratuvar da incelenmek üzere götürülen ve el konulan bilgisayar üzerinde veya veri depolama ünitelerinin orijinalleri üzerinde kesinlikle çalışılmamalıdır. Fakat her ne kadar üzerinde çalışma yapılacak olsa da dijital delillerin güvenliği açısından imajının(kopyasının) üzerinde çalışılmadır. Emanete yada incelenmek üzere laboratuvara götürülen her delilin mutlaka envanter kaydı yapılmalıdır. Envantere ya da incelenmek üzere laboratuvara götürülen her bilgisayarın toz, nem, rutubet, aşırı ısı ve manyetik gibi zararlı olabilecek etkenlerden uzak tutulmalıdır. Çizelge 2.1'de örnek adli bilişim olay yeri kontrol formu gösterilmiştir.

Çizelge 2.1 Örnek adli bilişim olay yeri kontrol formu

Hazırlık Aşaması	25-)DVD CD player içlerinin kontrol edildimi
1-) Adresle ilgili CMK 134 kararı kontrol edildi mi?	26-)Yazıcı kontrol edildi mi?
2-) İmaj alınması için kullanılacak yeterli boş disk mevcut mu?	27-) Fax kontrol edildi mi?
3-) Aramada bulunacak 2 adet hazurun mevcut mu?	28-) İnternet üzerinde FTP adres ve şifreleri kontrol edildi mi?
4-) Eldiven ve galoş takıldı mı?	29-) Materyallerin ait olduğu cihaz ve odalara göre iki taraflı numaralandırılması yapıldı mı?
5-) İşlemi kayda alacak kamera mevcut mu?	30-)- Açık halde bulunan bilgisayarlar tespit edil mi?
Tespit Aşaması	31-) Açık halde bulunan bilgisayarda deep freez, true crypte, pgp, bitlocker türü programların olup olmadığı kontrol edildi mi?
1-) Odalarda bulunan malzemeler tespit edildi mi?	32-) Özellikle cep telefonlanna ait pin kodu, güvenlik koduve benzeri tüm şifreleri n ku llanıcılara soruldu mu ve not edildi mi?
2-)Server	33-) Varsa açık imaj alma işlemi uygulamasına karar verildi?
	İmaj Alma Aşaması
3-)Masaüstü Bilgisayar	1-) İmaj alma işlemi için uygun masa ayarlandı mı elektrik tesisatı güvenli bir şekilde kuruldu mu?
4-)Dizüstü Bilgisayar	2-) İmaj alma işlemi gerçekleştirildi mi?
5-)Tablet Bilgisayar	3-) HASH bilgileri toplandı?
6-)PDA(cep bilgisayarı)	4-) İmajı alınanmayan materyallere el kon ulması için operasyon ekibine teslim edildi mi?
7-) Harici Disk	5-) El konulacak m ateryallere ait aparattar ci hazla beraber alı ndı mı? (güç kablosu, data kablosu, bilgisayar bağlantı kablosu)
8-) Sabit Disk	6-) İmaj yedeği istenip ist enmediği soruldu
9-) Flash Disk	7-) İstendiyse kopyalama yapıldı mı şahsa ve avukata teslim edildi mi?
10-)Hafıza kartı	8-) İmajı alınan materyaller tam sağlam çalışır vaziyette sahibine ya da el konu acaksa operasyon ekibine teslim edildi mi?
11-) Mp3,mp4 çalar	9-) İmaj alma tutanağı, önceden hazırlanan tutanak örneğine uygun olarak olay mahallinde yazıldı mı?
12-) Bluray Disk	10-) imajların alındığı diskler operasyon birimine tam sağlam çalışır vaziyette teslim edildi mi?
13-) Disket	11-) El konulacak materyaller ve imaj diskl eri delil zarflarına konuldu mu?
14-) Zip Disket	12-) El konulacak materyallerin bulunduğu zarfın ağzı kapatılarak taraflara paraflatıldı mı?
15-) Fotoğrafaf Makinesi	
16-) Dijital Kamera	
17-) Ses kayıt cihazı	
18-) Play Station	
19-) X-Box	
20-) Ninte ndo	
21-) Güvenlik Kamera Cihazları(DVR)	
22-) Modem	
23-) Databank	
24-) Cep Telefonu	

2.18 Hash Değeri Nedir

Hash değeri, bilgisayar medyasında bulunan tüm 0 ve1'lerin birbirleri ile belirli bir algoritma kullanılarak çarpılması sonucu elde edilen değerdir. Hash, MD5 için 0-9 ve a-f karakterlerinden oluşan 32 karakter uzunluğunda bir değer iken, SHA-1 için aynı karakterleri içeren 40 karakter uzunluğunda bir değerdir. En çok kullanılan hash değerleri MD5 ve SHA1'dir (Kılıç 2014). Elektronik deliller açısından imaj alma sırasında oluşturulan hash değeri ile güvenilirlik sağlanması amaçlanmaktadır. Dava sürecinde bir itiraz olduğunda, bu hash değerleri üzerinden delile müdahale olup olmadığı hususu açıklığa kavuşturulabilecektir (Demirkaya 2009).

2.19 Md5 ve Sha1 Hash Kodu Nasıl Hesaplanır

MD5 (Message-Digest algorithm 5) yaygın olarak kullanılan bir kriptografik özet fonksiyonudur. MD5 ve SHA-1 özet fonksiyonları 512 bitlik bloklar kullanır. Giriş mesajı 512-bitlik blok parçalarına ayrılır. İleti, uzunluğu 512 ile bölünebilecek şekilde doldurulur. Bu doldurma işlemi şu şekilde işler: İlk olarak mesajın sonuna bir bit 1 eklenir. Sonrasında mesajın uzunluğu 521'nin katından 64 bit eksik olacak şekilde 0'larla doldurulur. MD5 algoritması, A, B, C ve D olarak adlandırılan dört adet 32 bitlik kelimeye ayrılmış 128 bitlik parçalar üzerinde çalışır. Bunlar belirli sabit değerlerle başlatılır. Daha sonra ana algoritma, her 512-bit ileti bloğunu durumunu(128 bit) değiştirmek için kullanır. Bir mesaj bloğunun işlenmesi, tur denilen dört benzer aşamadan oluşur. Her tur, doğrusal olmayan bir fonksiyon, modüler toplama işlemi ve bit bazında sola kaydırma işlemlerinden oluşur. Toplamda 32 karakterlik bir kod oluşturur ve bu karakterler harf ve rakamlardan oluşmaktadır. (İnt.Kyn.10). SHA-1 (Secure Hash Algorithm 1) olarak bilinen 160 bit özet değer ve 40 karakterli bir kod oluşturur ve bu kodların tamamı rakamlardan oluşmaktadır. SHA-1, uzunluğu en fazla 264 bit olan mesajları girdi olarak kullanır ve 160 bitlik mesaj özeti üretir. Bu işlem sırasında, ilk önce mesajı 512 bitlik bloklara ayırır ve gerekirse son bloğun uzunluğunu 512 bite tamamlar. Hash sayesinde dosyalarda değişiklik yapılıp yapılmadığı öğrenilebilir.

2.20 Dosya İmzası Nedir

Dosya imzası, dosya içindeki verini tanımlanmasında ya da bir dosyanın içeriğini doğrulamada kullanılan verilerdir. Her dosya türünün kendine özel bir imzası vardır. Her dosya ikili dosya formatında başlık ve son bilgisine sahip olmaktadır. Dosya içeriklerine detaylı olarak bakmak için Unix tabanlı sistemlerde hexeditor komutunu kullanılabilir. Windows sistemlerde hex edit programını indirerek inceleme yapılabilir. (İnt.Kyn.11).

2.21 Artık Alan(Slack Space) Nedir

Bir sabit sürücünün depolama alanının sonundan, sabit sürücünün dosya kümesinin sonuna kadar olan sabit disk alanını ifade eder. Tipik sabit sürücülerde bilgisayar, dosyaları belirli bir dosya boyutundaki kümeler halinde sürücüde saklar. Örneğin, sabit sürücüdeki dosya sistemi, verileri dört kilobayt kümesinde depolayabilir. Bilgisayar dört kilobayt kümede yalnızca iki kilobayt olan bir dosyayı saklarsa, iki kilobayt boşluk olacaktır. (İnt.Kyn.12).

2.22 Dijital Delillerde İmaj Alma

Dijital delillerde alma konusu bu bölümde detaylı tasvir edilmiştir.

2.22.1 Adli İmaj

Adli imaj depolama aygıtının kurcalanmamış (üzerinde değişiklik yapılmamış) kopyası anlamına gelir. Yani delilin birebir kopyasına imaj denilmektedir. Adli imajın çeşitleri, yazılımlar ve donanımlar aşağıdaki gibi belirtilmiştir:

A-Çeşitleri

1-) Mantıksal İmaj

2-) Fiziksel İmaj

B-Yazılımlar

1-) Encase

2-) Ftk Imager

3-) X-Ways

4-) Tableau Imager

5-) Helix

C-Donanımlar

1-) Write-Blocker

2-) TD1

3-Forensic falcon

D-Mobil

1-) Cellebrite Ufed

2-) Mobiledit Forensic

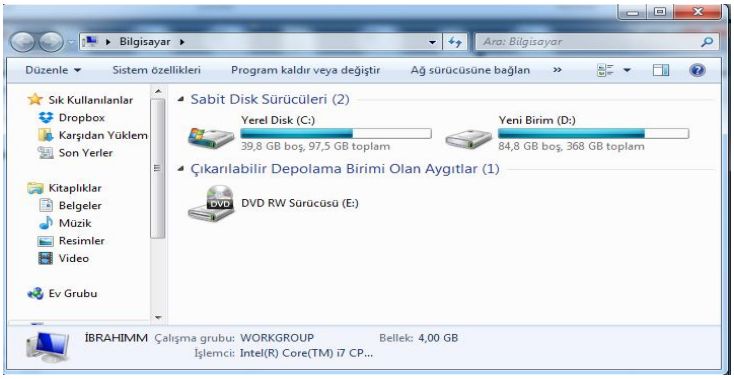
3-) Oxygen Forensic

2.22.1.1 Adli İmajın Gereklilikleri

Delillerin bütünlüğü (hash) değerleri, orijinal verilerin istenmeden zarar görmesine mani olunması adli imajın gerekliliklerindendir. Dijital delillerin orijinal halinin bozulmamasına özen gösterilmelidir. Adli imaj alınırken de orijinal hard diskin birebir imajının alınmasına özen gösterilmelidir. Adli olarak alınan imajın bozulması zor olduğundan dolayı suça konu dijital materyalin adli imajının alınıp saklanması doğru olacaktır.

2.22.1.2 Adli İmajın Çeşitleri

Mantıksal imaj bilgisayarda bulunan tüm dosya ve dizinlerin kopyası anlamına gelir. Şekil 2.12'de mantıksal imaj örneği verilmiştir



Şekil 2.12 Mantıksal İmaj

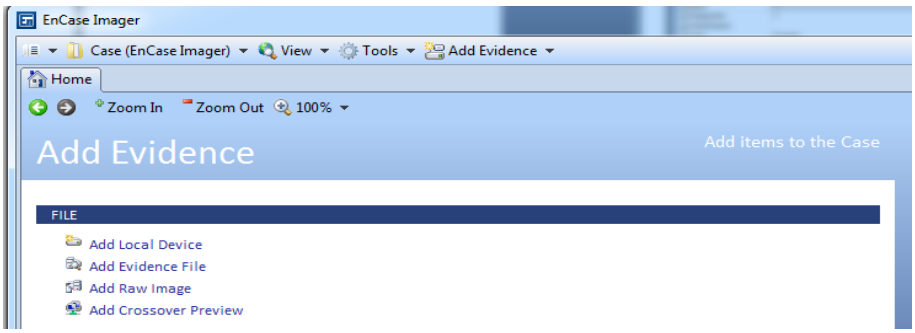
Fiziksel imaj sabit sürücüde bulunan bitlerin tek tek kopyası anlamına gelir. Yani hard diskin imajın E.01, Raw (dd), AFF olarak alınmasıdır. Şekil 2.13'de fiziksel imaj örneği verilmiştir.

Şekil 2.13 Fiziksel İmaj Almak İçin Kullanılan Harddisk

2.22.2 İmaj Alma Yazılımları

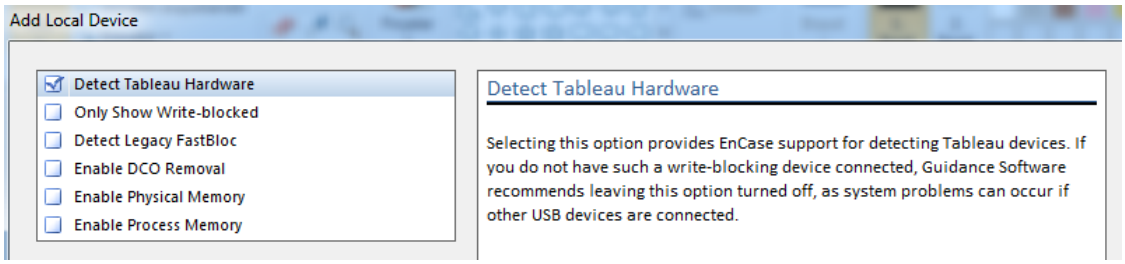
2.22.2.1 Encase Imager

Amerikan Firması Guidance Software şirketi tarafından yazılan dijital veri inceleme ve imaj alma programıdır. Program Encase V7 versiyonu öncesi E.01 imaj formatı kullanırken V7 sonrası EX01 formatını kullanmaya başlamıştır. Yazılım ile ağ üzerinden imaj alınmamaktadır. Yazılım imaj aldıktan sonra bu imajın doğrulamasını yapmaktadır. RAM İmajı alınabilmektedir.Md5 ve SHA1 hash değerleri ile imajlar hesaplayabilmektedir. Encase İmager programı program sitesinden ücretsiz olarak indirilebilmekte olup, inceleme programı ücretli olup Dongle (USB) ile çalışmaktadır (İnt.Kyn.4). Encase İmager programını açılma görüntüsü ve arayüzü Şekil 2.14'de verilmiştir.



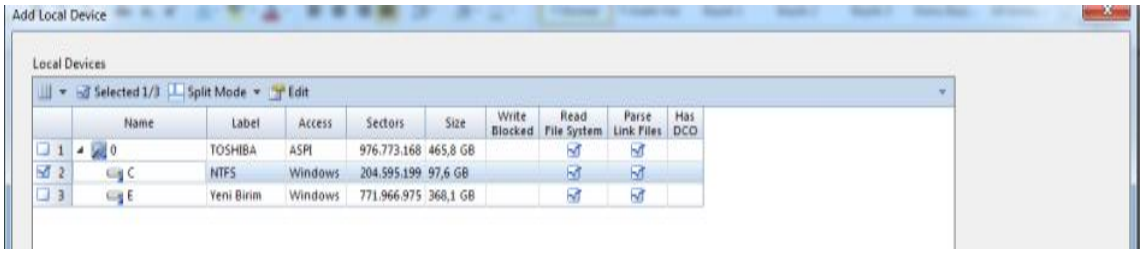
Şekil 2.14 Encase Program İmaj Alma Arayüzü 1

Yerel Cihaz Ekle (Add Local Device) tıklanır. Sonra Donanım Algıla (Detect Tableau Hardware) tıklanır. Encase İmager programını cihaz ekleme bölümü Şekil 2.15'de verilmiştir.



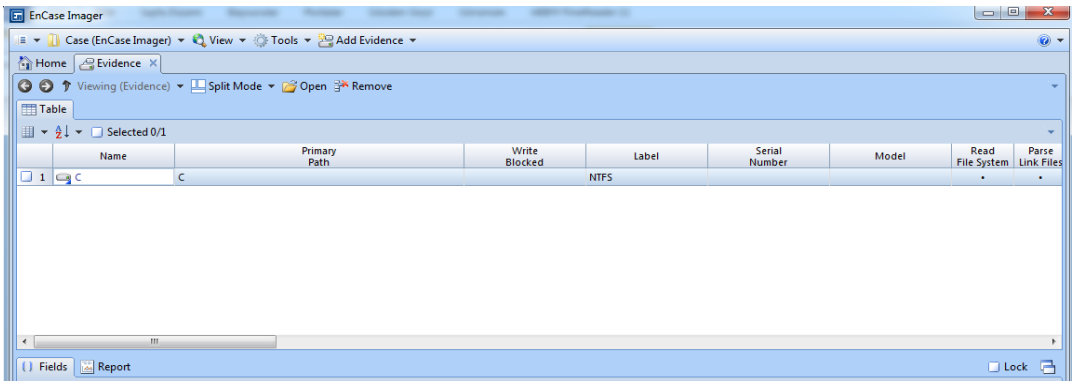
Şekil 2.15 Encase Program Arayüzü 2

Sonra gelen pencereden imaj alınacağı fiziksel alan seçilir ve son sekmesine tıklayarak imaj alınacak fiziksel alanı Encase yazılımına eklenir. Encase İmager programını fiziksel alan görüntüsü ve arayüzü Şekil 2.16'de verilmiştir.



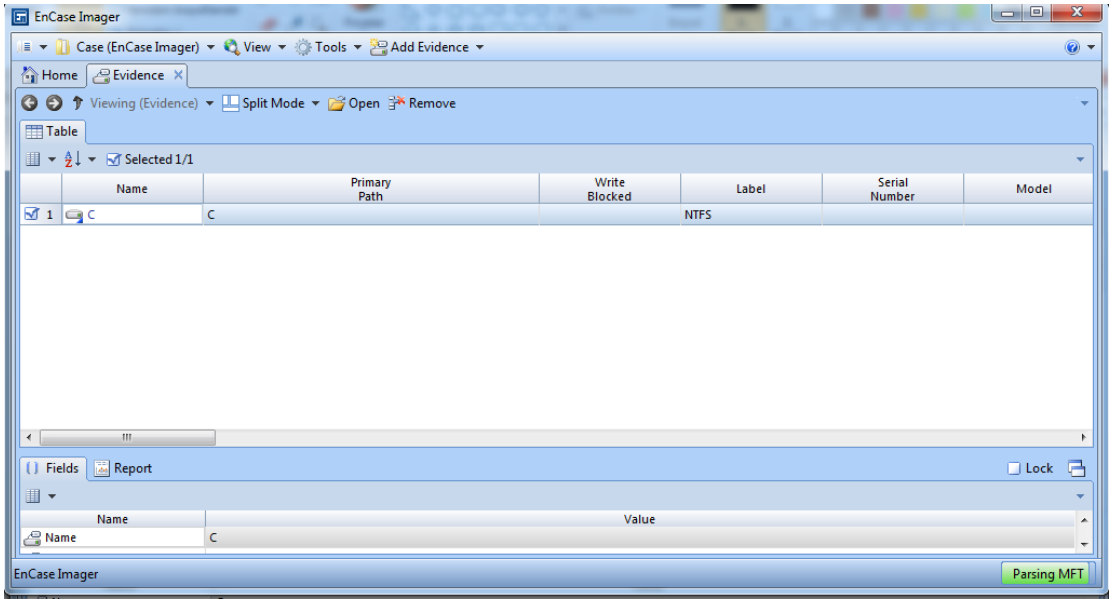
Şekil 2.16 Encase Yazılımı Cihaz Ekleme Arayüzü

Encase yazılımının Programına fiziksel alan eklenmiş olarak çıkmaktadır. Şekil 2.17'de Encase yazılımı üzerine fiziksel alan eklenmiş arayüzü verilmiştir.



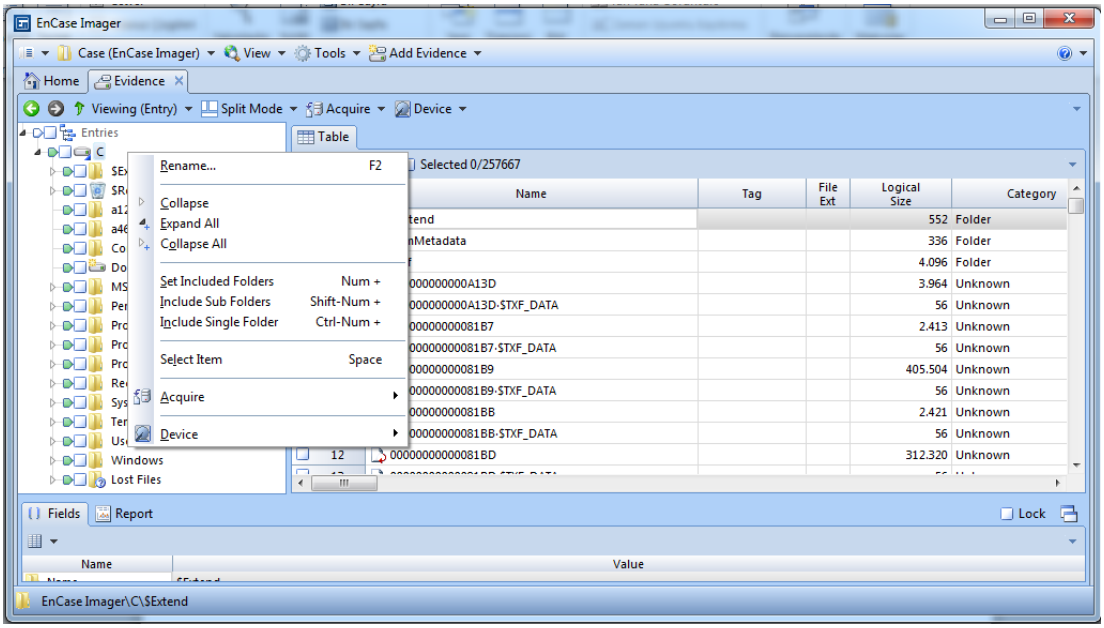
Şekil 2.17 Encase Fiziksel Alan Eklenmiş Arayüzü

Fiziksel alanının üzerine sol çift tıklanarak eklenilen fiziksel alanı Encase Programında doğrulatma yapılır. Doğrulama arayüzü Şekil 2.18'da gösterilmiştir.



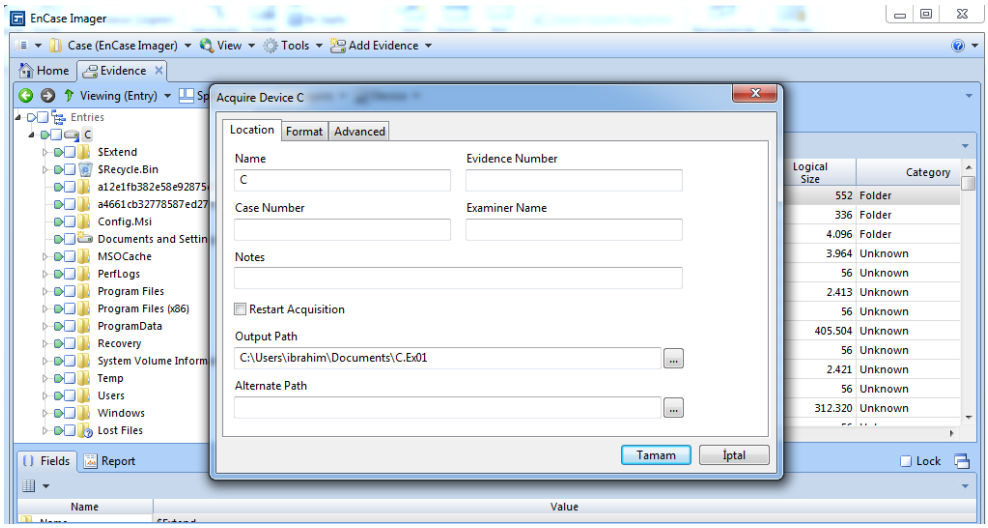
Şekil 2.18 Encase Fiziksel Alma Doğrulama Arayüzü

Sol tarafda ki Girdiler (Entries) bölümüne gelip farenin sağ tuşu ile ekleme (Acquire) sekmesi tıklanır. Encase İmager programını imaj ekleme ekranı Şekil 2.19'de verilmiştir.



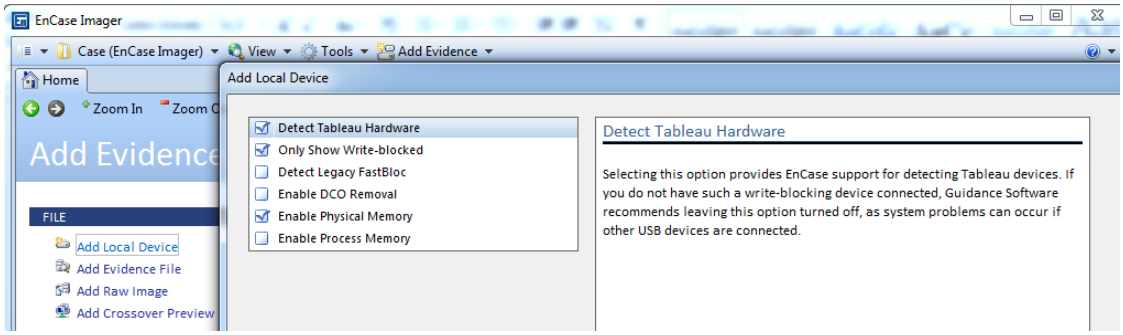
Şekil 2.19 Encase Programı İmaj Ekleme Arayüzü

Yer (Location) bölümündeki İmaj ismi (Name), Kanıt veya Dosya Numarasını (Evidence Number), Olay Vaka Numarasını (Case Number), İmaj alanın ismini (Examiner Name) Çıkış Yolu (Output Path) yani imajı nereye alınacağı seçilir ve tamam sekmesine basılarak imaj alma işlemine başlanır. Alternetif Yol (Alternete Path) tıklayarak imajımı başka bir alana çıkarmak istenilirse bu alanda seçilebilir. Encase İmager programını boşluk alanları doldurma arayüzü Şekil 2.20'de verilmiştir.

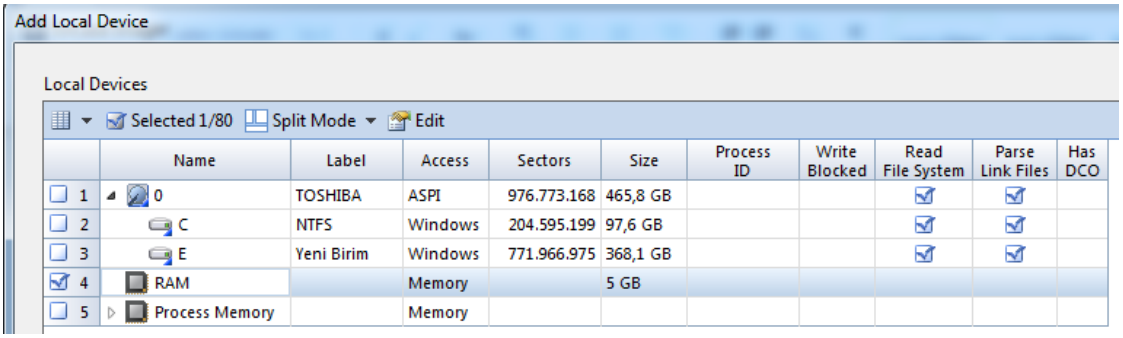


Şekil 2.20 Encase Program Boşlukları Arayüzü

Yerel Cihaz Ekle (Add Local Device) sekmesi tıklanır. Sonra Fiziksel Belleği etkinleştir (Enable Physical Memory) ve İşlem belleği etkinleştir (Enable Process Memory) sekmesini tıklanılarak RAM seçeneğini de seçtikten sonra son sekmesine tıklayarak ram imajı almaya başlanılabilir. Encase İmager programını RAM imajı alma arayüzü Şekil 2.21'de verilmiştir.



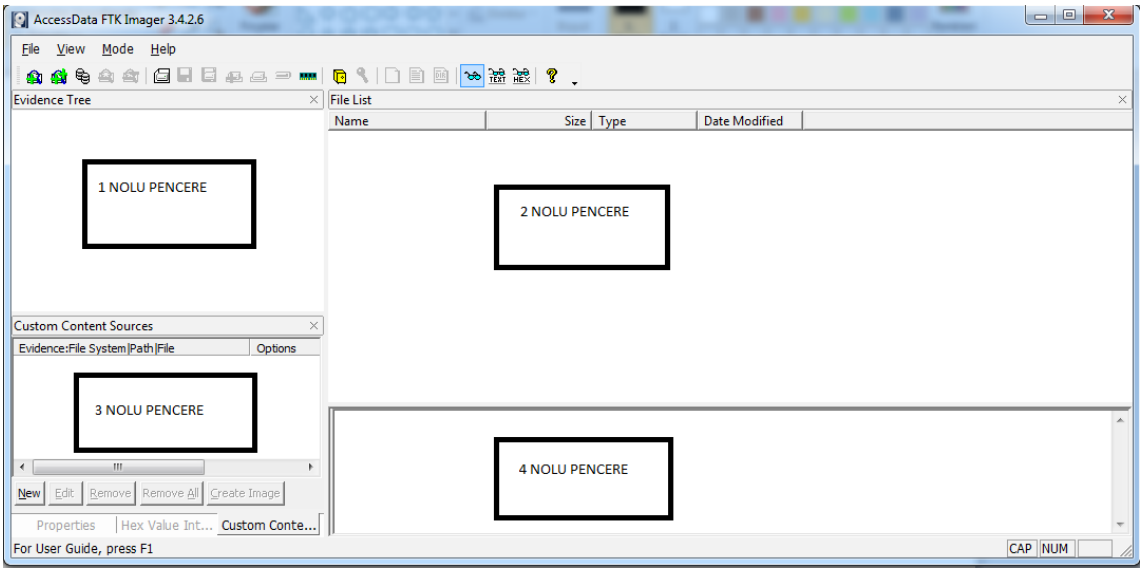
Şekil 2.21 Encase Ram İmajı Ekleme Arayüzü



Şekil 2.22 Encase Ram İmaj Alma Arayüzü

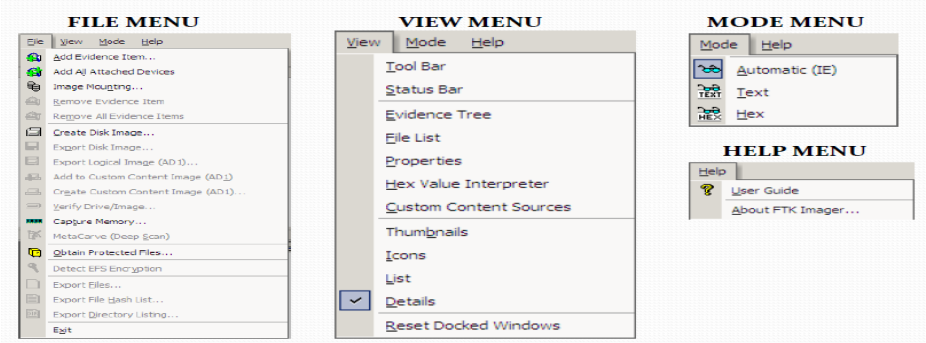
2.22.2.2 FTK (Forensic Toolkit) İle İmaj Alma

FTK Accesdata firması tarafından yazılmış imaj alma ve inceleme programıdır. Hard disk, zip dosyası, CD, den imaj alınabilmektedir. Aynı zamanda RAM imajı da alınabilmekte bu imaj (mount) eklenebilmektedir. Alınan hard disk ve diğer medya araçlarının hash değerleri hesaplanabilmektedir. FTK İmager imajları RAW (dd), Smart, E01 VE AFF uzantısında alabilmektedir. Bu yazılım ile ağ üzerinden imaj alma işlemi yapmak mümkündür. İmajların hash değerleri MD5 ve SHA1 ile hesaplayabilmektedir. FTK İmager programı program sitesinden ücretsiz olarak indirilebilmekte olup, İnceleme programı ücretlidir, inceleme programı Dongle USB ile çalışmaktadır (İnt.Kyn.5). FTK İmager programı ana ekran arayüzü Şekil 2.23'de verilmiştir.



Şekil 2.23 FTK Programı Ana Ekran Arayüzü 1

Dosya Menüsü(File Menü), Manzara Menüsü (View Menü),Mod Menüsü (Mode Menü), Yardım Menüsü(Help Menü) olmak üzere 4 menü bulunmaktadır. Dosya Menüsünün içerisinde imaj alma, RAM imajı alma, alınan imajların kontrol edilmesi gibi bölümler bulunmaktadır. Manzara Menüsünün içerisinde araç çubuğu, durum çubuğu, dosya listesi, simgeler gibi kısımlar bulunmaktadır. Mod menüsünün içerisinde otomatik görünüm kısmı bulunmaktadır. FTK İmager programı ana ekran menüler ara yüzü Şekil 2.24'de verilmiştir.



Şekil 2.24 FTK Menüleri Arayüzü

FTK İmager programı FTK Dosya Menü Açıklama Bilgileri ara yüzü Şekil 2.25 ve 2.26 de verilmiştir.

İlk bulunan sekmede yeni delil ekle sekmesi, sonra bağlı aygıtları ekle sekmesi, imaj mount etme sekmesi, eklenen delilin silinme sekmesi, yeni bir imaj oluşturma sekmesi imajı dışarı çıkart sekmesi, ram imajı al sekmesi dosyaların hash bilgileri sekmesi gibi sekmeler bulunmaktadır.

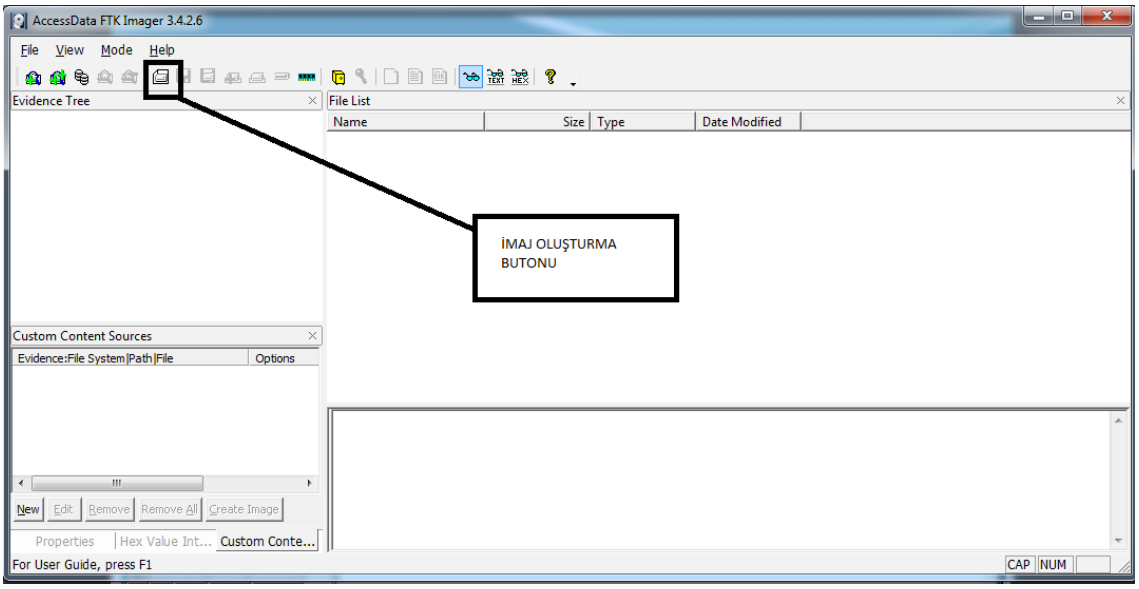
Button	Açıklama
	Add Evidence Item. (Yeni bir delil ekle)
	Add All Attached Devices. (Bağlı tüm aygıtları ekle)
	Image Mounting. (İmajı mount etmek)
	Remove Evidence Item. (Eklenen bir delili sil)
	Remove All Evidence Items. (Eklenen tüm aygıtları sil)
	Create Disk Image. (Yeni bir imaj oluştur)
	Export Disk Image . (İmajı dışarı çıkart.)
	Export Logical Image .(AD1) (Mantıksal imajı dışarı aktar)
	Add to Custom Content Image (AD1) (özel içerik kutusuna ekle)
	Create Custom Content Image (AD1) (özel içerik görüntüsü ekle
	Verify Drive/Image (sürücüyü doğrula)

Şekil 2.25 FTK Menü Açıklama Bilgileri

Butto n	Açıklama
	Capture Memory (rem'in imajını al)
	MetaCarve (Deep Scan) (Metadata bilgilerinin çıkartılması)
	Obtain Protected Files (Korunan sistem dosyalarını almak)
	Detect EFS Encryption (EFS'li dosyları tespit etmek)
	Export Files (Dosyanın aktarılması)
	Export File Hash List (Dosya listelerinin hash bilgileri)
	Export Directory Listing
	Choose IE, text, or hex viewer automatically
	View files in plain text
	View files in hex format
	Open FTK Imager User Guide

Şekil 2.26 FTK Menü Bilgileri 2

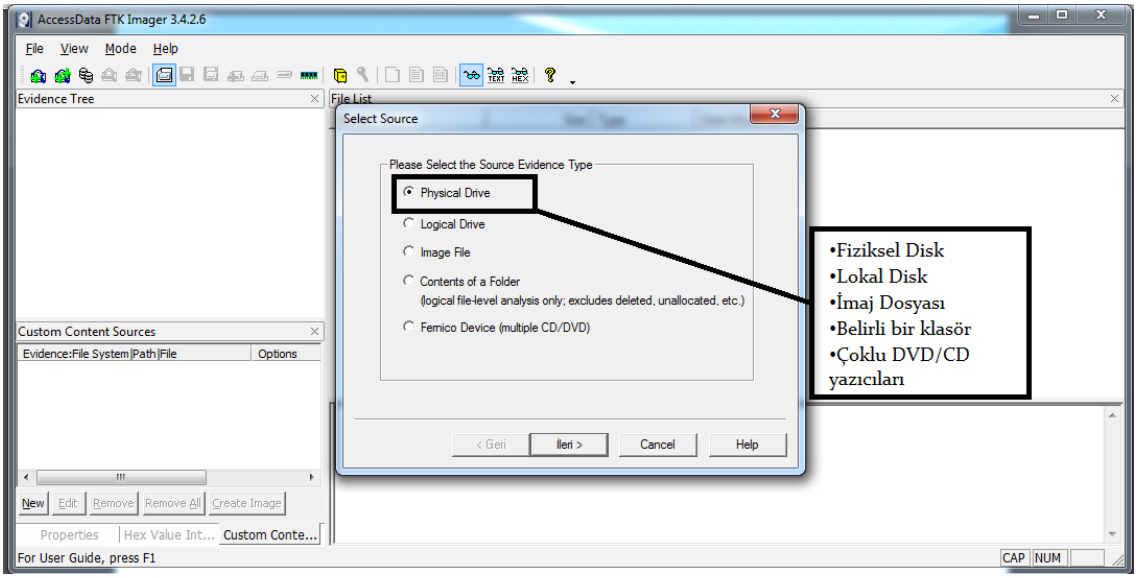
FTK ana ekran yüzü ve FTK İmager programı imaj oluşturma arayüzü şekil 2.27 verilmiştir.



Şekil 2.27 FTK İmaj Oluşturma Sekmesi

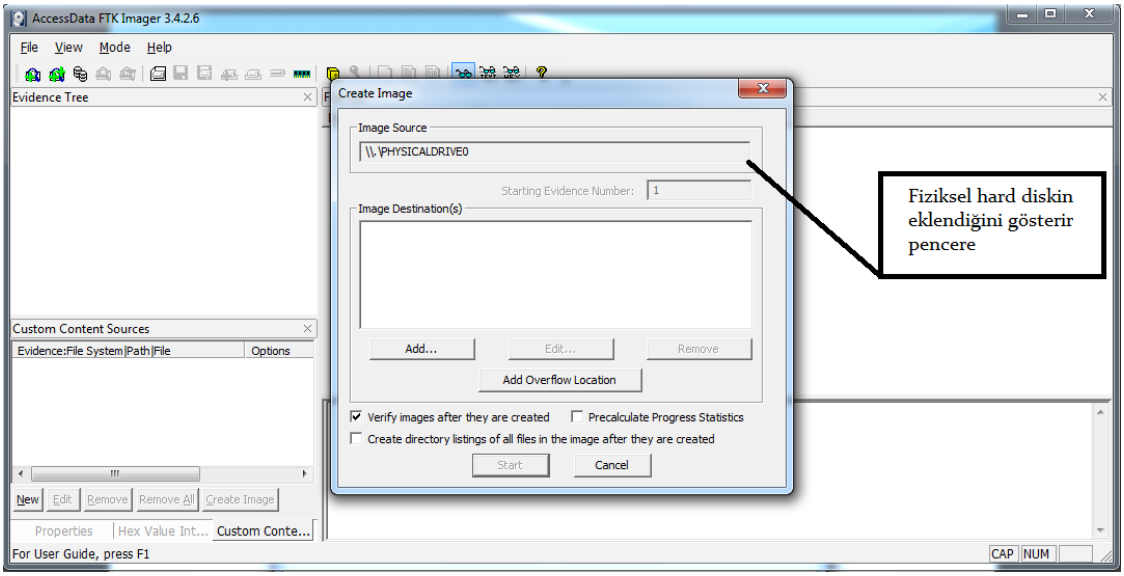
FTK İmager programı İmaj Bağlantı Oluşturma Arayüzü Şekil 2.28'de verilmiştir.

Bu kısımda imajın nasıl alınacağı, imajın alınacağı dijital materyal programa nasıl bağlantı kurulduğu, imaj alınan bir dosyanın mı açılacağı sorulmaktadır.



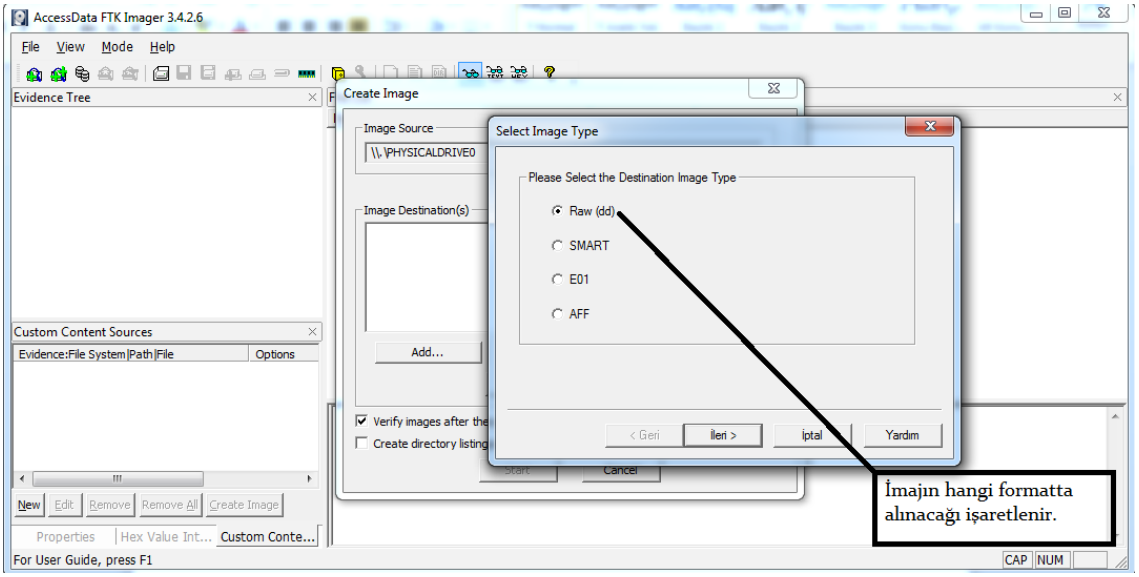
Şekil 2.28 FTK İmaj Bağlantı Oluşturma Arayüzü

FTK İmager programı İmaj Kaynağı (İmage Source) kısmında yazılıma eklenen Fiziksel Harddisk Bağlantı Arayüzü Şekil 2.29'de verilmiştir.



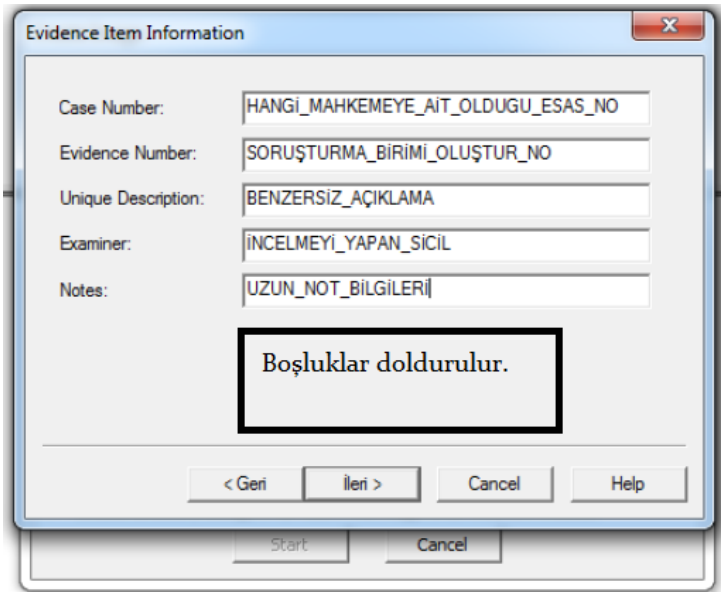
Şekil 2.29 FTK Fiziksel Harddisk Bağlantı Arayüzü

Yukarıda bulunan ADD sekmesine tıklanarak imaj oluşturmaya başlanır. Add sekmesi tıklandıktan sonra imajın hangi formatta alınacağı seçilir ve ileri sekmesine tıklanır.FTK İmager programı İmaj Türü Seçme Sekmesi Arayüzü Şekil 2.30'de verilmiştir.



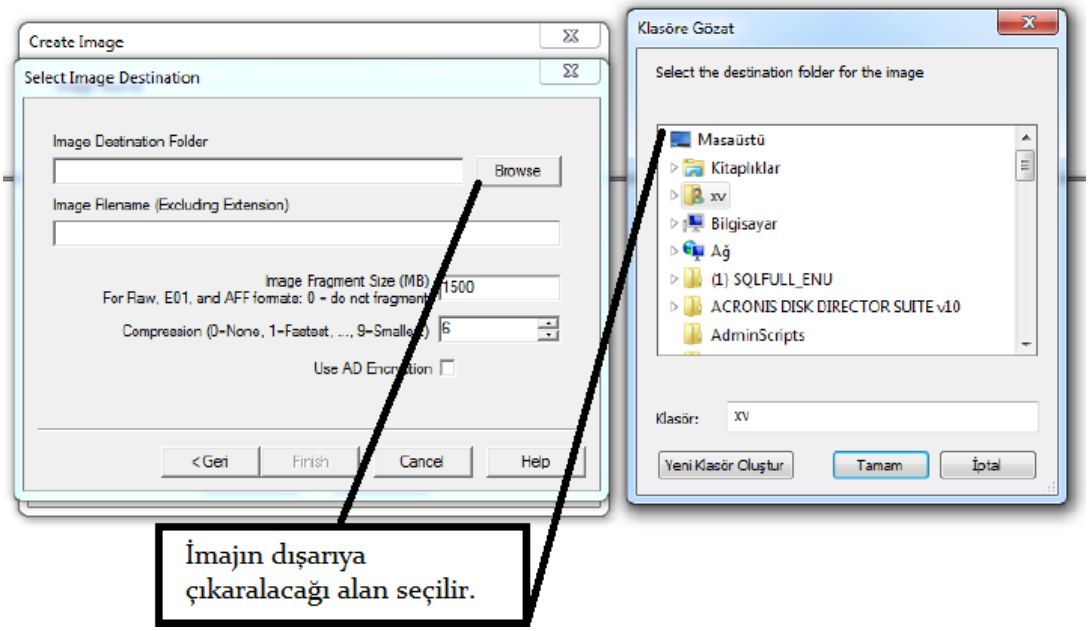
Şekil 2.30 FTK İmaj Türü Seçme Sekmesi

FTK İmager programı İmaj Boşlukları Doldurma Ekranı Arayüzü Şekil 2.31'de verilmiştir.Bu kısımda bulunan olay numarası(Case Number), soruşturma numarası (Evidence Number), benzersiz açıklama (Unique Description), incelemeyi yapan ismi (Examiner) ve not (Notes) kısımları doldurularak ileri sekmesi tıklanır.



Şekil 2.31 FTK İmaj Boşlukları Doldurma Ekranı

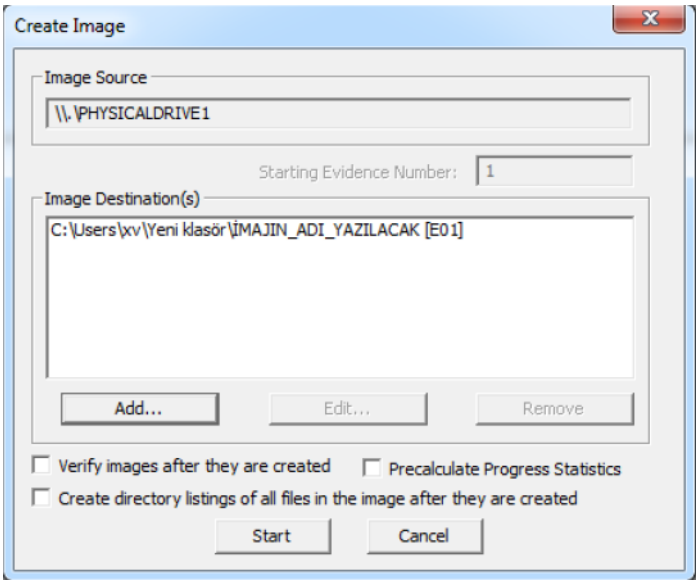
FTK İmager programı İmaj Dışarıya Çıkarılma Arayüzü Şekil 2.32'de verilmiştir. Resim Hedef Klasörü (Image Destination Folder) sekmesinin altında bulunan göz (browse) sekmesi tıklanarak oluşturulan imajın nereye çıkartılacağı seçilir.



Şekil 2.32 FTK İmaj Dışarıya Çıkarılma Arayüzü

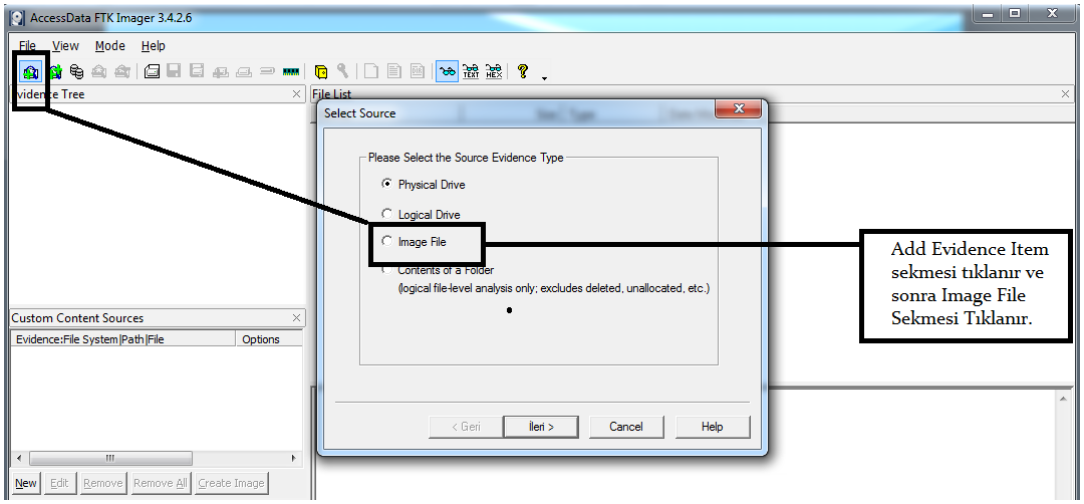
Başlat (Start) sekmesine tıklayarak imaj alınmaya başlanır.

FTK İmager programı imaj başlatma sekmesi arayüzü Şekil 2.33'de verilmiştir.



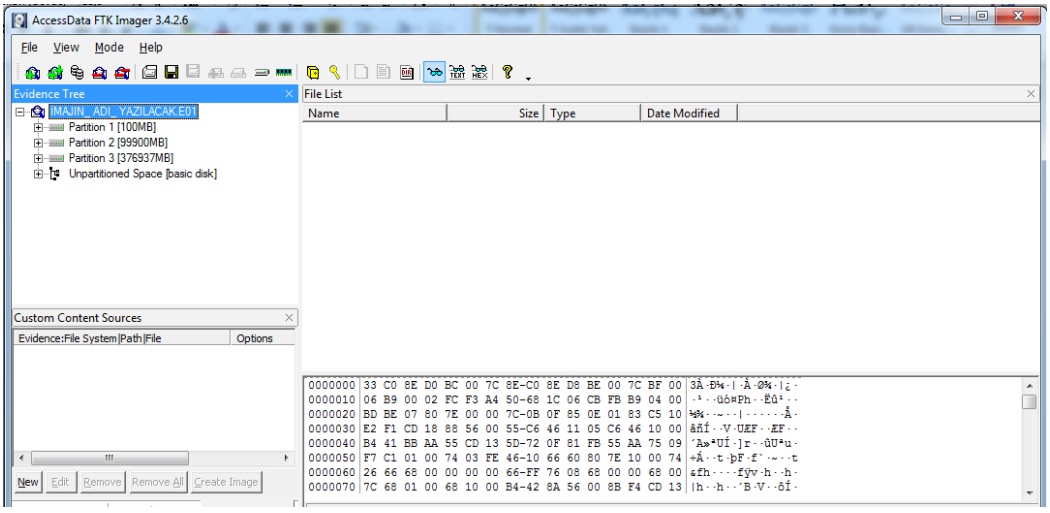
Şekil 2.33 FTK İmaj Başlatma Sekmesi Arayüzü

FTK İmager programında Dosya (File) sekmesi altında bulunan Kanıt Ekle (Add Evidence Item) sekmesi tıklanır. Sonra İmaj Dosyası sekmesine tıklanır. Çıkan Kanıt kaynağı (Evidence Source Selection) seçimi sekmesi tıkladıktan sonra imaj programa tanıtılır ve bitti (Finish) sekmesi tıklanarak programa imaj tanıtılır.Alınan İmajların Kontrol Edilme Arayüzü Şekil 2.34'de verilmiştir.



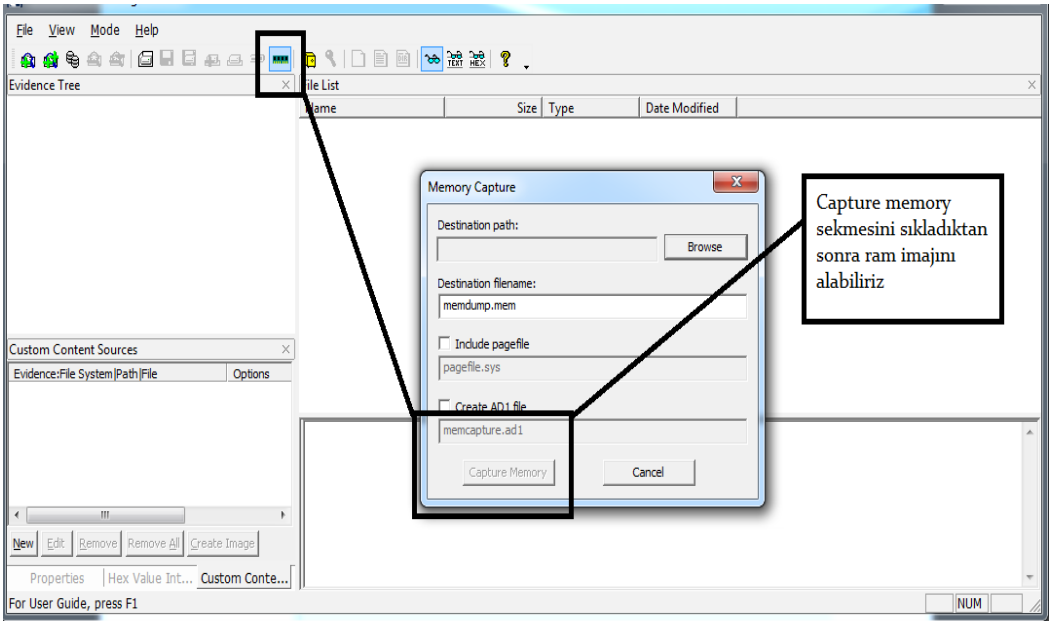
Şekil 2.34 FTK Alınan İmajların Kontrol Edilme Arayüzü

FTK programı sol üst tarafında bulunan Kanıt Ağacı (Evidence Tree) sekmesi altında bulunan imaja tıklanarak alınan imajın FTK programındaki hali Şekil 2.35'da verilmiştir.



Şekil 2.35 FTK Programındaki İmaj

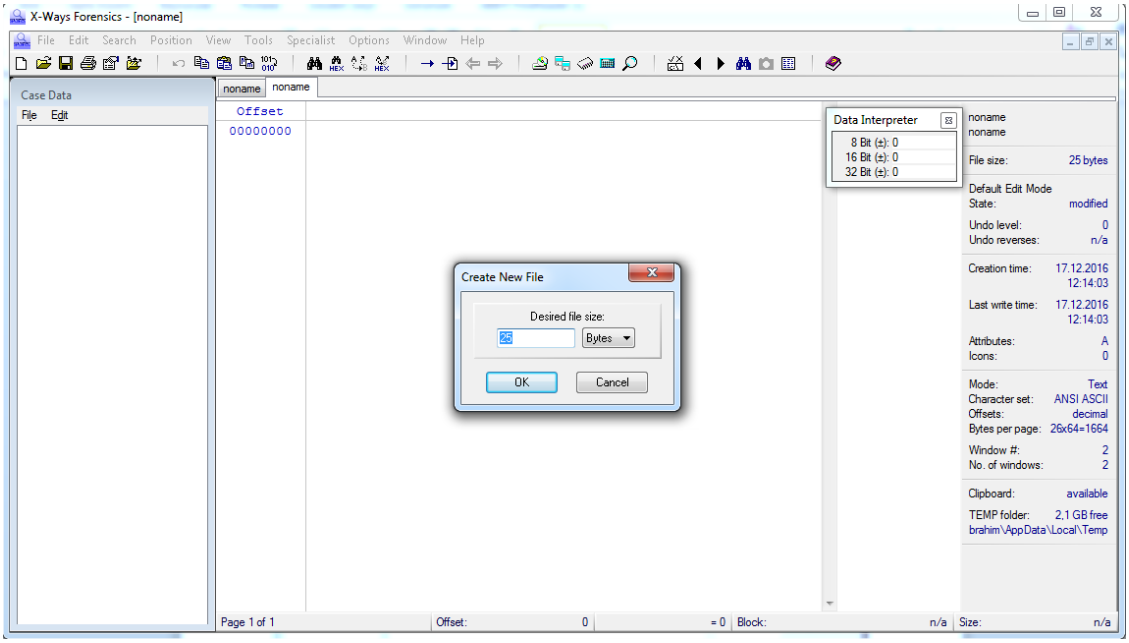
FTK İmager programında Dosya (File) sekmesi altında bulunan bellek (Capture Memory) sekmesine tıklanır. Sonra hedef yolu (destination path) tıklanarak ram imajının nereye alınacağı seçilir. Daha sonra bellek (Capture Memory) sekmesine tıklanarak ram imajı alınmaya başlanır. FTK İmager programını ram imaj alma ekran arayüzü Şekil 2.36'de verilmiştir.



Şekil 2.36 FTK Programı Ram İmaj Alma Ekran Arayüzü

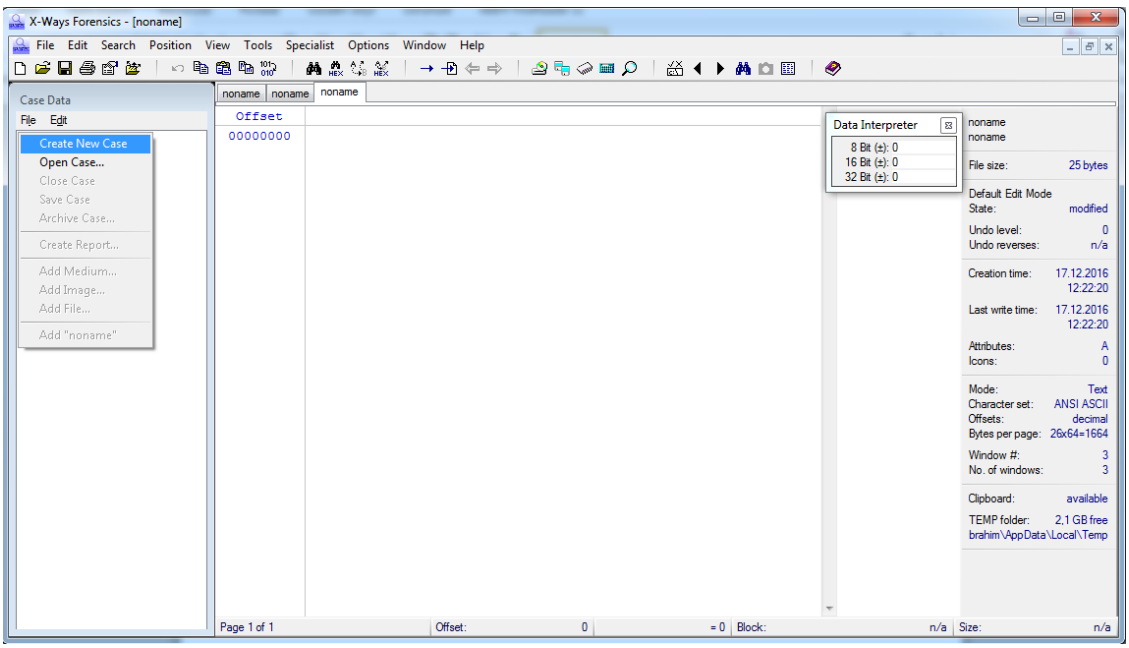
2.22.2.4 X-WAYS Forensic İle İmaj Alma

X-Ways firmasının ürettiği yazılım, hard diskin fiziksel mantıksal alanını görebilmektedir. Sektörleri hex ve metin olarak görebilmektedir. X-Ways forensic İmager yazılımı inernet sitesinden ücretsiz indirebilmektedir (İnt.Kyn.5). Aldığı imajları E.01,Raw, dd Formatında almaktadır.Programın sağ üst köşesinde bulunan Dosya (File) sekmesi içerisinde bulunan Yeni (New) Sekmesine tıkladıktan sonra yeni imajın sektör boyutunu seçilir. X-Ways Forensic imaj sektör boyutu belirleme ekran arayüzü Şekil 2.37' de gösterilmiştir.

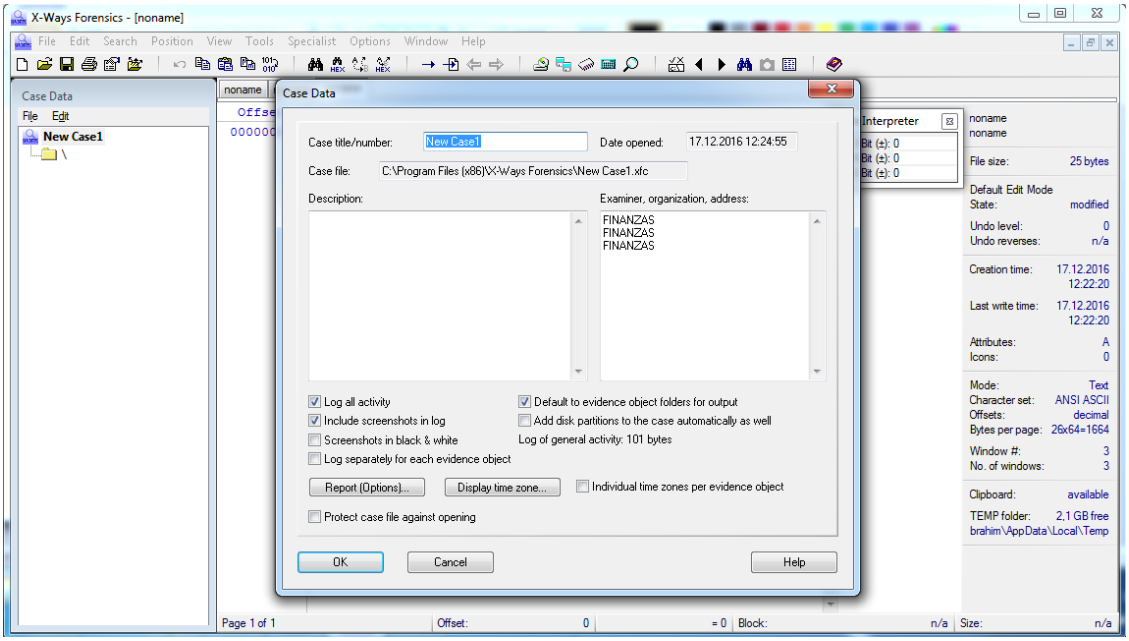


Şekil 2.37 X-Ways Forensic İmaj Sektör Boyutu Belirleme Ekran Arayüzü

Daha sonra Dosya (File) sekmesinden Yeni Vaka Oluştur (Create New Case) sekmesi tıklanır. Yeni Vaka Oluştur (Create New Case) sekmesi içerisinde bulunan Vaka Başlığı (Case Title) yeri doldurulur. Sağ tarafında bulunan İnceleyen adı (Exnaminer) kısmı doldurulur ve tamam (Ok) sekmesi tıklanır. "X-Ways Forensic Yeni Vaka Oluşturma Ekran Arayüzü şekil 2.38 ve 2.39'da verilmiştir.

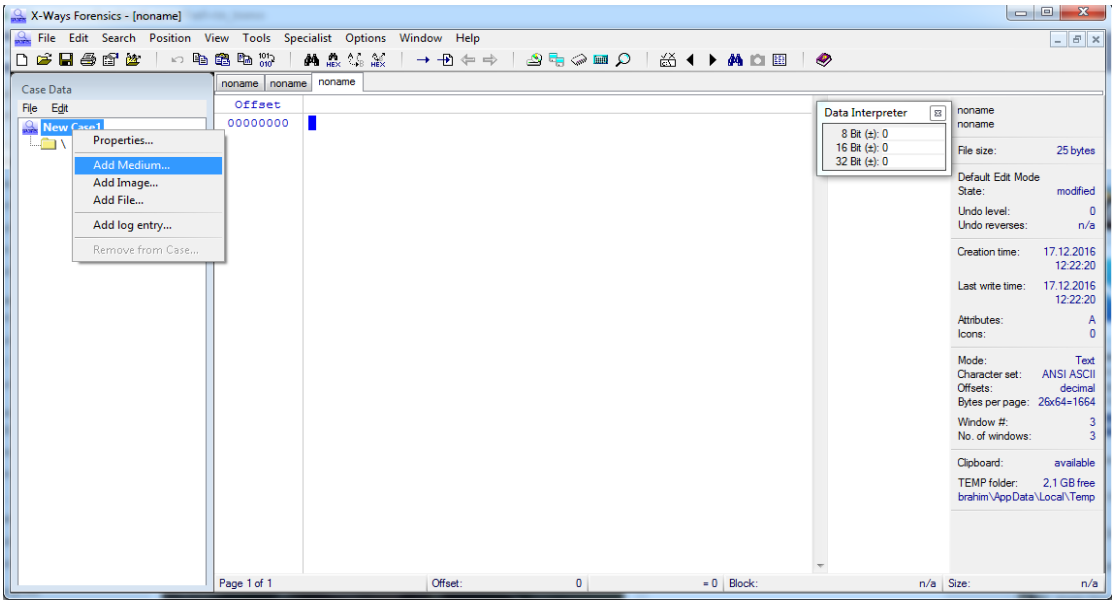


Şekil 2.38 X-Ways Forensic Yeni Vaka Oluşturma Ekran Arayüzü



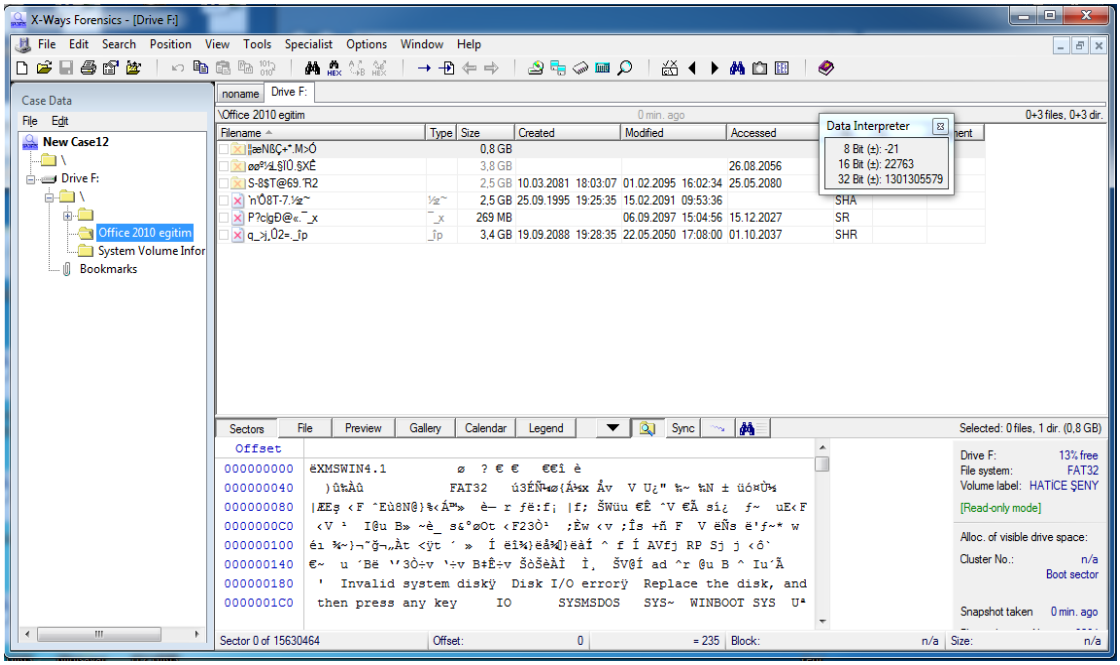
Şekil 2.39 X-Ways Forensic Yeni Vaka İsim Oluşturma Ekran Arayüzü

Cihaz ekle (Add Medium) kısmına tıklanır. X-Ways Forensic Yazılımına Cihaz Ekleme Arayüzü 2 Şekil 2.40 da gösterilmiştir.



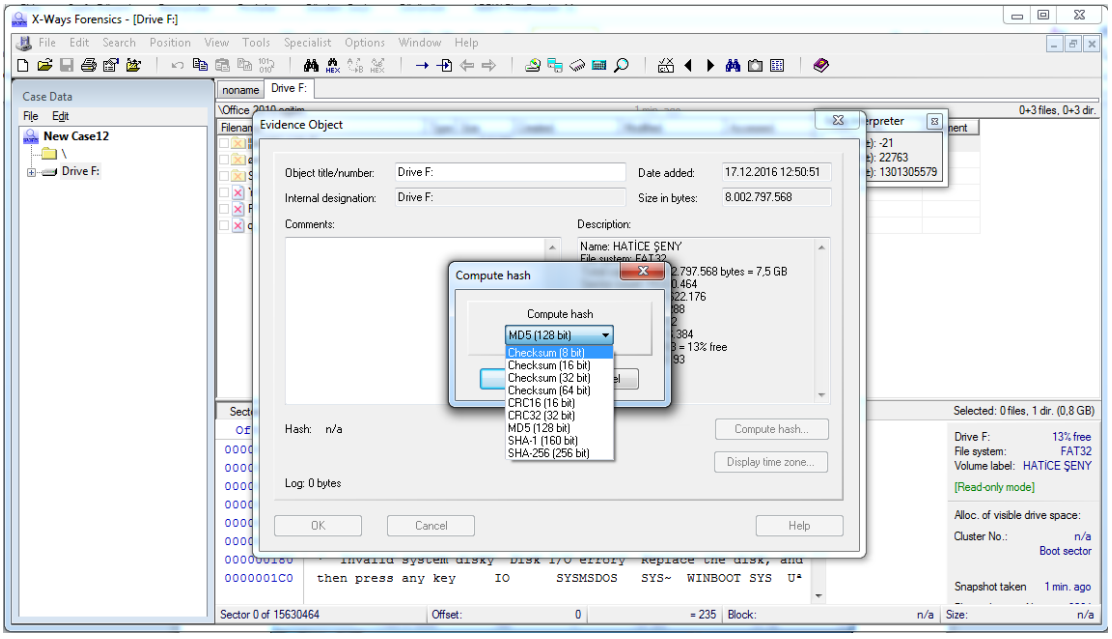
Şekil 2.40 X-Ways Forensic Yazılımına Cihaz Ekleme Arayüzü 2

Add Medium sekmesi tıklandıktan sonra hangi bölümün imajı alınacaksa o bölüm seçilerek tamam (Ok) basılır. X-Ways Forensic Yazılıma Cihaz Ekleme Arayüzü 3 şekil 2.41'de gösterilmiştir.



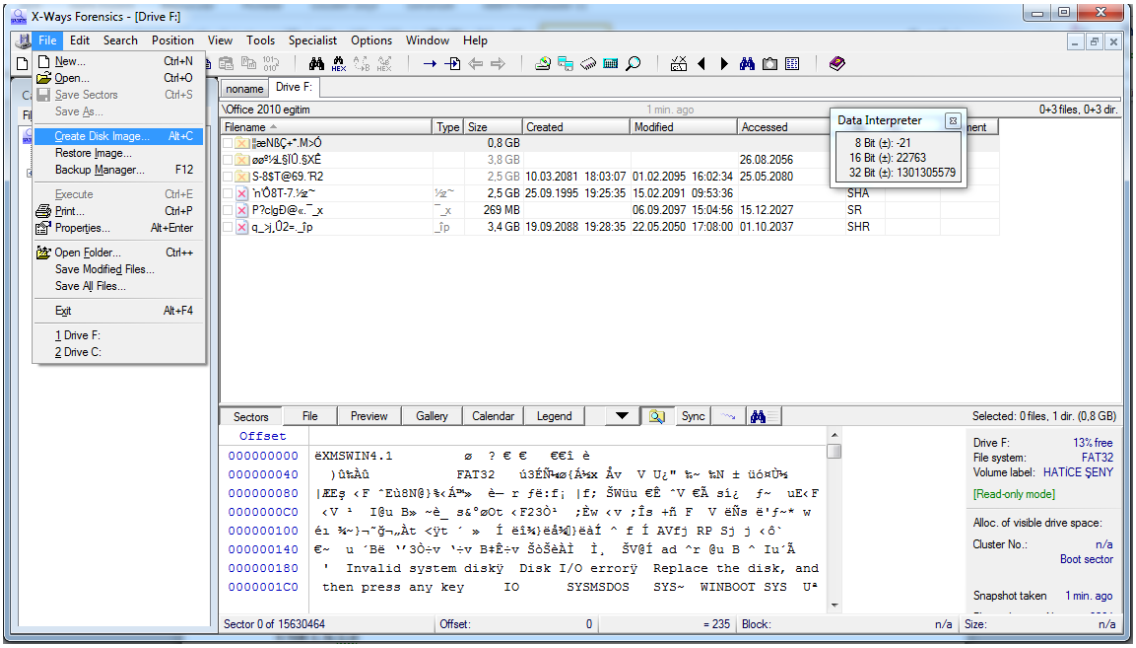
Şekil 2.41 X-Ways Forensic Yazılıma Cihaz Ekleme Arayüzü 3

Yeni oluşturulan vakanın üzerine çift tıklanarak hash değerleri hesaplanabilir. X-Ways Forensic Hash Türü Seçme Arayüzü şekil 2.42'de gösterilmiştir.



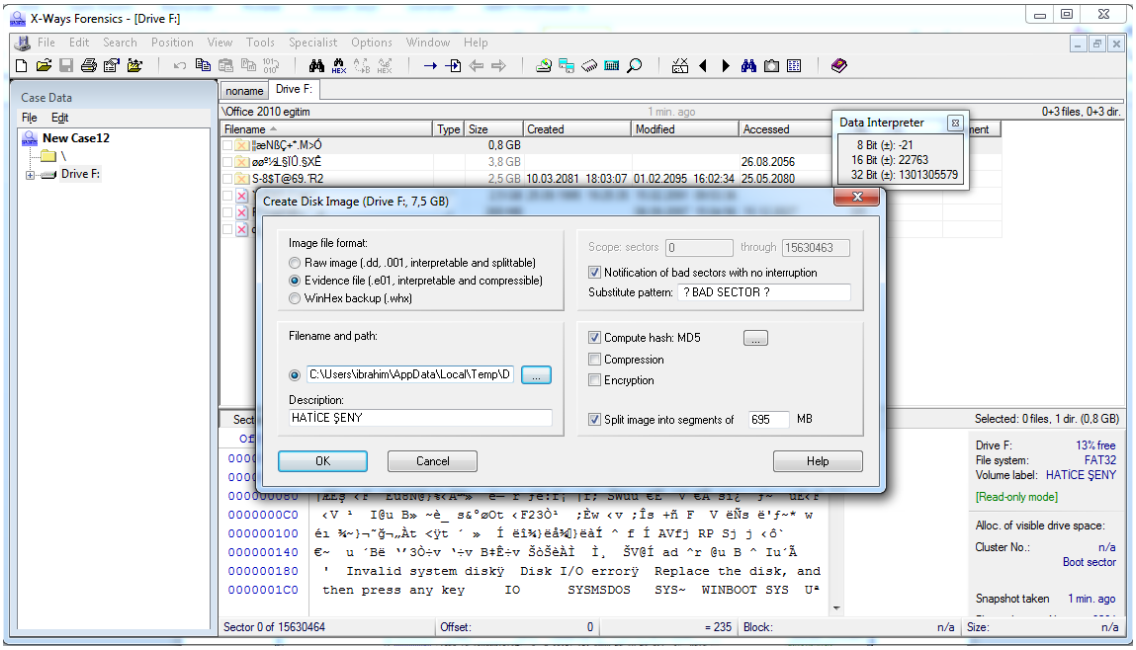
Şekil 2.42 X-Ways Forensic Hash Türü Seçme Arayüzü

Dosya (File) sekmesinden Disk Görüntüsü Oluştur (Create Disk Image) sekmesi tıklanır. X-Ways Forensic İmaj Oluşturma Ekran Arayüzü 1 şekil 2.43'da gösterilmiştir.



Şekil 2.43 X-Ways Forensic İmaj Oluşturma Ekran Arayüzü 1

Görüntü Dosyası (Image File) Formattan İmaj alınacak format belirlenir. Sonra Dosya adı ve yolu (Filename and Path) sekmesinden imajın nereye alınacağı seçilir ve tamam (Ok) dedikten sonra imajı alma işlemine başlanılır. X-Ways Forensic İmaj Bitirilme Ekran Arayüzü şekil 2.44'de verilmiştir.

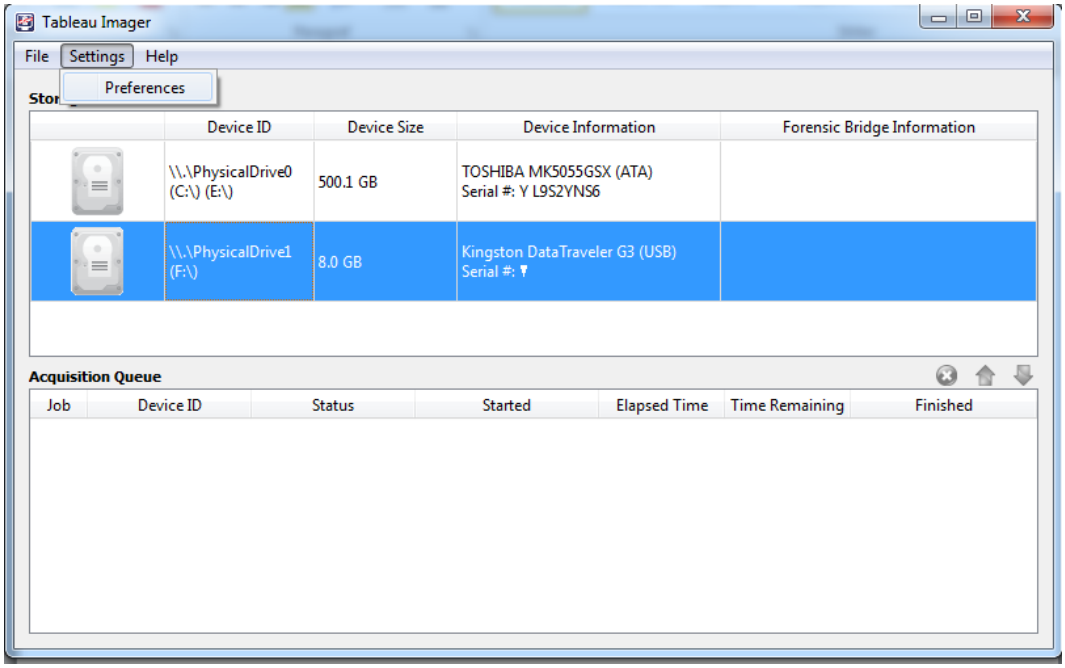


Şekil 2.44 X-Ways Forensic İmaj Bitirilme Ekran Arayüzü

2.22.2.5 Tableau Imager

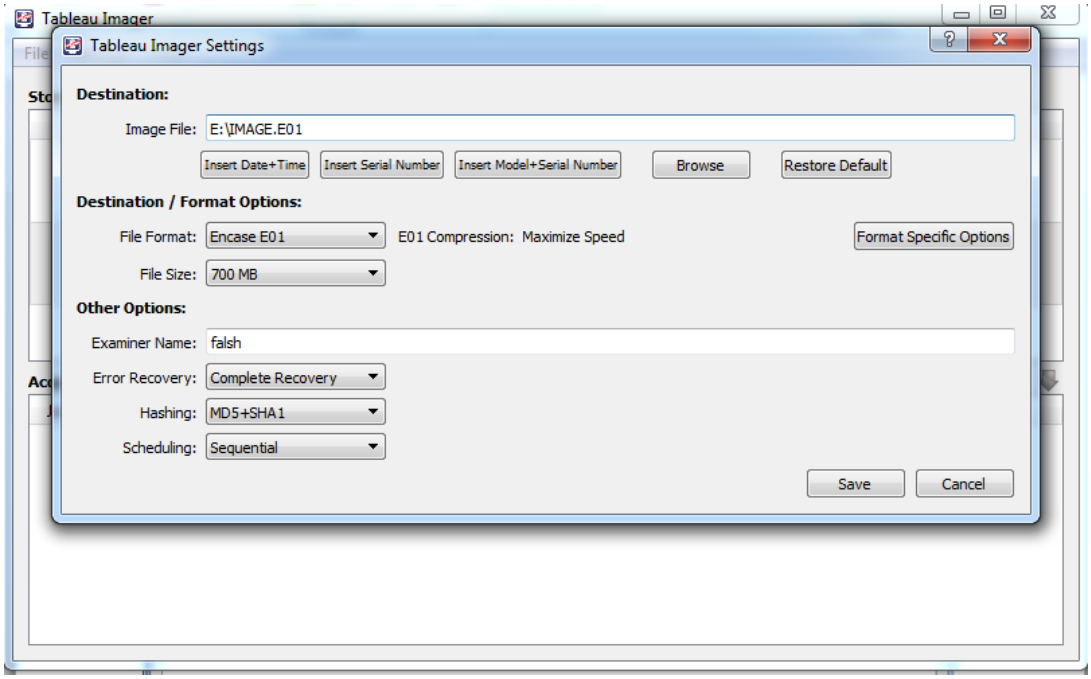
Guidance Software Firmasına ait olan İmaj alma programıdır. Bu program çalıştırıldığında cihaz bilgisi, imaja başlama zamanı, kalan zaman, görevin tamamlama durumu gibi bilgiler görülebilmektedir. Alınan İmajların hash MD5 ve SHA1 ile hesaplayabilmektedir. X-Ways forensic İmTableu Imager yazılımı internet sitesinden ücretsiz indirebilmektedir (İnt.Kyn.7).

Tableau Imager ekranında bulunan ayarlar (Settings) tıklanır. Sonra tercihler (Preferences) sekmesi tıklanır. Tableau Imager arayuz ekranı Şekil 2.45'de gösterilmiştir.



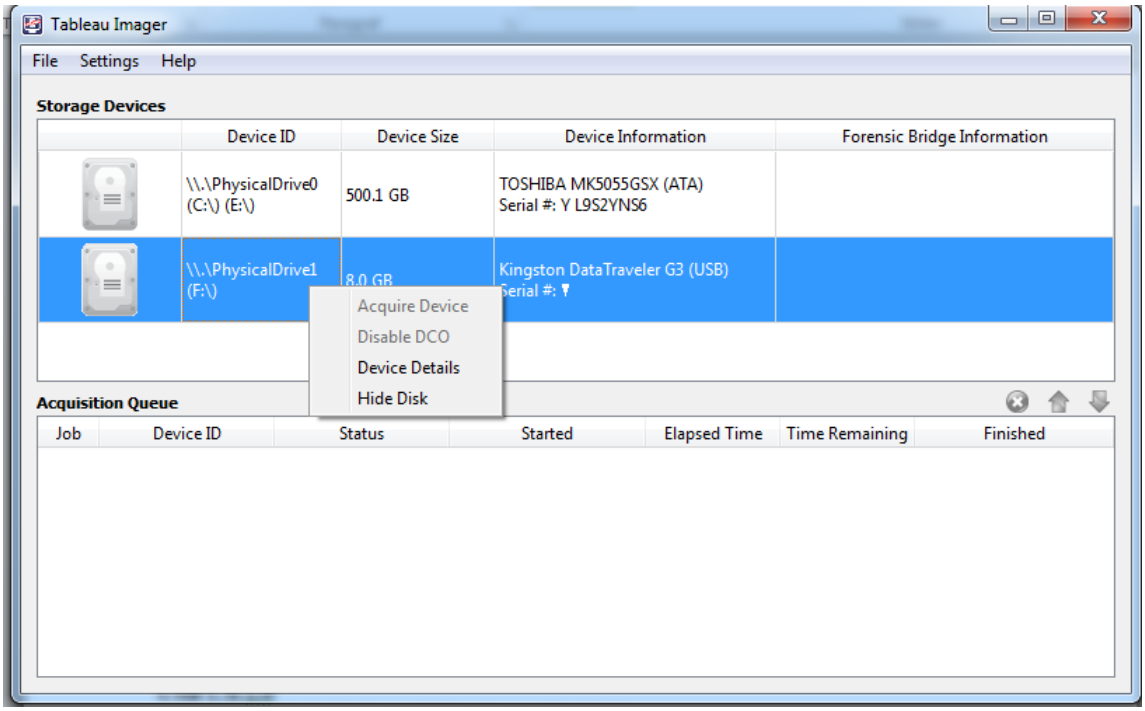
Şekil 2.45 Tableau Imager Arayüzü

Tercihler (Preferences) sekmesi açıldıktan sonra alınacak imajın ismi, tarih ve zamanı, hangi formatta alınacağı, kaç MB alınacağı ve hash format bilgileri yazıldıktan sonra kaydet(Save) sekmesi tıklanır. Tableu Imager bilgileri doldurma ekranı Şekil 2.46'de gösterilmiştir.



Şekil 2.46 Tableau Imager Bilgileri Doldurma Ekranı

Sonra Cihaz Ekle (Acquire Device) tıklayarak imaj alma işlemine başlanır ve imaj alma işlemi bitirilir.İmaj bitirilme ekran arayüzü Şekil 2.47'da verilmiştir.



Şekil 2.47 Tableau Imager Arayüz 1

2.22.2.6 Helix Programı

Çalışan sistemlerde, Linux tabanlı inceleme, imaj alma, Network bağlantılarını tespit etme, Ip adresi bulma gibi fonksiyonları yerine getiren bir yazılımdır. Helix, tamamen adli bilişim sistem incelemeleri için tasarlanmış, hem doğrudan Windows üzerinde çalışabilen uygulamalara, hem de boot edilebilir bir Linux dağıtımı ile, Windows ve Linux sistemleri offline olarak inceleyebilme özelliğine sahip gelişmiş bir yazılımdır. Uçucu verilerin hızlı kolay bir şekilde imaj alınmasını sağlar. Helix Imager programı internet sitesinden ücretsiz olarak indirilebilmektedir (İnt.Kyn.8).

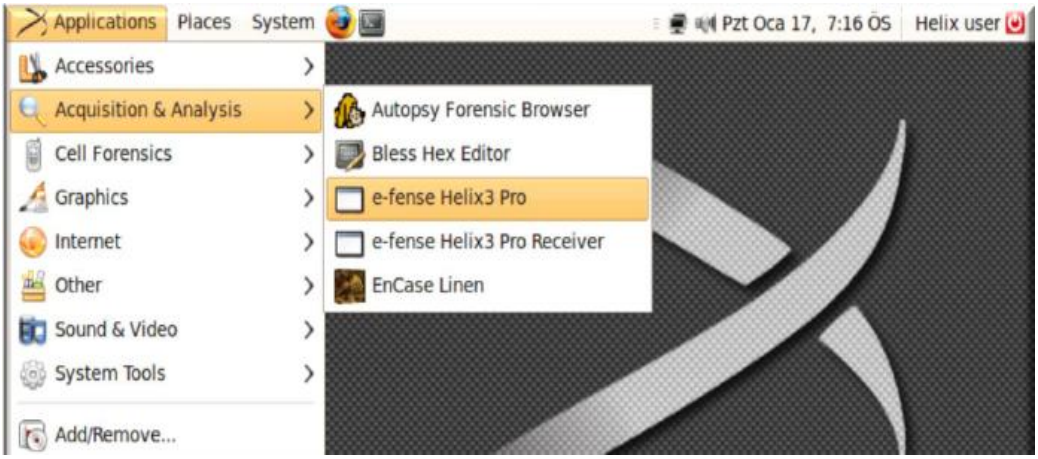
Desteklediği linux versiyonları aşağıda verilmiştir:

1. Fedora,
2. Pardus,
3. Debıan,
4. Ubuntu.

Helix3 Pro'nun özellikleri aşağıda belirtilmiştir. Bunlar;

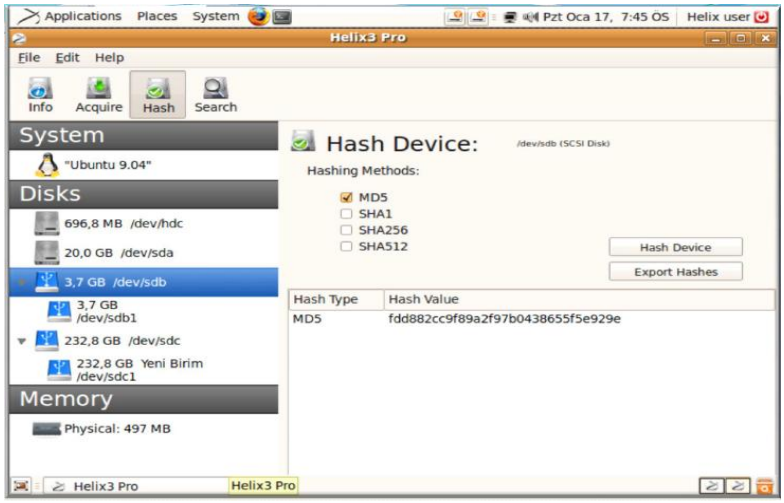
1. Mac OS X, Windows ve Linux gibi yeni bir kullanıcı ara yüzüne sahiptir.
2. Mac OS X dahil çoğu intelx86 makinelerinde çalışır.
3. Güvensiz 3.parti imaj alma araçlarına göre daha güvenilir özelliklere sahiptir.
4. Adli bilişim ile ilgili imaj alma araçlarının çoğunu herhangi bir harici kütüphaneye ihtiyaç duymadan barındırır.
5. Uçucu verilerin hızlı kolay bir şekilde imaj alınmasını sağlar.
6. Yeni adli bilişim araçlarını çalıştırabilecek kapasiteye sahiptir
7. Silinmiş dosyaları kurtarır ve görür.
8. Tüm grafik dosyalarını gösterir.
9. Sistem log dosyalarının imajını alır.
10. CDROM ve USB'den kullanılabilir.
11. Ram analizi yapar ve Ram üzerinde canlı arama yapılabilir.
12. Tüm çalışan prosesleri gösterir. (rootkit tarafından gizlenen dosyalar dahil)
13. Hafızadaki yüklü sürücülerin tamamını tanımlar (rootkit tarafından gizlenen dosyalar dahil)ç
14. Sürücü ve aygıtları raporlar ve yüklenen tüm kernel modüllerini tanımlar.

Helix 3 programı arayüzü şekil 2.48'de verilmiştir. Program açıldıktan sonra Uygulamalar (applications) sekmesi sonra Analiz (acquisition Analysis) daha sonra E-fense Helix3 Pro sekmesi tıklanır.



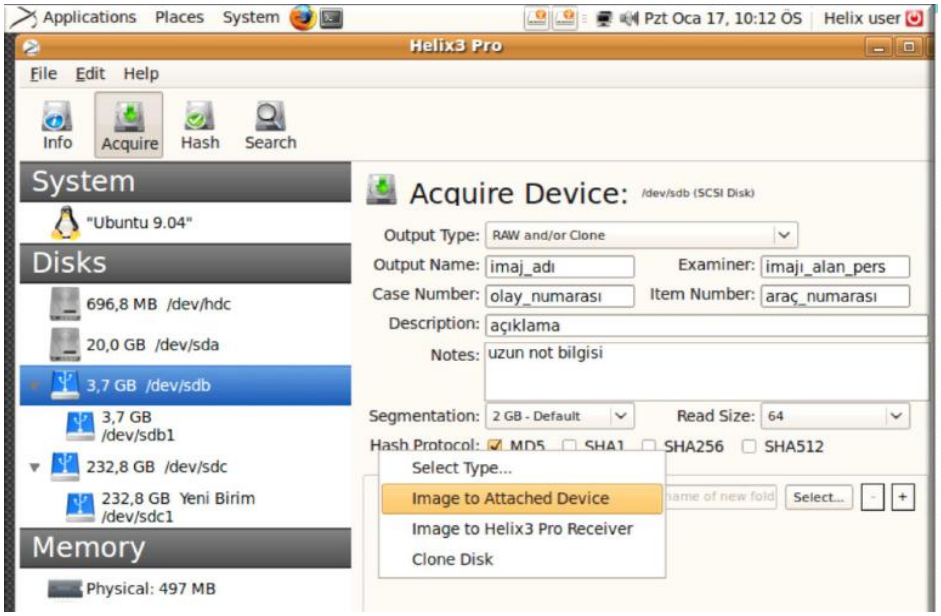
Şekil 2.48 Helix Programı Arayüzü

Sonra imaj alınmak istenilen dijital materyal ve hash türü seçilir. Sol tarafta bulunan disk (Disk) sekmesi içerisinden imajı alınmak istenilen dijital materyal seçilir. Sonra Hash Aygıtı kısmı (Hash Device) alanından hangi tür hash almak isteniliyorsa o çentik tıklanır. Hash aygıtı (Hash Device) kısmına tıklanarak imajı alınmak istenilen dijital materyalin hash hesaplaması yapılır. Şekil 2.49'de Helix programı imaj alınacak metaryal ve hash türü seçme arayüzü verilmiştir.



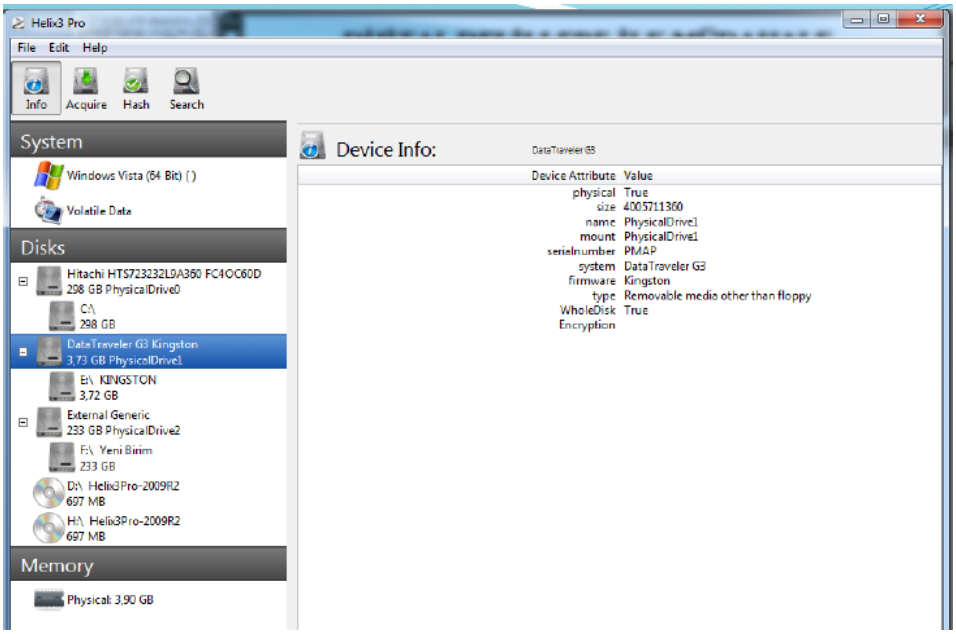
Şekil 2.49 Helix Programı İmaj Alınacak Metaryal ve Hash Türü Seçme Arayüzü

Boşluklar doldurulur ve bağlı aygıtı görüntüle (Image to Attached Device) sekmesi tıklanır. Şekil 2.50'da Helix programı boşluk doldurma arayüzü verilmiştir.



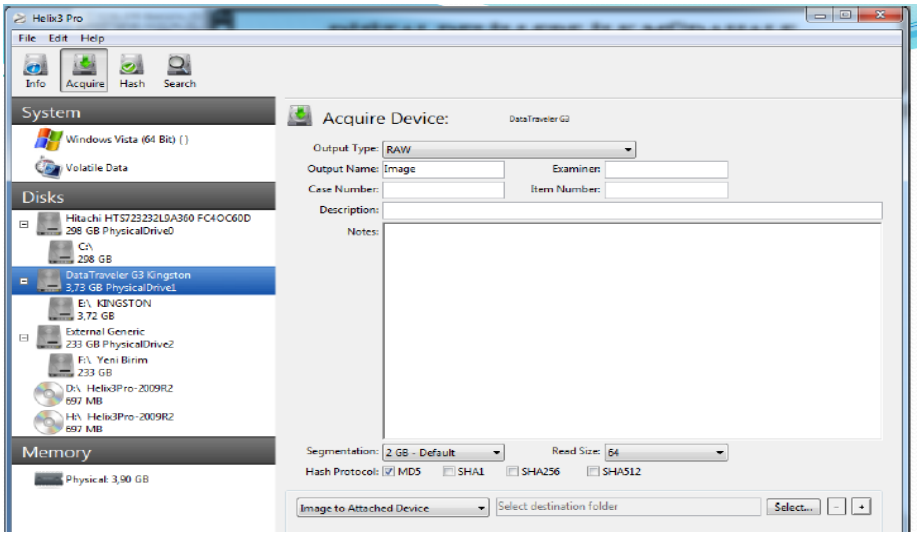
Şekil 2.50 Helix Programı Boşluk Doldurma Arayüzü

Sol tarafında bulunan imaj alacağımız ögeye tıkladıktan sonra ekleme (Acquire) sekmesi tıklanır. Şekil 2.51'de Helix Programı Microsoft Arayüzü gösterilmiştir.



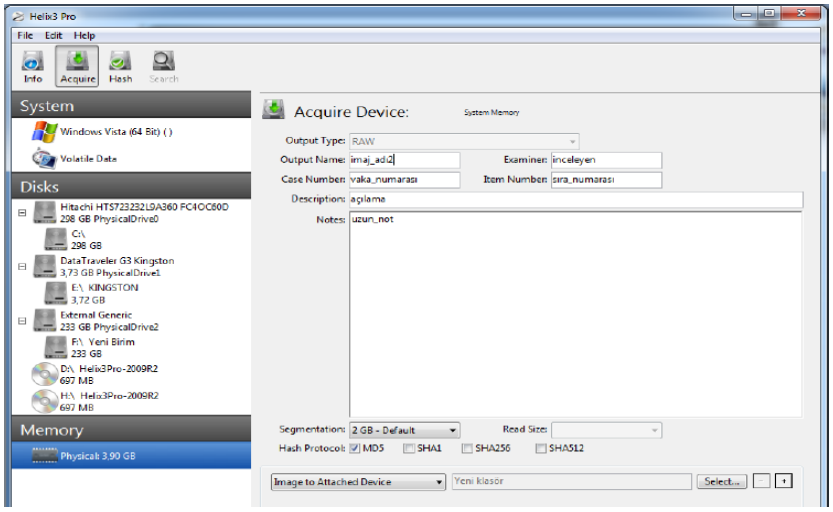
Şekil 2.51 Helix3 Programı Microsof Arayüzü

Çıktı türü (Output Type) sekmesi tıklanarak imajın hangi formatta alınacağı seçilir ve boşlukları doldurduktan sonra edinmeyi başlat (Start Acquistion) sekmesi tıklanarak imaj alma işlemine başlanılabilir. Şekil 2.52 Helix3 Programı Microsoft cihaz ekleme ekran arayüzü gösterilmiştir.



Şekil 2.52 Helix3 Programı Microsoft Cihaz Ekleme Ekran Arayüzü

Helix3 pro ana ekranında bulunan bellek (Memory) sekmesine tıklanır boşluklar doldurulur ve edinmeyi başlat (Start Acquistion) sekmesi tıklanılarak RAM imaj alma işlemine başlatılabilir. Şekil 2.53'de Helix3 Programı Ram imajı alma ekran arayüzü verilmiştir.



Şekil 2.53 Helix3 Programı Ram İmajı Alma Ekran Arayüzü

2.22.2.7 Write Blocker Ultrakit

UltraBlock disk sürücüsünü harici bir donanım olarak kişisel bilgisayarımıza yazma korumalı olarak bağlayarak içerisinde inceleme ve analiz yapmamıza yarayan fiziksel bir aygıttır.

UltraBlock'lar kullanıcı isteğine bağlı olarak salt okunur ya da yazılabilir konuma getirilerek de kullanılabilir. UltraBlock'lar desteklediği aygıtlara aşağıda belirtilmiştir.

1. Serial ATA (UltraBlock-SATA),
2. SCSI (UltraBlock-SCSI),
3. Host PC via FireWire400(1394A),
4. FireWire800 (1394B),
5. USB 1.X/2.0,
6. SD ve MMC

2.22.2.8 Ultrakit Çantası

UltraBlock, UltraBlock USB, UltraBlock FCR olmak üzere parçadan oluşan bağlantı kabloları, bilgisayar bağlantısı ile imaj almada kullanılan Forensic araçlarının başında gelmektedir.

UltraKid içerisindeki Ekipmanlar ile IDE, SATA, SCSI hard disklerin, USB aygıtlarının 2,5' inç 1,8 inç Hard disklerin, SD ve MMC kartların imajlarının alınması mümkündür.

2.22.2.9 Bilgisayara Bağlantı

UltraBlock'lar bilgisayara iki tür bağlantı tipi ile bağlamak mümkündür. Bağlantılar FireWire (400, 800) ya da USB bağlantısıdır. Birden fazla UltraBlockda birbirlerine bağlanarak USB Bağlantısı üzerinden bilgisayara bağlantı kurulması da mümkündür. UltraBlock'lar FireWine400 veya FireWire800 bağlantı kablosu ile birbirlerine bağlantı yapıldıktan sonra USB kablosu aracılığı bilgisayara bağlantı yapılmak suretiyle çoklu UltraBlock kullanılması da mümkündür.

2.22.2.10 Sürücüler (Drivers)

Ultra Block kullanımın da bilgisayarımıza herhangi bir sürücü yüklememize gerek yoktur. IDE, SATA, SCSI ve SDMMC aygıtlar için tüm sürücü desteği otomatik olarak sağlanmaktadır. Win98 işletim sistemleri için sürücü desteğine ihtiyaç duyulmaktadır. Tableu Marka sürücü örneği Şekil 2.54'de verilmiştir.

Şekil 2.54 Tableu Marka sürücü örneği

2.22.2.11 TD1 İmaj Alma Cihazı

TD1 Adli bilişim standartlarına uygun olarak adli makamlara sunulmak üzere diskin imajının (adli kopyasının) alınmasında kullanılan temel araçlardan biridir. Diğer kopyalama araçlarına ek olarak TD1 daha çok adli bilişim uygulamaları açısında özel yeteneklere sahip bir cihazdır. TD1 dakikada 4 GB'ye kadar veri kopyalama hızını destekleyen çok hızlı bir veri kopyalama aygıtı olmasının yanında girdi ve çıktı olarak SATA ve IDE sabit diskleri destekleyen çok yönlü bir araçtır. Alınan imajlarda parmak izi olarak da adlandırılan diskin bütünlüğünü doğrulayan ve günümüzde en yaygın olarak kullanılan ve uluslararası nitelikte geçerliliği olan HASH algoritmalarından MD5 ve SHA-1 HASH değerlerini hesaplayarak rapor halinde bizlere sunar. Çizelge 2.2 'de verilmiştir.

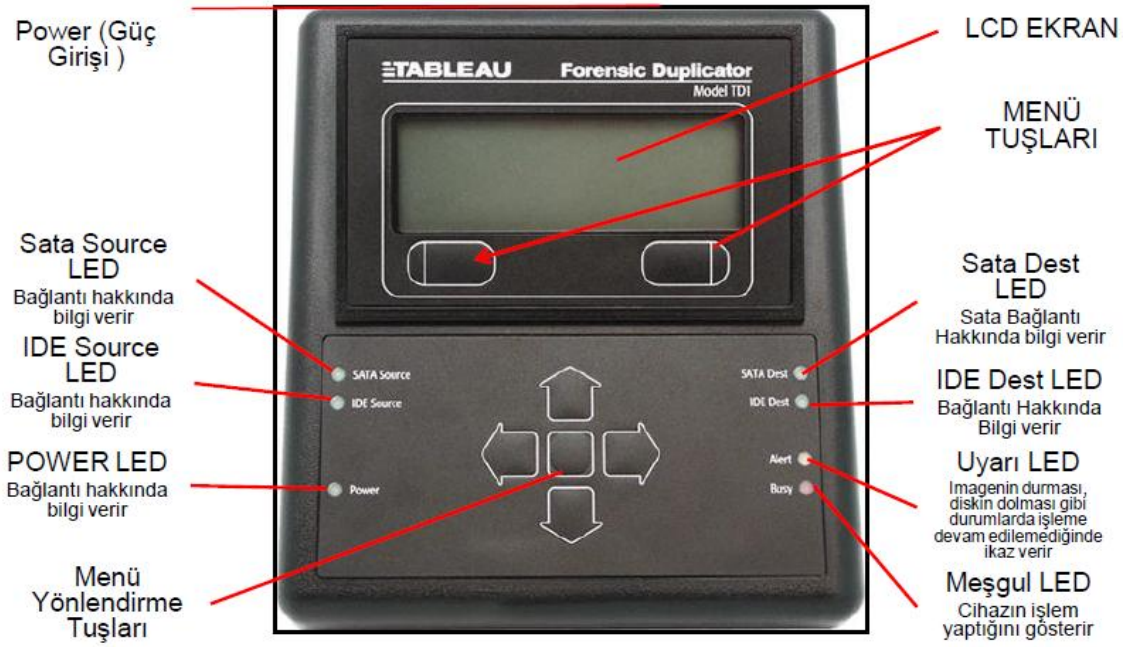
Çizelge 2.2 Tableu marka TD1 imaj alma cihazı tanımlar 1

Ürün Resmi	Tableu Model	Açıklama
	Td1	Dublicatior Genel Menüsü
	TP-3 NC	T01 ile kullanılan yüksek çıkışlı güç kaynağı, TP3 kaynak ve hedef sabit diskler için en yaygın kombinasyonları sağlamak için yeterli güç sağlar.TP3 evrensel 2-pinli AC hattı kablosunu kullanır ve 110-240VAC hat gerilimi ile dünya çapındaki tüm şebekeler için uyumludur
	TP2-LC-US	Kuzey Aınerika için üretilmiş TP3-NC güç kaynağı ile kullanım için TP 2-LC-ABD AC hat kablosu
	TC2-8	"iDE-TiPi " güç kablosu (2 adet).
	TC5-8	"SATA-TiPi" güç kablosu (2 adet).

Tableu Marka TD1 İmaj Alma Cihazının sol kısmında bulunan Kaynak (Source) kısmına imajı alınmak istenilen hard disk takılır. Sağ kısmında bulunan Hedef (Dest) kısmına ise boş olarak imajın alınacağı hard disk takılır ve imaj alınma işlemine başlanabilir. Tableu Marka TD1 imaj alma cihazı görüntüsü 2.55'de verilmiştir

Şekil 2.55 Tableu Marka TD1 İmaj Alma Cihazı Görüntüsü

Tableu Marka TD1 İmaj Alma Cihazı Tuş Bilgileri Şekil 2.56'de verilmiştir.



Şekil 2.56 Tableu Marka TD1 İmaj Alma Cihazı Tuş Bilgileri

Tableu Marka TD1 ile 2 tür kopyalama işlemi gerçekleştirilmektedir.

Birinci işlem Diskten Diske (Disk-to-Disk) Kaynak disk içerisindeki tüm verilerin olduğu gibi başka bir diske tüm sektörleri ile kopyalanmasını içerir. Diğer bir ifade ile klonlamadır. Delil olarak kullanılmaz. Disk sahibi ya da avukatına istemesi halinde imajın bir kopyasını verirken imaj diskinin klonlanmasında kullanılır. Sonunda HASH değeri verilmez.

Diskten Diske kaynak (Source) bölümündeki diskin hedef (Destination) bölümündeki diske sektör sektör tüm diskin birebir kopyalanmasıdır. Kaynak Disk (Source Disk'in) Hedef Diske (Dest Diske) Diskten Diske (Disk-To-Disk) seçeneği ile kopyalanması TD1'in LCD ekranında yukarıda belirtilen şekilde her iki diskinde doğru olarak bağlandığından ve cihazın diskleri tanıdığından emin olduktan sonra "Start" menüsünden kopyalama başlatılır. Start seçeneğine basıldıktan sonra kopyalamaya başlayacak ve kopyalama ile ilgili özet bilgi verilecektir.

İkinci işlem Diskten Dosyaya (Disk-to-File) seçeneğidir.

Kaynak disk içerisinde bulunan tüm veriler hedef diske dosyalar halinde aktarılır. Bu seçenekte hedef diskin boyutuna göre birden fazla kaynak diskin imajı hedef disk içerisine aktarılması sağlanabilir. Delil olarak kullanılır. Sonunda bir HASH değeri verilir Diskten Dosyaya (Disk to File) Kaynak (Source) kısmı bölümündeki diskin Hedef (Dest) bölümündeki diske sektör sektör tüm diskin imaj olarak dosyalar halinde kopyalanmasıdır.

2.22.2.12 TD1 İmaj Alma Cihazı İle Format

TD1 ile Hedef (Destination) disk olarak bağlanan (SATA veya IDE) veya USB portundan bağlanılan USB belleklerin formatlanabilmektedir.

Formatlama işlemi SATA ve IDE hard diskler veya Usb belleklerin için FAT32 File Sistemine göre yapılmaktadır.

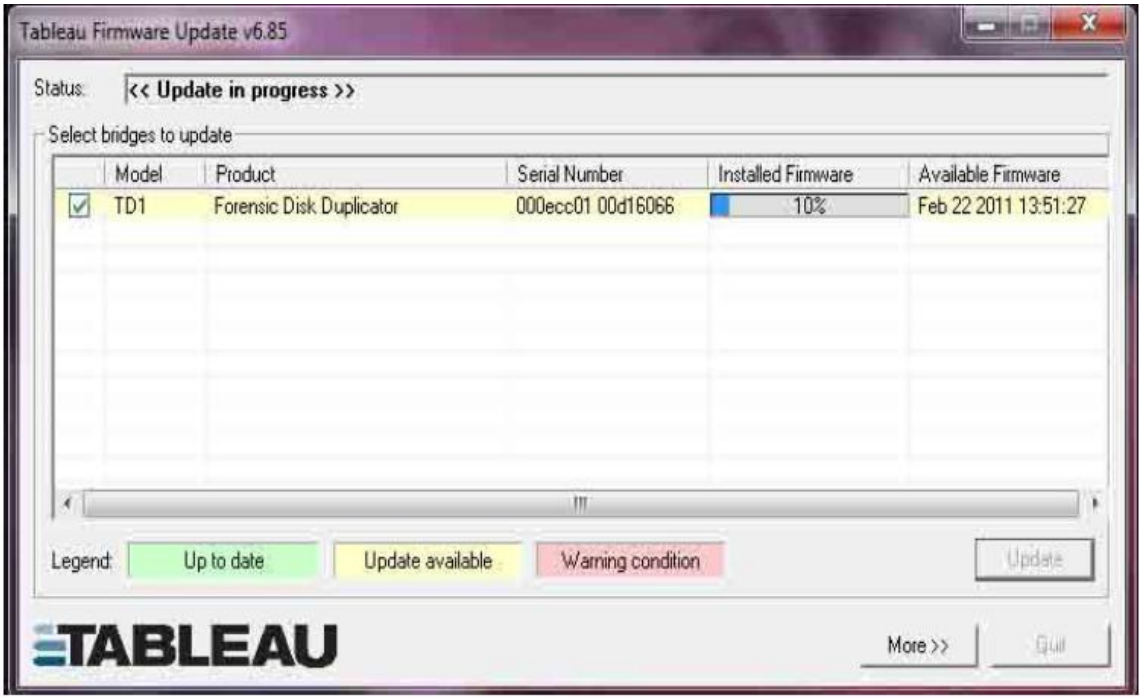
2.22.2.13 TD1 İmaj Alma Cihazı İle HDD Wipe

TD1'in Menüleri içerisinde bulunan Silme (Wipe) disk seçeneğinden Hedef (Destination) bölümüne bağlanılan diskin Silme (Wipe) yapılmasıdır. Silme (Wipe) işleminde iki seçenek mevcut olup birinci normal Silme (Wipe), İkinci seçenek ise Çoklu Silme (Multi Pass Wipe) şeklinde yapılmaktadır.

Çoklu Silme (Multi Pass Wipe) Write seçeneğinde birden fazla disk üzerine veri yazmak suretiyle Silme (Wipe) işlemi yapılmaktadır.

2.22.2.14 TD1 İmaj Alma Cihazı Güncelleme

TD1 bilgisayar ortamına FireWire veya USB ile bağlantısı Bağlanır. Bilgisayara kurduğumuz Tableau Firmware Update programı açılır. TD1'in güncellemesi eksikse Program otomatik olarak eksik güncellemeyi yüklemek için hazırlanır. Güncelleme (Update) seçilerek güncelleme (Update) sekmesine basılınca işlem için uyarı ekranı açılır. Tamam diyerek geçilince güncelleme işlemi başlanır. Tableu Marka TD1 İmaj alma cihazı bilgisayar güncelleme ekranı Şekil 2.57'de gösterilmiştir.

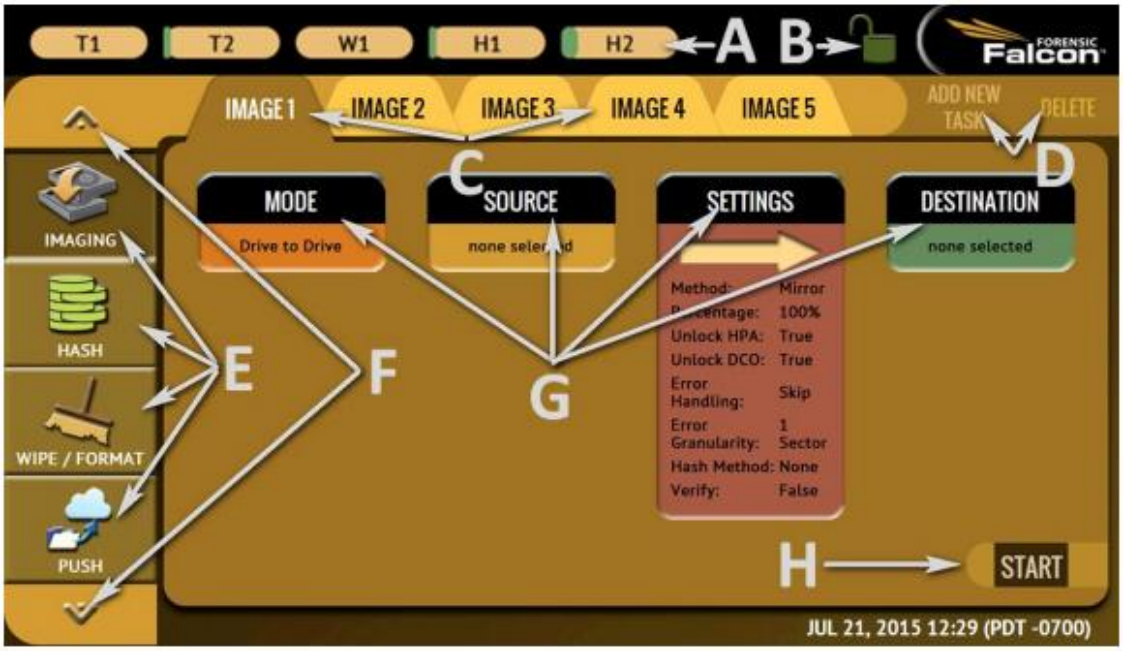


Şekil 2.57 Tableu Marka TD1 İmaj Alma Cihazı Bilgisayar Güncelleme Ekranı

2.22.2.15 Forensic Falcon

Logicube şirketi tarafından geliştirilmiş imaj alma cihazıdır. Kullanılan disk ve imaj alma formatına bağlı olarak dakikada 10 Gb imaj alabilmektedir. E001 ve EX01 farklı formatlarda imaj alabilmektedir. SHA1 SAH265 VE MD5 formatında da hash değeri vermektedir. Falcon Cihazında imaj almak için yazma korumalı olarak 2 adet

SAS/SATA potu 1 adet USB 3.0 PORTU ve 1 adet Firewire portu bulunmaktadır. İmajın kaydedileceği hedef için ise 2 adet SAS/SATA portu adet USB 3.0 PORTU ve 1 adet Firewire girişi vardır. Bu cihazın ayrıca har diskleri silme (wipe) etme ve format atma özelliği de bulunmaktadır. Forensic Falcon ara yüzü Şekil 2.58'de gösterilmiştir.



Şekil 2.58 Forensic Falcon Ana Ekran Ara Yüzü

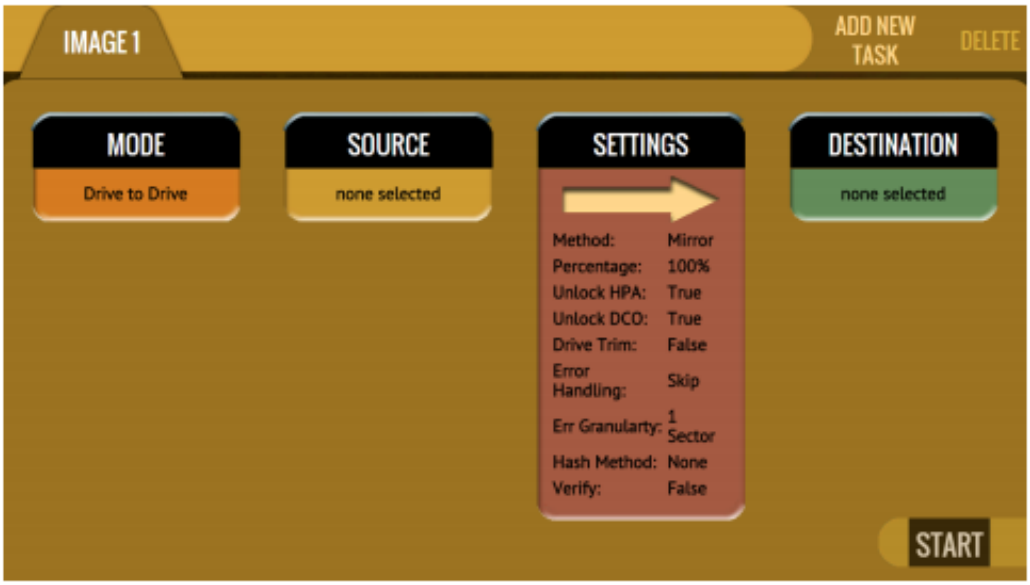
Forensic Falcon programındaki menülerin özellikleri aşağıda verilmiştir. Bunlar;

A. Çalışmakta olan İşlemler / Görevler,
B. Kilit göstergesi / kısayolu,
C. İşlemler / Görevler,
D. Görev ekleme veya silme,
E. İşlem Türleri,
F. Yukarı ve aşağı kaydırma okları,
G. İşlem seçenekleri ve ayarları,
H. Başlangıç.

2.22.2.16 Forensic Falcon İmaj Alma

İmaj modu altında bulunan Sürücüden Sürücüye (Drive To Drive) ve (Dosyadan Sürücüye) Drive to File sekmesine tıklanır. Hangi mod ile imaj alacaksak onu tıklanır.

Sonra kaynak sekmesine tıklayarak bağlı olan kaynak seçilir ve tamam sekmesi tıklanır. Sonra ayarlar (Settings) sekmesine tıklayarak imaj alınacak hard disk hakkında bilgileri doldurulur. Forensic Falcon İmaj alma ekranı Şekil 2.59'de gösterilmiştir.

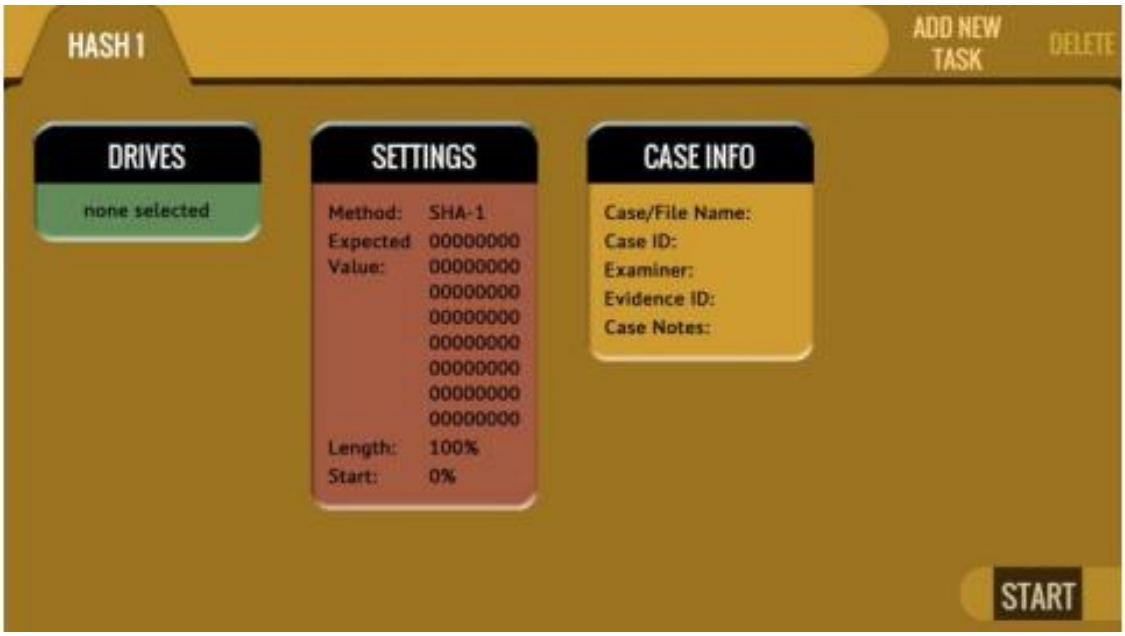


Şekil 2.59 Forensic Falcon İmaj Alma Ekranı

Sonra hedef simgesi tıklanarak kullanılacak olan hedef hardisk seçip ve tamam tıklanır. Bu ekran Şekil 2.60'de gösterilmiştir.

Şekil 2.60 Forensic Falcon Hedef Harddisk Ekranı

Alınan İmajın Hash değerini almak için Sürücüler (Drivers) sekmesine tıklanır SHA-256 or MD5 bu formatların hangisi ile hash alınacağı tıklanır ve tamam sekmesine tıklanır. Bu ekran Şekil 2.61'de gösterilmiştir (İnt.Kyn.9).



Şekil 2.61 Forensic Falcon Hash Belirleme Ekranı

2.23 Mobil Cihazlarda İmaj Alma

Günümüzde teknolojinin gelişmesi ile birlikte cep telefonları artık bilgisayar gibi kullanılmaya başlanılmış ve akıllı telefonlar ile birlikte cep telefonları küçük bir bilgisayar halini almıştır. Dolayısıyla bu cihazların içerisine yüklenen bilgilerde bir o kadar değerli olmuş ve bu cihazlarında incelenmesi gün geçtikçe önemli hale gelmiştir.

2.23.1 Cep Telefonları Hakkında Genel Bilgiler

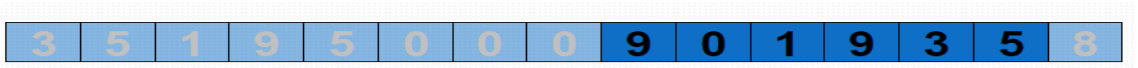
IMEI International Mobile Equipment Identifier açılımına gelmektedir. Türkçe karşılığı ise uluslararası mobil cihaz tanımlayıcıdır. Bir nevi cep telefonun seri numarası olarak tanımlanabilir.

Ürün, model, tarih ve ülke kodlarını barındırmaktadır. İmei Kodunu öğrenmek için telefondan *#06# basıp göndermeniz yeterlidir.

14 yada 15 numaradan meydana gelmektedir Bazen numaralar arasında "/" ya da "–" işareti kullanılır. İlk sekiz numara ürün tahsis kodu "Type Allocation Code" (TAC) Üretici kimliği, modeli ve üreten ülkeyi belirler. İlk Sekiz numara Şekil 2.62'de gösterilmiştir.

Şekil 2.62 IMEI İlk Sekiz Rakamı

9 ve 14 arasındaki numaralar" cihazın seri numarasıdır." Her bir telefon için ayrı numara üretilir. Cihazın seri numarası olan rakamlar Şekil 2.63'de gösterilmiştir.



Şekil 2.63 Cihazın Seri Numarası Olan Rakamlar

15. Numara "kontrol numarası olarak tanımlanabilir." (ControlDigit) IMEI numarasının doğruluğu teyit eder. Cihazın Kontrol Numarası Şekil 2.64'da gösterilmiştir.

Şekil 2.64 Cihazın Kontrol Numarası olan Rakam

Sim kart açılımı Subscriber Identity Module ve Türkçe karşılığı abone kimlik modülüdür. Cep telefonlarının içerisine yerleştirilen küçük bir karttır. Bu kart sayesinde cep telefonu ile mobil veri akışı sağlanmaktadır.

Mobil cihazlarda hafıza cihazın kendi hafızası, cihaza takılı bulunan hafıza kartı ve cihaza takılı bulunan sim kart olarak üç kısma ayrılmaktadır.

Mobil Cihazlardan elde edilebilcek veriler:

1-) Arama Kayıtları(Gelen arama, Giden arama, Cevapsız arama),

2-) Mesajlar,

3-) Sohbet kayıtları(Watsap, Viber, Tango, Messenger vb.),

4-) Fotoğraflar,

5-) Videolar,

6-) E-postalar,
7-) Takvim Bilgisi,
8-) Ajanda Bilgileri,
9-) GPS Kayıtları,
10-) Cep telefonuna yüklü bulunan uygulamalar Mobil cihaz içerisinden çıkartılabilir.

Akıllı telefonlar günümüzde artık bilgisayar gibi kullanılmaya başlanılmıştır. Bu akıllı telefonlar bir bilgisayarın bütün özelliklerini barındırırlar. Örneğin internete girme, yazı yazma yazı çıkartma vb. Akıllı telefonların bilgisayar gibi kullanılmaya başlanması akıllı telefonlarında imajının alınması ve incelenmesi gibi sorunları beraberinde getirmiştir. Bu telefonlarında artık içerisindeki bilgiler alınabilmekte ve kurtarılmaktadır. Akıllı telefonlar işletim sistemi olarak İphone nin kullandığı İOS ve Samsung Google vb. gibi telefonların kullandığı Android işletim sistemidir.

Akıllı telefonlar artan popülaritesi ve becerileri sonunda, bilgisayar korsanlarının (hacker) yeni hedefi olmaya başladı. Milyonları aşan mobil uygulamalar hayatımıza kolaylık, eğlence ve heyecan katarken bir yandan da ciddi güvenlik tehditleri getirmiş durumda. İndirdiğiniz basit bir uygulamayla dahi cihazımıza bulaşabilen bu zararlı yazılımlar bazen bir mailin ekiyle bazen de bir bağlantıyı tıkladığınızda indirilen bir dosya ile sisteme efekte olabilmektedir. Günümüzde işlenen suçların %70'den fazlasında cep telefonları bir şekilde dahil olmaktadır. Böyle bir durumda suçu aydınlatmada mobil cihaz incelemelerinin önemi de artmaktadır. Eski nesil cep telefonlarından rehber, mesaj, multimedia mesaj, gelen giden ve cevapsız aramalar, notlar ve takvim bilgisi gibi sınırlı sayıda bilgi elde edilirken yeni nesil cep telefonlarda bu bilgilere ek olarak video, şekil, ses, konum bilgisi, e-postalar, internet geçmişi, internet yazışmaları ve uygulama bilgilileri elde edilebilmektedir (Ekim 2013).

2.23.2 Cep Telefonlarında Adli İnceleme

Dünya çapında ve Türkiye'de yaygın olarak kullanılan ve uluslararası kabul görmüş Cellebrite Ufed ve Mobil Edit programları aşağıda detaylı bir şekilde anlatılmıştır. Mobil İncelemede iki tür inceleme bulunmaktadır. Birincisi mantıksal inceleme bu inceleme de cihaz içerisinde bulunan belgeler elde edilir. İkincisi ve önemli olan ise

fiziksel incelemedir. Fiziksel incelemede cihaz içerisindeki silinmiş verilere de ulaşmak mümkündür.

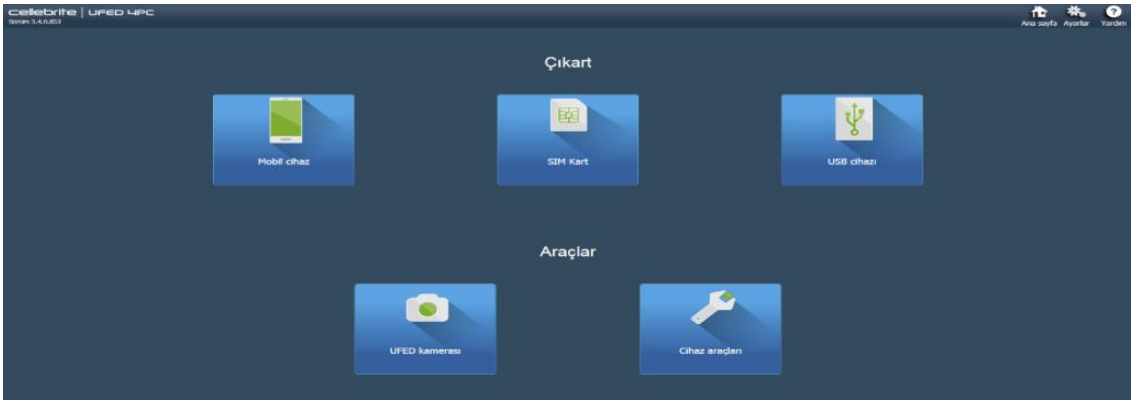
Cellebiride Ufed donanım cihazı bu donanım cep telefonları, akıllı telefonlar, tabletler, Çin telefonları gibi cihazların fiziksel ve mantıksal olarak imajını alabilmektedir. UFED cihazı Windows işletim sistemi ile çalışan mobil cihazların imajını almak için kullanılan bir cihazdır. İmaj alınacak cihaz Ufed cihazında marka ve modeli bulunur. UFED cihazında marka ve modeli seçilen cep telefonun ufed kiti ile birlikte gelen hangi numaralı kablo ile bağlanacağını gösterir. Sonra UFED Cihazına takılı olan flash belleğe cep telefonun fiziksel imajı almaya başlanır. Daha sonra bu flash belleğe alınan fiziksel imaj bilgisayarda bulunan Ufed Physical Analyzer programı ile incelenerek imaj alınan cihazın içerinde olan bilgilere ulaşılabilmektedir. UFed cihazına kablo ile bağlanan cep telefonları cihazın bluetooth ve kızılötesi bağlantısı sayesinde kablosuzda bağlanabilmektedir. Ufed Donanım Cihazı Şekil 5.65'de gösterilmiştir.

Şekil 2.65 Cellebrite Ufed Donanım Cihazı

Cellebride Ufed Yazılımı Ufed Firması tarafından çıkarılan bu program Dongle (Yazılımın çalışması için bilgisayara takılan bir çeşit usb aygıt) vasıtası ile çalışan yazılımdır. Bu yazılım sayesinde yukarıda anlattığım Cellebride Ufed Cihazına ihtiyaç

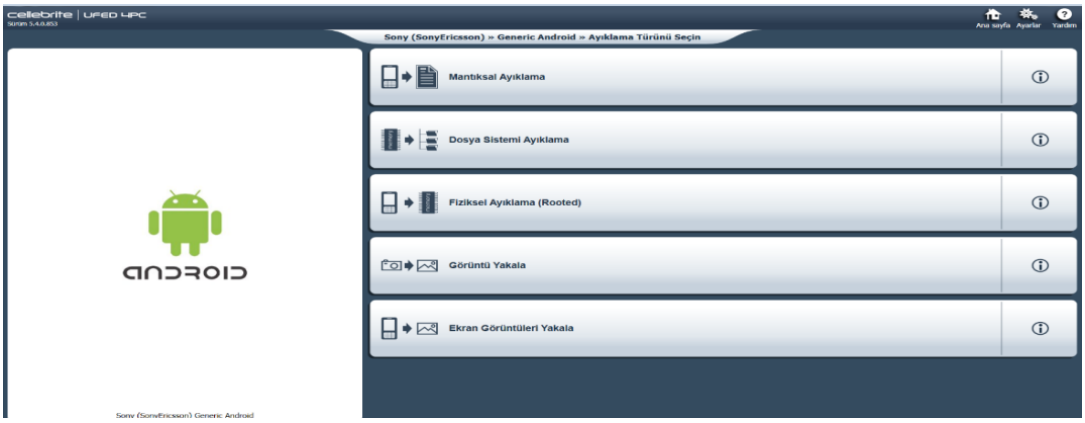
kalmadan mobil cihazların fiziksel ve mantıksal imajlarını alınmasını gerçekleştirmektedir.

Ufed Cellebride yazılımı açtığımızda gelen ekran aşağıdaki gibidir. Burada ne yapmak istenildiğini seçerek devam edilmesi gerekmektedir. Konu imaj alma konusu olduğu için Mobil cihaz sekmesine tıklanır. Cellebrite Ufed yazılımı ilk ekranı Şekil 2.66'de gösterilmiştir.



Şekil 2.66 Cellebrite Ufed Yazılımı Ana Ekran Arayüzü

Mobil cihaz bilgisayara bağlandıktan sonra yazılım otomatik mobil cihazı bulacak ve sonra yazılım ne gibi bir işlem yapmak istenildiği soracaktır. Bu kısımda mantıksal ayıklama telefonun içerisindeki bilgilerin dışarı çıkartılması, dosya sistemi ayıklama cihazın bilgilerin dışarı çıkartılması, fiziksel ayıklama cihaz içerisindeki silinmiş belgelerin dışarıya çıkartılması, görüntü yakalama ekran görüntüsünün alınması, ekran görüntüleri yakala kısmından ise telefon içerisindeki ekran görüntüsünün yakalanma arayazü verilmiştir. Cellebrite Ufed yazılımı menü seçme arayüzü Şekil 2.67'de gösterilmiştir.



Şekil 2.67 Cellebrite Ufed Yazılımı Menü Seçme Arayüzü

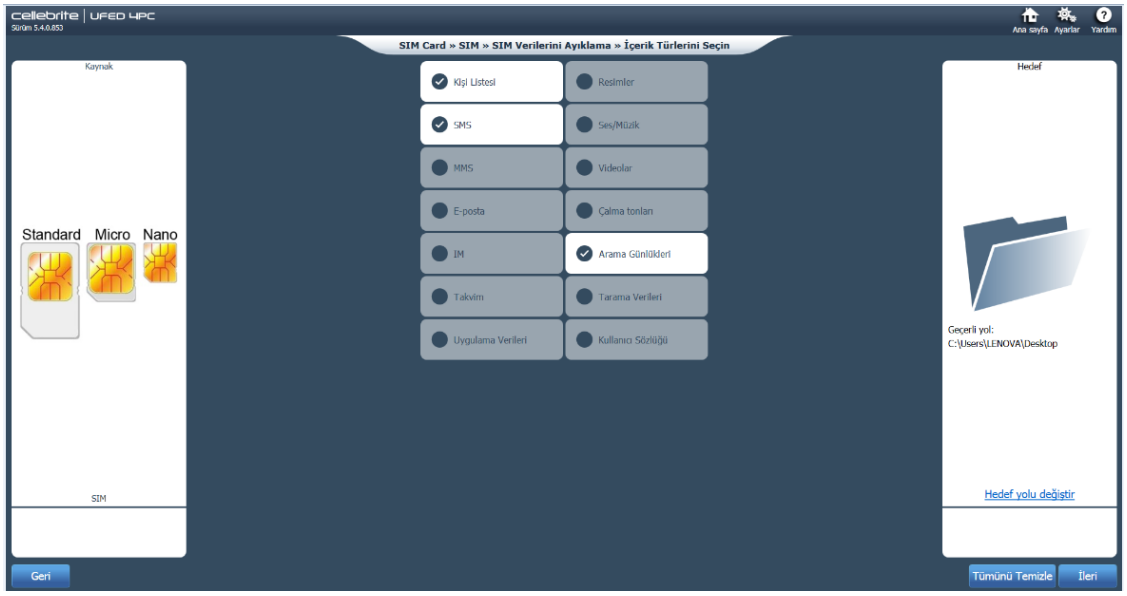
Gelen ekrana Mantıksal Ayıklama Modülünü seçilir ise telefon ve sim kart içeresinde bulunan rehberi ve telefon içerisinde bulunan diğer belgeleri çıkartır. Cellebrite Ufed yazılımı sim kart seçme arayüzü 2.68'de gösterilmiştir.

Şekil 2.68 Cellebrite Ufed Yazılımı Mantıksal İmaj Ayıklama Arayüzü

Gelen ekrana fiziksel ayıklama modülü seçilir ise Mobil cihazın içerisinde bulunan silinmiş belgelere ulaşılmış olur. Cellebrite Ufed yazılımı fiziksel imaj arayüzü Şekil 2.69'de gösterilmiştir.

Şekil 2.69 Cellebrite Ufed Yazılımı Fiziksel İmaj Ayıklama Arayüzü

Ana ekran üzerinde bulunan SIM Kart sekmesi tıklandığında SIM kart içerisinde ne yapılması gerektiğini sorulmaktadır. Bu gelen ekranlar içerisinden SIM verilerini ayıkla sekmesine tıklandığında Sim kart içerisinde bulunan bilgilerin çıkartılması sağlamaktadır. Burada rehber sms ve arama günlüklerini elde edebiliriz. Cellebrite Ufed yazılımı sim kart ayıklama arayüzü Şekil 2.70'de gösterilmiştir.

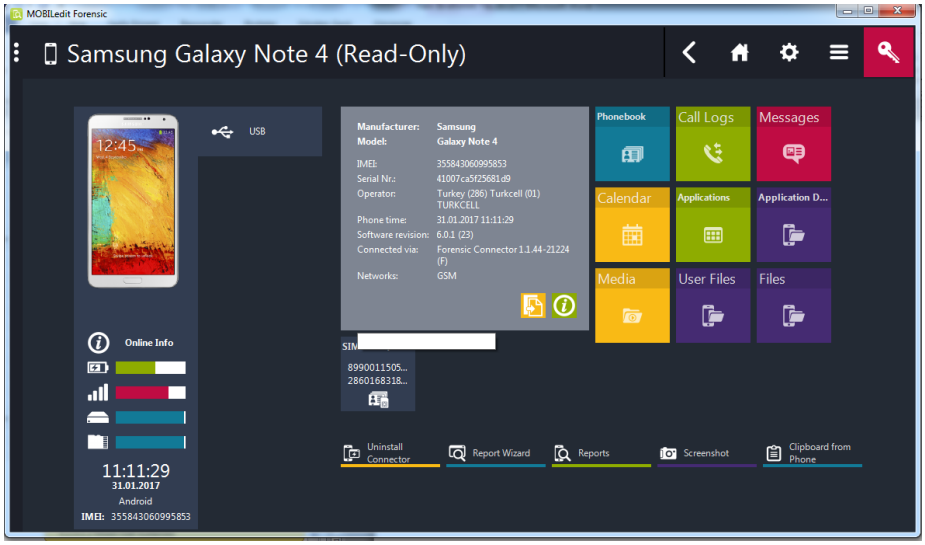


Şekil 2.70 Cellebrite Ufed Yazılımı Sim Kart Ayıklama Arayüzü

Mobil Edit Forensic programı lisans ile kullanabilen ücretli bir yazlımdır. Mobil Edit yazılımı mantıksal ve fiziksel olarak çıkarım yapabilmektedir. Mobil cihaz Mobil Edit programına kablo, bluetooth ve kızıl ötesi ile bağlanabilmektedir. Mobil Edit yazılımı mobil cihaz ile bağlantı kurduktan sonra mobil cihazın model numarasını, Imei numarasını ve cihaz resmini programın ara yüzüne getirmektedir. Mobil Edit yazılımı cep telefonları, tabletler, akıllı cihazlar ve Çin malı cihazlar içerisinde bulunan mevcut mesaj, rehber, görüşme kaydı, telefon içerisinde bulunan video, fotoğraf, not bilgisi ve takvime kayıt edilen bilgileri ve mobil cihaz içerisinde bulunan silinmiş belgelere de ulaşmamızı sağlar.

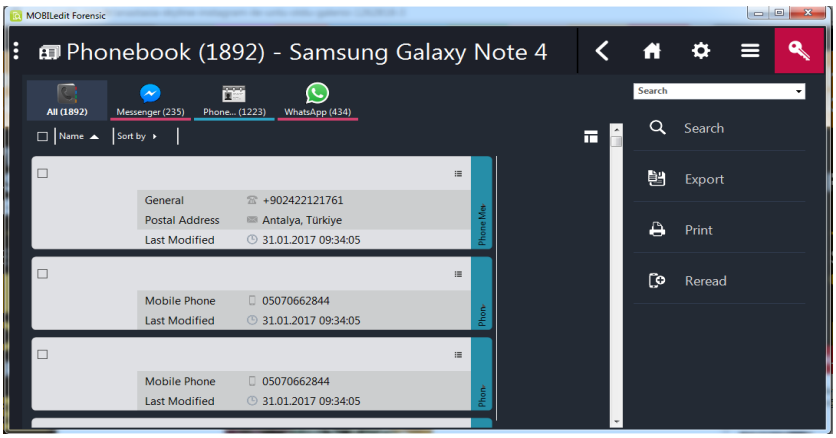
Mobil Edit yazılımının ilk ara yüz sayfasında sol tarafta cihaz resmi, cihazın şarj durumu, mobil verinin cihaza nasıl geldiği, mobil cihazın doluluk oranı ve sim kartın doluluk oranın ne durumda olduğu ve cihazın IMEI numarası, bu ekranın yanında mobil cihazın markası, modeli, Imei numarası, operatörü gibi bilgiler bulunmaktadır. Bu

ekranın yan tarafında ise mobil cihazın rehber (Phonebook), arama kayıtları (Call Logs), mesajlar (Message), takvim (Calender), uygulama (Application), uygulama verileri (Application Data), medya (Media), kullanıcı dosyaları (User Files), Dosyalar (Files) bölümleri bulunmaktadır. Bu bölümler Şekil 2.71'de gösterilmiştir.



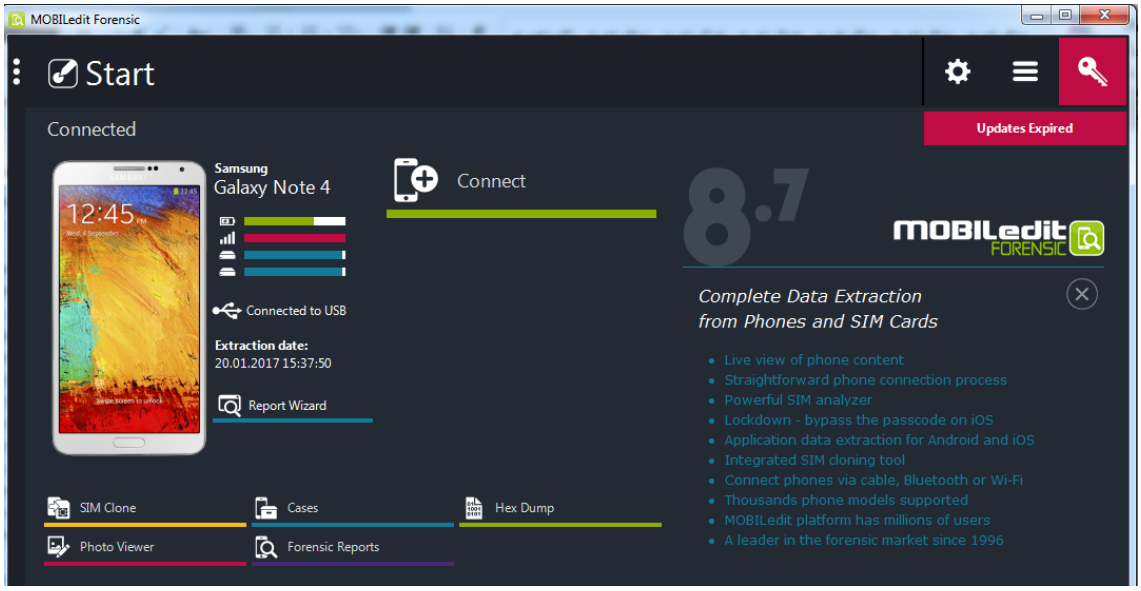
Şekil 2.71 Mobil Edit Ana Ekran Ara Yüzü

Mobil Edit rehber (Phonebook) sekmesinde mobil cihazın rehber kısmı ve mobil cihazda yüklü olan uygulamalar içerisinde bulunan Rehber gözükmektedir.(Messenger, watsapp vs.) Mobil cihazda bulunan rehber listesini sağ tarafta bulunan dışarı çıkart (Export sekmesi vasıtasıyla dışarı çıkarılmaktadır.) Mobil Edit rehber bölümü Şekil 2.72'de gösterilmiştir.



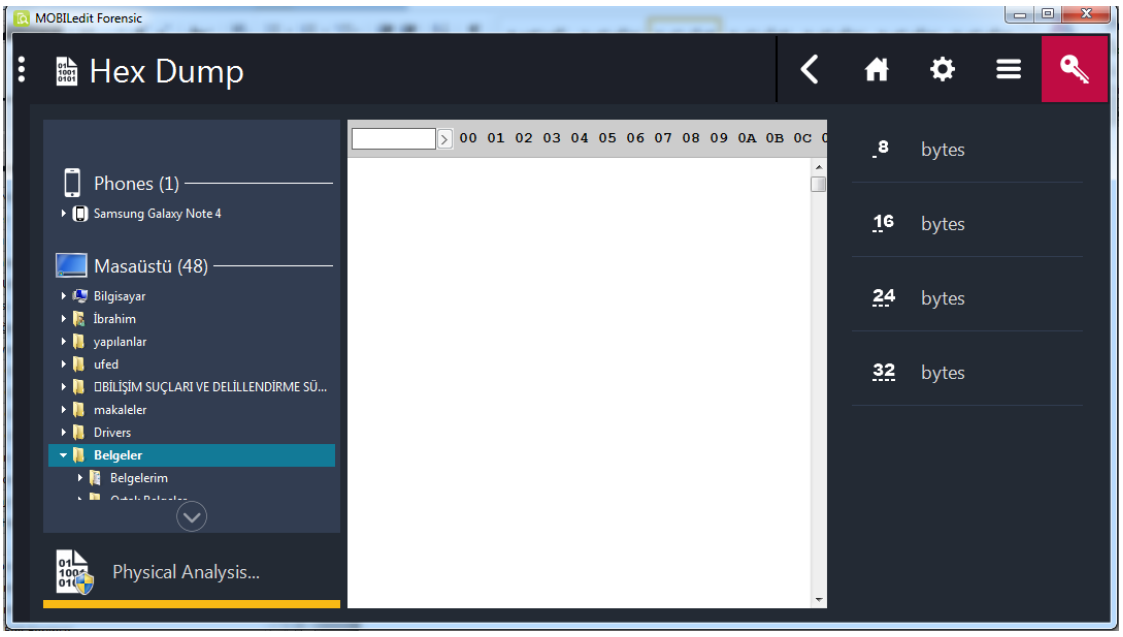
Şekil 2.72 Mobil Edit Rehber Bölümü

Mobil Edit yazılımının ana ekranında bulunan Hex dökümü (Hex Dump) ekranı tıklanır. Mobil Edit Hex Dump bölümü Şekil 2.73'de gösterilmiştir.



Şekil 2.73 Mobil Edit Fiziksel İmaj Alma Arayüzü

Mobil Edit Hex Dump Sekmesi içerisinde bulunan Fiziksel analiz (Physical Analysiser) sekmesine tıklayarak mobil cihaz içerisinde bulunan silinmiş belgelere ulaşılır. Fiziksel analiz (Physical Analysiser) bölümü Şekil 2.74'de gösterilmiştir.



Şekil 2.74 Physical Analysiser (Fiziksel analiz) Arayüzü

3. MATERYAL ve METOT

Bu bölümde, banka ve/veya kredi kartlarının kötüye kullanılması suçu ile ve mail adresi çalınması ve bilişim sistemine girme suçu ile ilgili senaryo hazırlanmış, bu senaryo kapsamında senaryo için hazırlanan dijital materyaller üzerinde CMK 134. Maddesi kapsamında önce imaj alma işlemi yapılmış ve daha sonra Encase, Autopsy ve X Ways Samsung cep telefonu ise Mobil Edit yazılımları vasıtasıyla inceleme yapılmıştır. Bu işlem vasıtasıyla yoğun olarak kullanılan bu programların ergonomi (kolay kullanım), arama hızı ve raporlama gibi özelliklerinin karşılaştırmaları yapılmıştır. Bunun yanında adli olarak bir imaj alma işlemi ve incelemelerin nasıl yapılacağı konusunda siber suç ile ilgili çalışan birimlere bilgi sahibi olmaları amaçlanmıştır.

İmaj alma ve inceleme işlemi yapılan bilgisayara ait özellikler Çizelge 3.1'de gösterilmiştir.

Çizelge 3.1 İmaj alma ve inceleme yapılan bilgisayara ait özellikler

Hard Disk Kapatesi	**Ram Hızı**	**Windows Versiyonu**	**Windows Sistem Türü**	**Windows İşlemcisi**
500 Gb	6 Gb	Windows 7	64 Bit Ultimate	İntel Core İ7

İmaj alma işlemi 5 ayrı yazılım ve TD1 Cihazı ile yapılmıştır. Bu çalışmada kullanılan yazılımlar ile TD1 cihazının karşılaştırmaları yapılmıştır.

Tez kapsamında dijital delilin oluşturulmasında kullanılan bilgisayarın özellikleri Lenova Marka CBG0553224 Seri Numaralı diz üstü bilgisayar ve Samsung Marka cep telefonudur.Bu diz üstü bilgisayardan www.hepsiburada.com isimli web sitesine 212.252.84.159 IP numaradan bağlanılıp ibosaraydere15@hotmail.com adresi ile kayıt yapılmıştır. Kayıt yapılan bu mail adresi İbrahim Saraydere isimli şahsın rızası ve bilgisi dışında kullanılmıştır. Bu senaryoda aktif olarak kullanılan bir kredi kartı ile alışveriş yapılmıştır. Bu süreçte kullanılan bu bilgisayar 1 numaralı dijital delil olarak adlandırılmış içerisine suça konu bilgi, belge ve dokümanlar kopyalanmıştır. Bu verilerden bazıları saklanmış veya silinmiş ve bilgisayara format atılmıştır.

Çizelge 3.2 Lenova Marka CBG0553224 Seri Numaralı diz üstü bilgisayara ait özellikler

Hard Disk Kapatesi	**Ram Hızı**	**Windows Versiyonu**	**Windows Sistem Türü**	**Windows İşlemcisi**
160 Gb	2 Gb	Windows 7	64 Bit Ultimate	İntel Core 2 Duo

Yukarıda belirtilen işlemler bilgisayarın imajı alınmadan önce yapılan işlemlerdir. Bu dosyalar Çizelge 3.3'de verilmiştir. Verilen bu dosyalar Windows işletim sistemi içerisinde muhtelif yerlere kaydedilmiştir.

Çizelge 3.3 Bilgisayar içerisinde bulunan veriler

Bilgisayardaki Mevcut Veriler	**Bilgisayardaki Silinmiş Veriler**	**Bilgisayardaki Uzantısı Değiştirilmiş Veriler**	**Bilgisayardaki Yüklü Programlar**
Msn adresleri.rar	Kart bil.jpg	Hack olacak msn adresleri.kkk	IP Hider Pro
Kart ko111pyala	Kart bil2.jpg	Kart kopyalanacak.aaa	Registry Life
nacak.jpg	Kart bil3.jpg	Kart kopyalanacak3.aaa	
	Kart bil4.png	Kart kopyalanacak5.bbb	
	KART BİLGİLERİ.docx	Kart kopyalanacak6.ccc	
	Kart bilgileri.txt	Kart kopyalanacak2.ddd	
	Kart kopyalama.jpg	Msn Adresleri.lll	
	Kart Kopyalanacak444.jpg		
	Kart merkezi kartlar.rar		
	Kart merkezi kartlar.txt		
	Kart.jpg		
	Kart123.jpg		
	Karttt.jpeg		
	Kredi kartı kopyalama		
	güvendemisin.com.flv		
	Mail adresleri.txt		
	Yeni Metin Belgesi(3).txt		

Bu tez çalışması için hazırlanan senaryoda kullanılan bu bilgisayar 1 numaralı dijital delil olarak adlandırılmış içerisine çizelge verilen bilgi, belge ve dokümanlar kopyalanmıştır. Bu dokümanlar ve veriler işlenen bir bilişim suçu delili olarak nitelendirilmektedir. Bu verilerden bazıları saklanmış veya silinmiş ve bilgisayara

format atılmıştır. Böylece inceleyenin işini zorlaştırılacağı düşünülmüştür. Yine aynı ikametten ele geçirilen Samsung Marka Not 4 Model 355843060995853 IMEI numaralı cep telefonu üzerinde Mobil Edit programı vasıtasıyla inceleme yapılmış telefona ait bilgiler çizelge 3.4'de verilmiştir. Samsung Not 4 telefon içerisine muhtelif yerlere Çizelge 3.5'de gösterilen bilgiler yüklenmiş ve silinmiştir.

Çizelge 3.4 Samsung Not 4 marka telefona ait özellikler

Telefon Model	İşlemcisi	Ram Bilgileri	Dahili Hafızası
Not 4	Android 4.4	3 GB	32 GB

Çizelge 3.5 Samsung Not 4 telefon içerisinde bulunan veriler

Telefon İçerisinde Mevcut Veriler	Telefon İçerisinde Silinmiş Veriler	Telefon İçerisinde Yüklü Programlar
kredi kartı bilgileri.docx kart ko1111pyalanacak.jpg	kredi kartı kopyalanacak.docx	Super Best Proxy Clean My Android

4. BULGULAR

Bilişim suçu kapsamında elde edilen Lenova Marka CBG0553224 Seri Numaralı diz üstü bilgisayarın imajı FTK, Encase, X-Ways, Helix, Tablue İmager ve TD1 cihazı ile alınmıştır. Tüm bu yazılımlarla ve TD1 cihazı ile imaj alma işlemi bittikten sonra imaj ile ilgili bilgileri gösteren TXT belgesi imaj dosyalarının bulunduğu klasör içerisine kaydedilir. Daha sonra inceleme işlemini yapan personel imajın kaç saat sürdüğü hard diske ait bilgileri ve imajın hash değerini bu TXT dosyası içerisinden görebilmektedir.

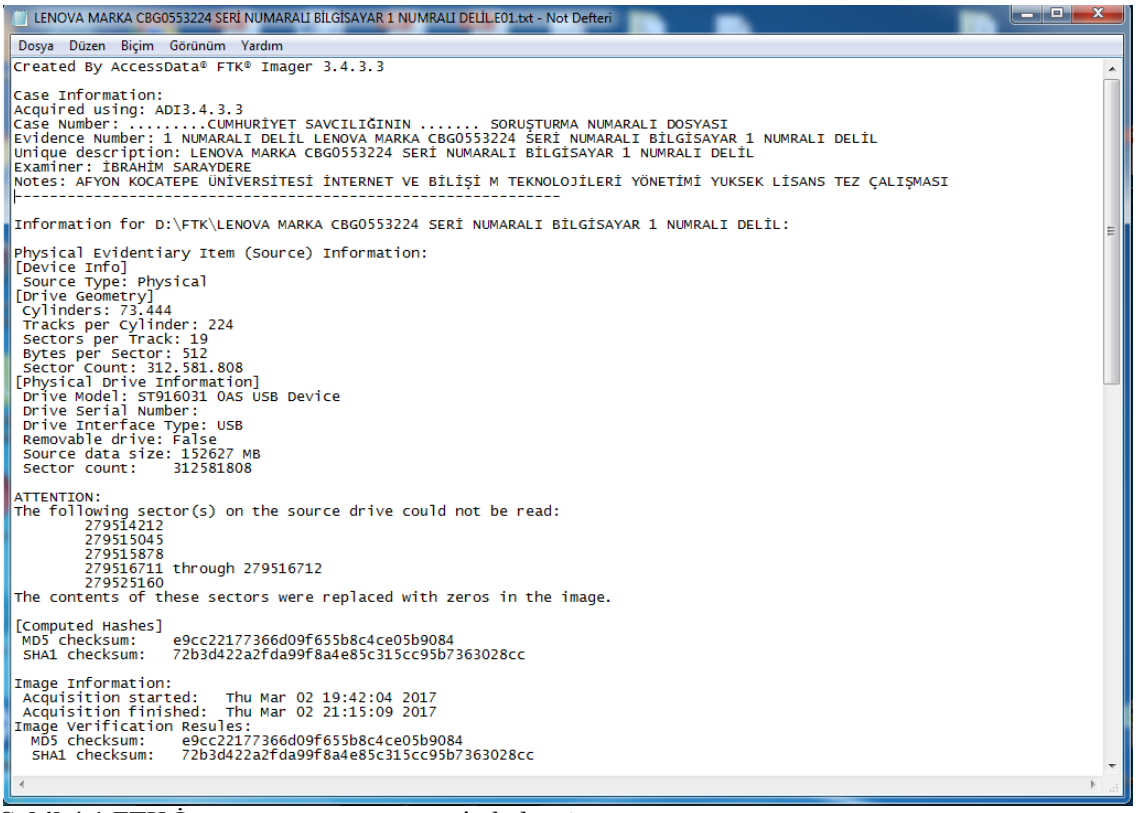
5 adet yazılım ve 1 adet cihaza ait genel bilgiler çizelge 4.1'de gösterilmiştir. El konulan ve imajı alınan 160 Gb kapasiteli hardisk FTK Programı ile 1 saat 25 dakikada ve 81,3 Gb fiziksel imaj aldığı görülmüştür. Encase programı ile 1 Saat 13 dakikada ve 83,4 Gb Fiziksel İmaj aldığı görülmüştür. X-Ways Programı ile 1 Saat 15 Dakikada ve 85.3 Gb Fiziksel İmaj aldığı görülmüştür. Helix Programı vasıtası ile 1 Saat 28 Dakika ve 79.4 Gb Fiziksel İmaj aldığı görülmüştür. Tablue İmager Programı vasıtası ile 50 Dakika ve 72.6 Gb Fiziksel İmaj aldığı görülmüştür. Son olarak TD1 Cihazı ise 44 dakika ve 64.4 Gb Fiziksel İmaj aldığı görülmüş bu tabloya göre en hızlı imaj alan donanım TD1 cihazı olduğu tespit edilmiştir.

Çizelge 4.1 İmaj alınan yazılım hash değerleri ve cihaz listesi

İmaj Alma Yazılımı	**Bilgisayar Bağlantı Türü**	**İmaj Alma Zamanı**	**İmaj Alma Kapasitleri (1.4 Gb Olarak Sabitlenmiştir)**	**Hash Değer Bilgileri**
FTK	Ex-Sata	58.02 Dakika	81,3 Gb	MD5:29e84023b9d1482f27fbc0a8c584f4c4 SHA1c79cf01dff9bece7aef69639a161a013e5386ddc
Encase	Ex-Sata	1 Saat 13 Dakika	83,4 Gb	MD5:29e84023b9d1482f27fbc0a8c584f4c4 SHA1c79cf01dff9bece7aef69639a161a013e5386ddc
X-Ways	Ex-Sata	1 Saat 15 Dakika	85.3 Gb	MD5:29e84023b9d1482f27fbc0a8c584f4c4 SHA1c79cf01dff9bece7aef69639a161a013e5386ddc
Helix	Ex-Sata	1 Saat 28 Dakika	79.4 Gb	MD5:29e84023b9d1482f27fbc0a8c584f4c4 SHA1c79cf01dff9bece7aef69639a161a013e5386ddc
Tablue İmager	Ex-Sata	50.25 Dakika	72.6 Gb	MD5:29e84023b9d1482f27fbc0a8c584f4c4 SHA1c79cf01dff9bece7aef69639a161a013e5386ddc
TD1 Cihazı	Ex-Sata	44.47 Dakika	64,4 Gb	MD5:29e84023b9d1482f27fbc0a8c584f4c4 SHA1c79cf01dff9bece7aef69639a161a013e5386ddc

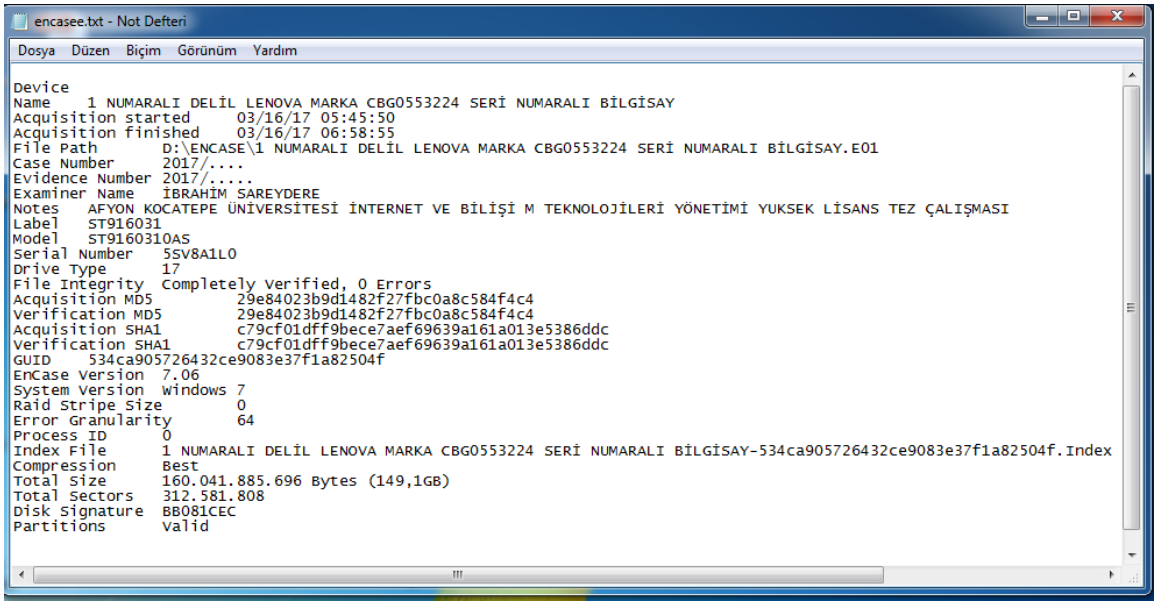
FTK İmager programı tarafından imaj alındıktan sonra üretilen metin belgesinde üst kısmında programın versiyonu yazmaktadır. Alt kısımda ise FTK imager programı tarafından doldurulması istenilen alanlar gelmektedir. Onun altında ise imajı alınan

bilgisayarın hard diskine ait özellikler çıkartılmaktadır. Sonra imaja ait hash değerleri ve en sonunda da imajın başlanma ve bitirilme tarihi verilmektedir. FTK Imager programının metin belgesi Şekil 4.1'de verilmiştir.



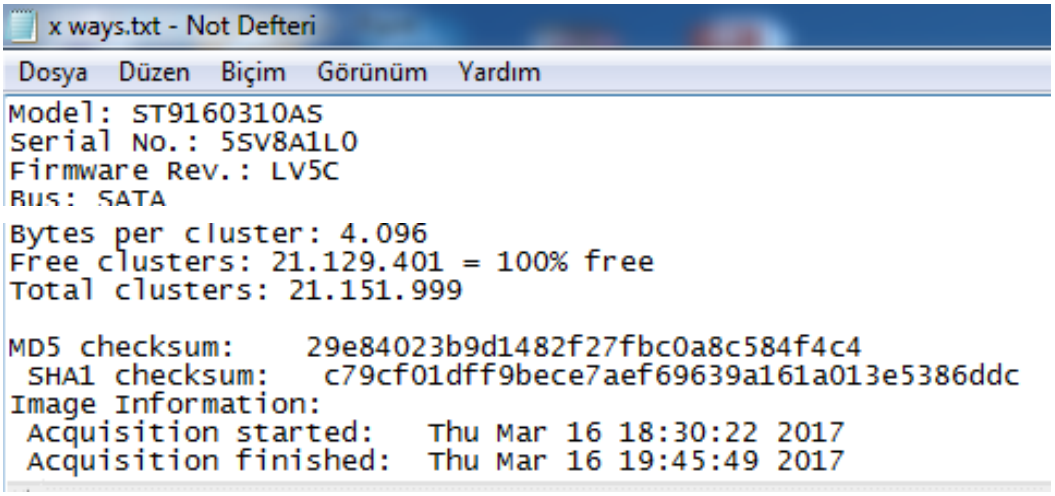
Şekil 4.1 FTK İmager programının metin belgesi

Encase İmager tarafından imaj alındıktan sonra üretilen metin belgesinde üst kısmında imajı alınan dijital materyalin ismi altında imaj alınmaya başlanma ve bitiş tarihi onun altında programda verilen olay numarası, imaj alan personel ismi ve alınacak not ile ilgili bilgiler bulunmaktadır. Sonra imajı alınan hard diskin modeli, hard diskin seri numarası sonra ise oluşturma ve doğrulama hash bilgileri en son da ise hard diske ait kapasite bilgisi bulunmaktadır. Encase Imager Programının metin belgesi şekil 4.2'de gösterilmiştir.



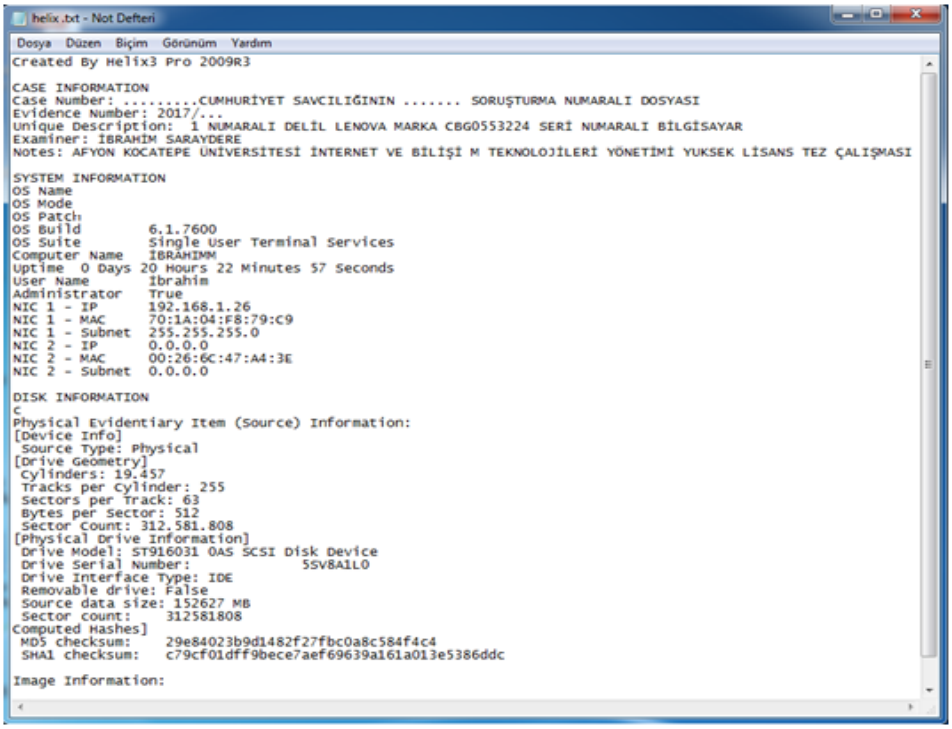
Şekil 4.2 Encase ımager programının metin belgesi

X-WAYS İmager Programı tarafından imaj alındıktan sonra üretilen metin belgesinde en üst kısımda imajı alınan hard diskin modeli ve seri numarası yer almaktadır. Bunların altında ise hard disk kapasitesi, hard disk kafa sayısı, hard disk sektör sayısı, hangi sistem ile çalıştığı, sonrasında hard diske ait hard disk bölümleri (partition), kapasiteleri ve bunların sonunda ise hard diske ait hash hesaplamaları bulunmaktadır. En sonda ise imaj almaya başlama ve bitiş tarihi yer almaktadır. X-WAYS İmager Programının metin belgesi Şekil 4.3'de gösterilmiştir.



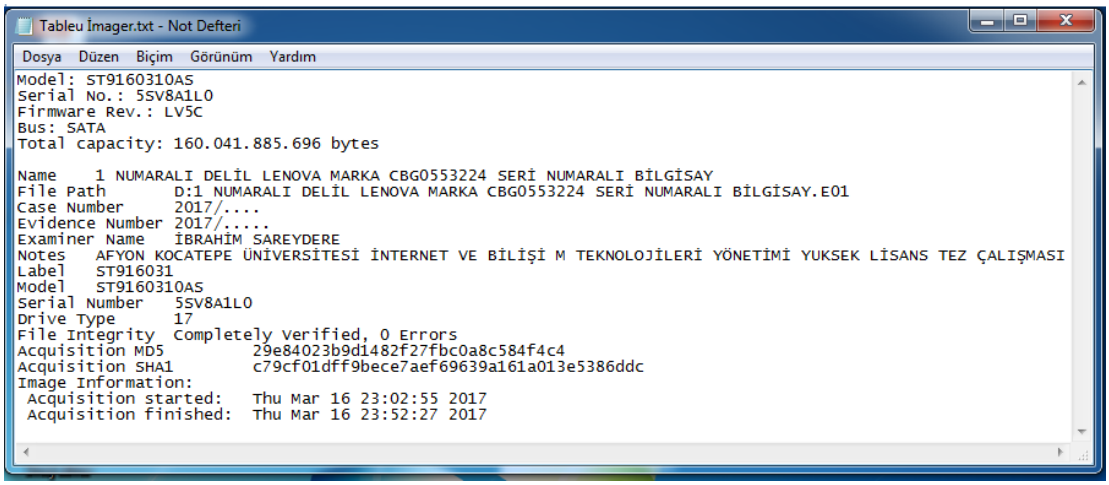
Şekil 4.3 X-WAYS İmager Programının metin Belgesi

Helix3 Pro Imager Programı tarafından imaj alındıktan sonra üretilen metin belgesinin en üst kısmında program modeli sonra hard disk hakkında programa yazılan olay bilgileri sonra hard disk sistem bilgileri Windows modeli bilgisayar gibi bilgiler, sonra disk bilgileri, hard disk kapasitesi, sonra hard disk modeli ve seri numarası en sonda da hash bilgileri bulunmaktadır. Helix3 Pro Imager programının metin belgesi şekil 4.4'de gösterilmiştir.



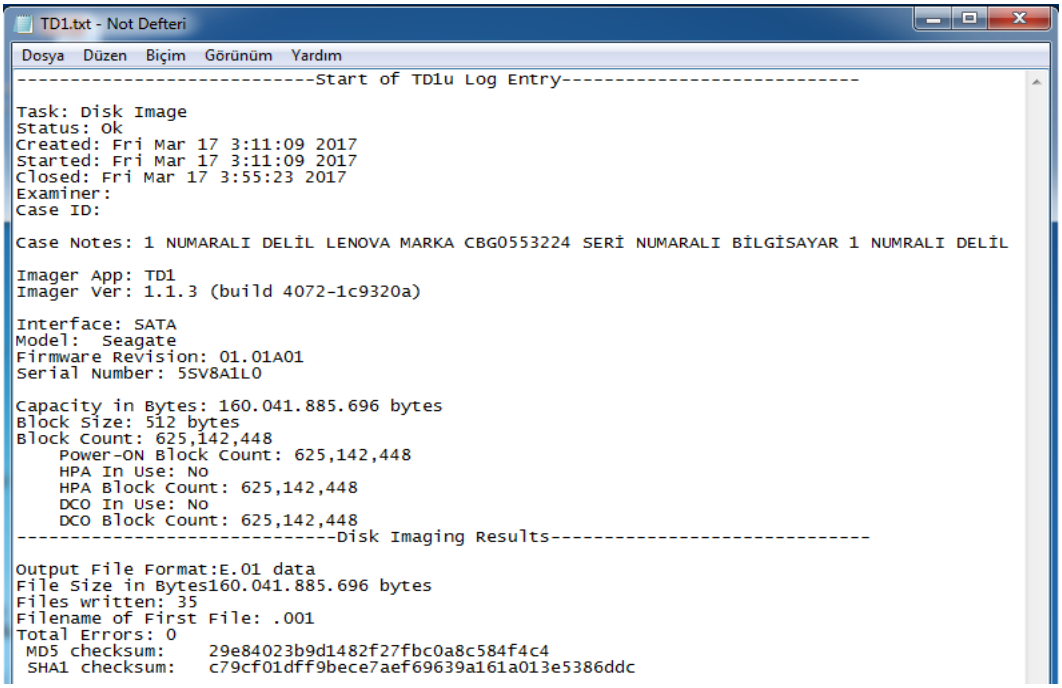
Şekil 4.4 Helix3 Pro Imager programının metin belgesi

Tablue Imager Programı tarafından imaj alındıktan sonra üretilen metin belgesinin en üst kısmında hard disk modeli sonra hard diskin seri numarası ve sonrada hard disk kapasitesi bulunmaktadır. Bunların altında programa yazılan olay bilgileri imajı alan personel ismi ve olay ile ilgili alınan not bulunmaktadır. Bunların altında da hard disk hash bilgileri en sonda ise de imaj alınmaya başlanma ve imaj bitiş tarihi verilmiştir. Tablue Imager programının metin belgesi Şekil 4.5'de gösterilmiştir



Şekil 4.5 Tablue Imager Programının Txt Belgesi

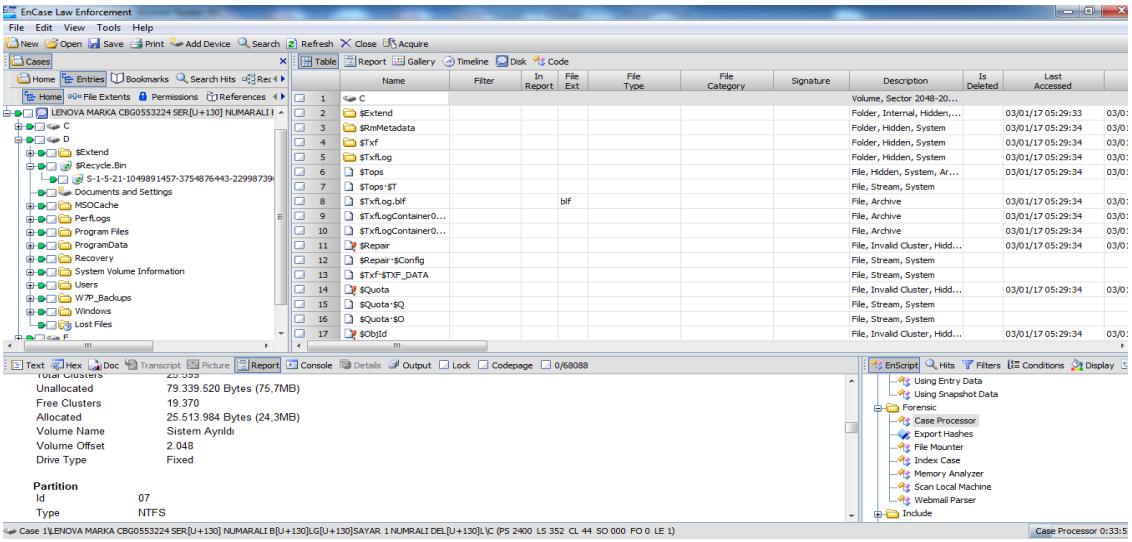
Tableu marka Td1 Cihazı tarafından imaj alındıktan sonra üretilen metin belgesinin en üst imajın nasıl alındığı onun altında imajın alınmaya başlanma ve bitiş tarihi onun altında ise imaj alanın ismi ve imaj ile ilgili yazılan notlar bulunmaktadır. Sonra imaj alınan cihaz adı ve cihaz sürümü, sonra imajı alınan hard disk modeli ve seri numarası, sonra hard disk kapasitesi ve en sonda hard disk hash bilgileri bulunmaktadır.TD1 Cihazına ait metin belgesi şekil 4.6'de gösterilmiştir.



Şekil 4.6 TD1 cihazına ait metin belgesi

4.1 Encase Programı İle Adli İnceleme

Alınan imaj dosyaları EnCase Forensic (Ver. 6.19) yazılımı ile incelenmek üzere açılarak tekrar Doğrulama (Verifing) yapması sağlanmış ve inceleme işlemine geçilmiştir. Bir önceki bölümde bahsedildiği gibi dijital materyal içerisinde kayıtlı bulunan dosyalar (silinmiş ve gizlenmiş) dosyalar bu inceleme ile çıkarılmaya çalışılmıştır. Dijital materyale ait imaj içerisinde silinmiş ve gizlenmiş dosyaların kurtarılma işlemi gerçekleştirilmiştir. EnCase Forensic yazılımının senaryo kapsamındaki incelemeye ait kullanıcı ara yüz ekran görüntüsü Şekil 4.7'de gösterilmiştir.



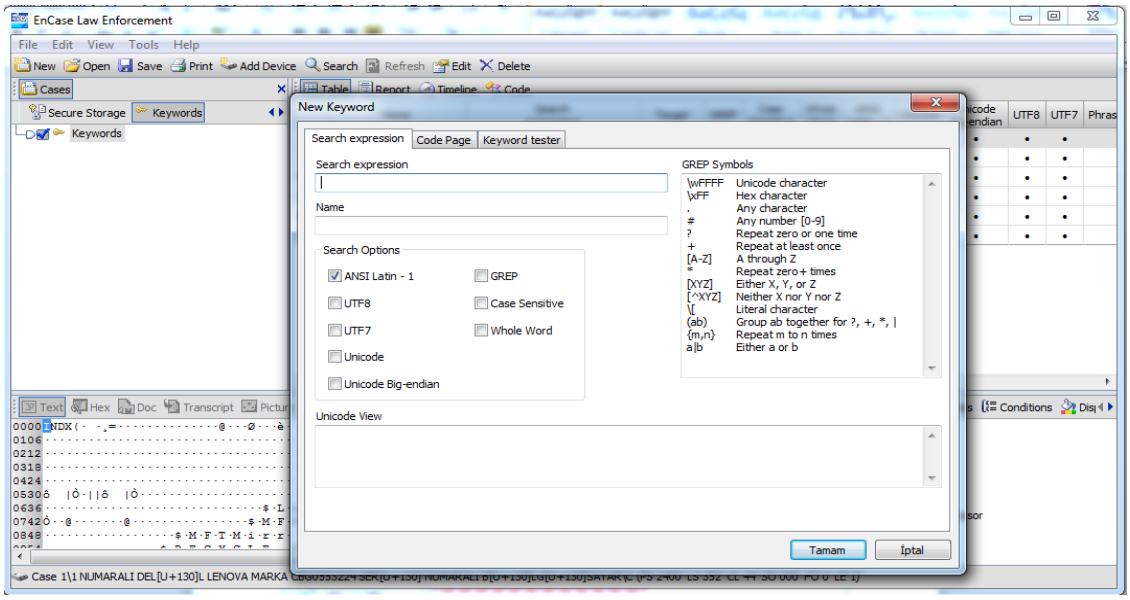
Şekil 4.7 EnCase Forensic yazılımının ana yüz ekran görüntüsü

Şimdi silinmiş dosyaların tespiti amacıyla Kurtarma (Recovery) işlemi gerçekleştirilerek silinmiş veriler üzerinden delil elde edilmeye çalışılmış kredi kartı bilgileri ve mail adresleri üzerinde çalışılma yapılmıştır. Sağ tarafta bulunan Olay işlemcisi (Case Processor) sekmesinin altında bulunan Bilgi Bulucu (Information Finder) sekmesinden kredi kartı ve mail adresi bilgileri taratılmış ayrıca İbrahim Saraydere isimli şahsın kredi kartı numarası programda taratılmak yöntemiyle programa girilerek bulunmaya çalışılmıştır.

Hepsiburada.com isimli internet sitesinden alınan IP numarası bilgilerinin tespiti yapılmış ve senaryo gereği alışveriş esnasında kullanılan ve soruşturma kapsamında

tespiti yapılan IP numarası ve mail adresinin bu bilgisayar tarafından kullanılıp kullanılmadığı tespit edilmeye çalışılmıştır. İbrahim SARAYDERE isimli şahsın kullanmış olduğu 5549 **** *** 7066 numaralı kart bilgisi EnCase Forensic yazılımı üzerinden anahtar kelime (keyword) taraması yapılarak çıkan sonuçlar değerlendirilmiş ve senaryoda kullanılan kredi kartı bilgisi ile ilgili olanlar suç unsuru olarak aşağıda gösterilmiştir.

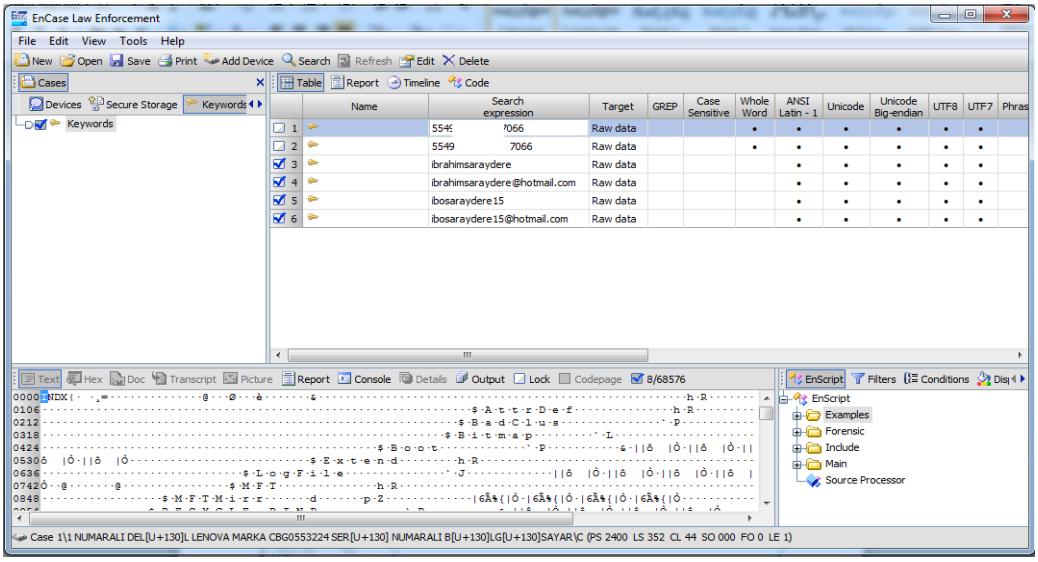
Encase programının Anahtar Kelime (Keywords) kısmına tıklanır. Sonra sağ tarafta bulunan boşluk bölümüne sağ tıklanarak Arama Açıklamaları (Search Expression) kısmına Encae programında aratmak istediğimiz kelimeleri girerek Encase programında senaryoda geçen ibosaraydere15@hotmail.com ve yine İbrahim SARAYDERE isimli şahsa ait olan 5549 **** *** 7066 numaralı kart bilgileri anahtar kelime olarak programa girilerek program vasıtasıyla taratılmıştır. Sonra Encase programının üst kısmında bulunan Arama (Search) kısmına gelinerek aratma yapılmaktadır Şekil 4.8'de EnCase programı arama ekranı ara yüzü gösterilmiştir.



Şekil 4.8 EnCase Programı Arama Ekranı Ara Yüzü

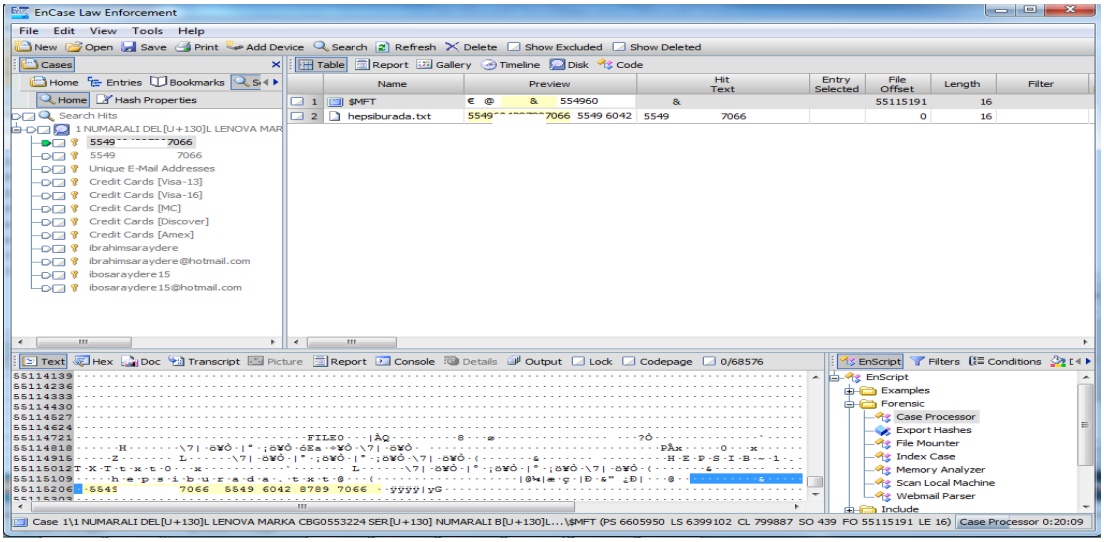
Şekil 4.9'da gösterilen Encase ekran görüntüsünde Anahtar Kelime (Keywords) yazma yöntemiyle İbrahim Saraydere isimli şahsın kullanmış olduğu 5549 **** *** 7066 isimli kart numaraları program vasıtasıyla taratılmış ve MFT kayıt tablosunda 5549 **** *** 7066 numaralara rastlanılmıştır. MFT kayıt tablosu ise Master File Table

kelimelerinin kısalmasıdır. Yani bir bilgisayar sistemi içerisinde NFTS dosya sistemi içerisinde tüm dosyaların izlemesini yapar. Dosyalara ait konum bilgilerini hangi dizine ait fiziksel metadataları içerir. Şekil 4.9'da Encase programı aranan kelimeler ara yüzü gösterilmiştir.



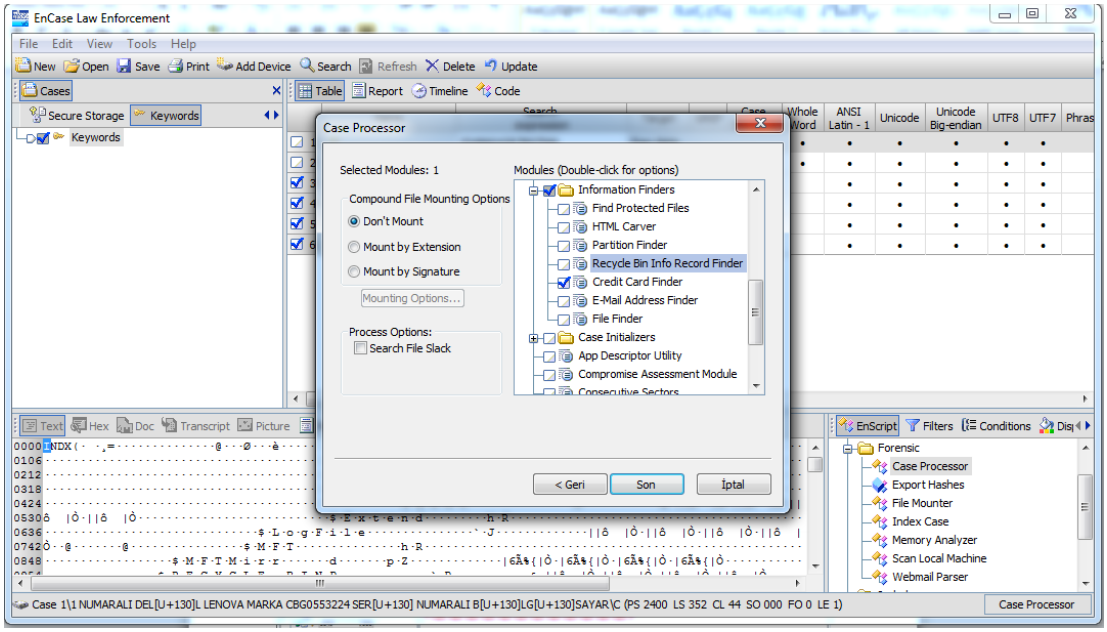
Şekil 4.9 EnCase Programı Anahtar Kelimeler

Şekil 4.10'da Encase programı aranan ve bulunan kredi kartı numaraları gösterilmiştir. Burada gösterildiği gibi hepsiburada adındaki bir metin dosyası içerisinde kredi kartı bilgilerinin saklandığı tespit edilmiştir.

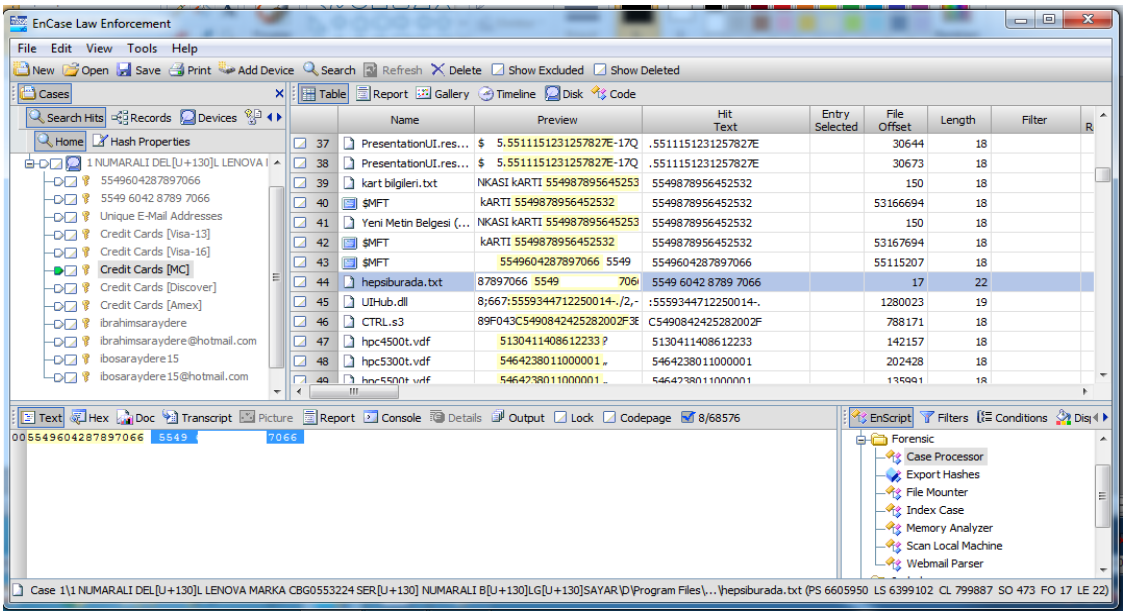


Şekil 4.10 EnCase Programı Bulunan Kelimeler Ara Yüzü

Yine Encase Programının Olay İşlemcisi (Case Processor) bölümünde bulunan Kredi kartı bulucu (Credit Card Finder) sekmesine tıklayarak bilgisayar içerisinde kullanılan tüm kredi kartı bilgileri bulunmaya çalışılmış bu bölümde de İbrahim Saraydere isimli şahsın kullanmış olduğu 5549 **** *** 7066 numaralara rastlanılmıştır. Şekil 4.11'de EnCase Programı Kredi Kartı Bulucu Ekran Ara Yüzü gösterilmiştir.



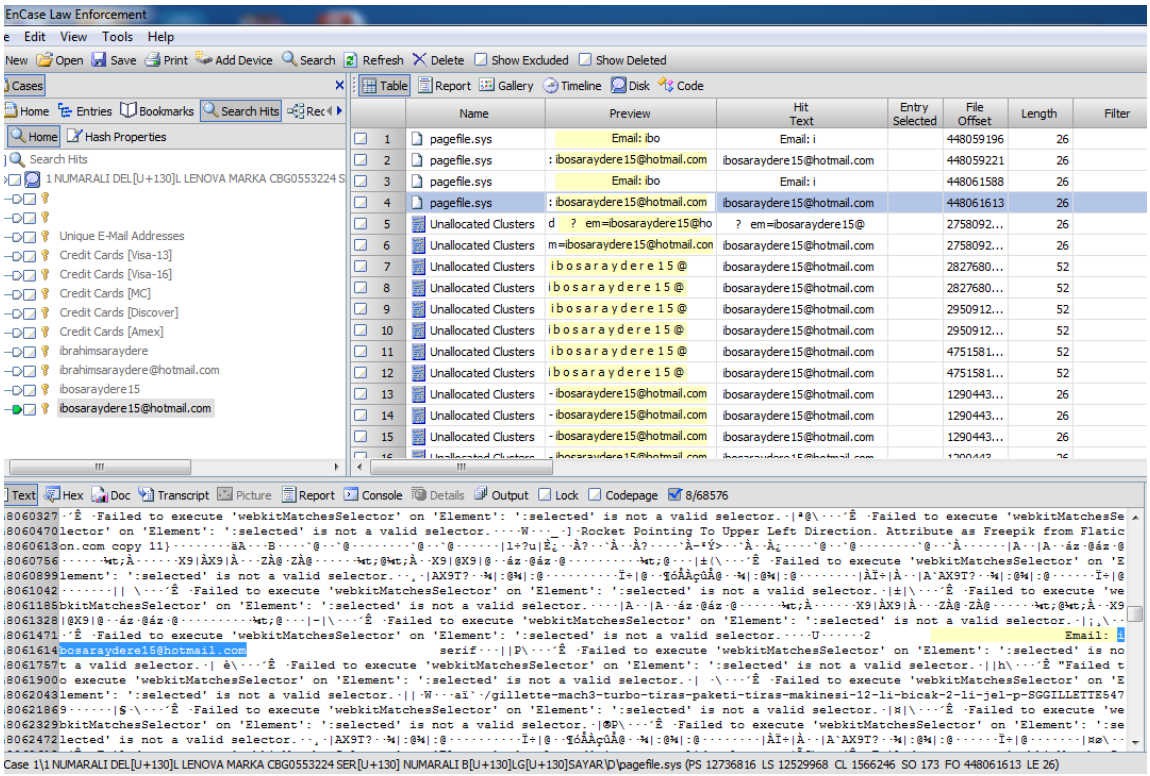
Şekil 4.11 EnCase Programı Kredi Kartı Bulucu Ekran Ara Yüzü



Şekil 4.12 EnCase Programı Kredi Kartı Sonuç Ekran Ara Yüzü

Kelime (Keywords) yazma yöntemiyle ibosaraydere15@hotmail.com isimli mail adresinin şifresinin kırılarak bu bilgisayarda kullanılıp kullanılmadığı tespit edilmeye çalışılmış ve ibosaraydere15@hotmail.com isimli mail adresi bu bilgisayarda erişim sağlandığı belirlenmiştir.

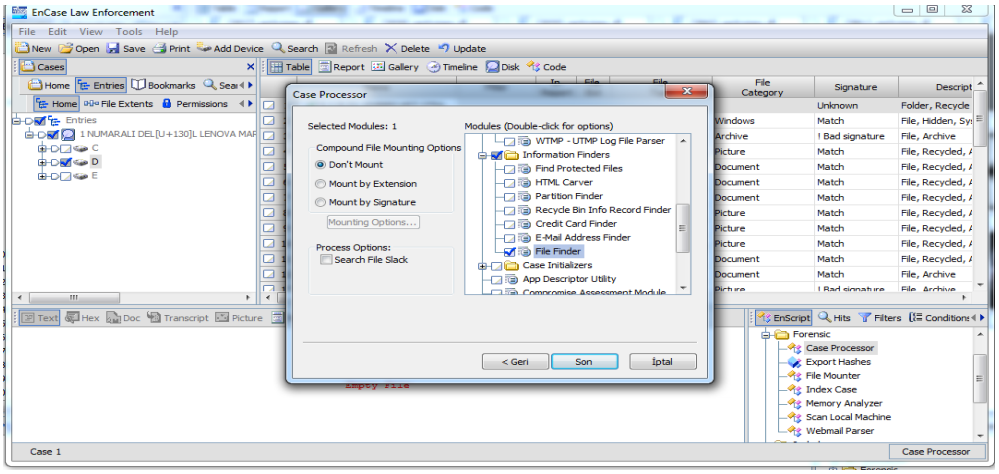
İbosaraydere15@hotmail.com isimli mail adresi bilgisayar içerisinde bulunan pagefile.sys isimli alandan tespit edilmiş pagefile.sys (pagefile.sys dosyası işletim sisteminin sanal bellek dosyasıdır. Sanal bellek dosyası, sabit diskin bir bölümünü bellek olarak kullanmaktadır. ibosaraydree15@hotmail.com isimli mail adresi bu bilgisayarda kullanılmıştır. Şekil 4.13'de EnCase Programı kelime aratma sonuç ekranı ara yüzü verilmiştir.



Şekil 4.13 EnCase Programı Kelime Aratma Sonuç Ekranı Ara Yüzü

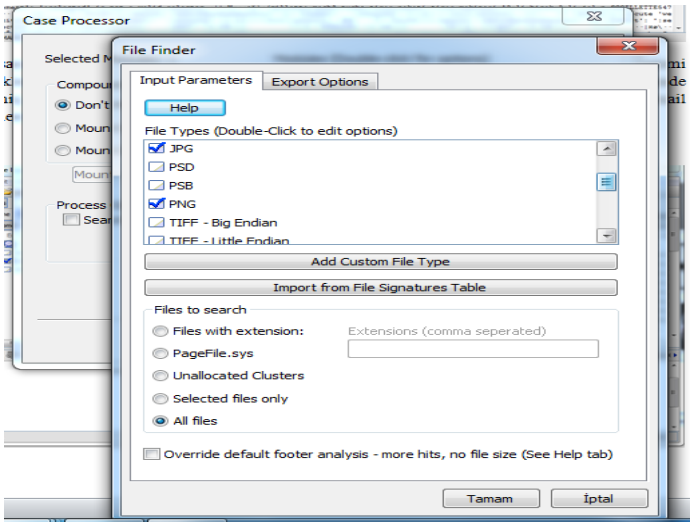
Bilgisayar içerisinde silinmiş belgelerin tespiti amacıyla Kurtarma (Recovery) işlemi gerçekleştirilerek silinmiş veriler üzerinden delil elde edilmeye çalışılmış bilgisayar içerisinde silinmiş olarak kredi kartı fotoğrafları, kredi kartı kopyalama cihazları ve kredi kartı ve mail adresleri metin bilgilerine ulaşılmıştır. Kurtarma (Recovery) işlemi aşağıda açıklanmıştır.

Sol aşağıda bulunan Dava İşlemcisi (Case Processor) sekmesine tıklanarak Bilgi Bulucular (İnformation Finders) sekmesi tıklanır. Sonra Dosya bulucu (File Finder) sekmesi tıklanır. Bu sekme içerisinde bulunan hangi silinmiş dosya uzantılarını bulmak istiyorsak o sekme tıklanır. Sonra tamam diyerek bilgisayar içerisinde silinmiş bilgiler bulunmaya başlanır. Şekil 4.14 Encase programı Silinmiş belgeler ara yüzü gösterilmiştir.



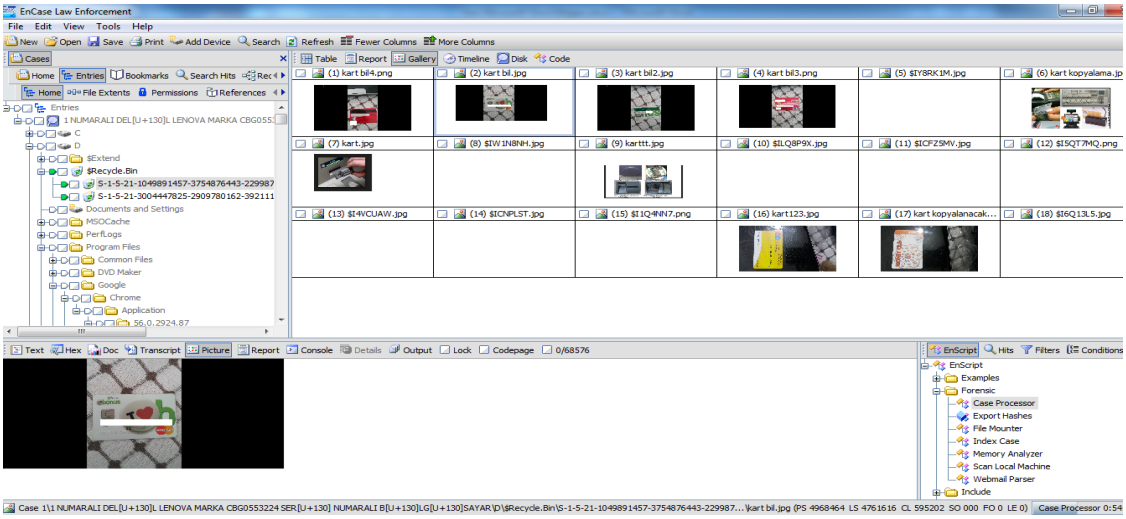
Şekil 4.14 EnCase Programı Silinmiş Belgelerde Arama Ekran Ara Yüzü 1

Şekil 4.15 Encase programı Silinmiş belgeler ara yüzü dosya uzantıları verilmiştir. Burada bilinen dosyaların uzantıları verilmektedir. Bunun yanında kullanıcı yeni programların uzantılarını da tanımlayabilmektedir.



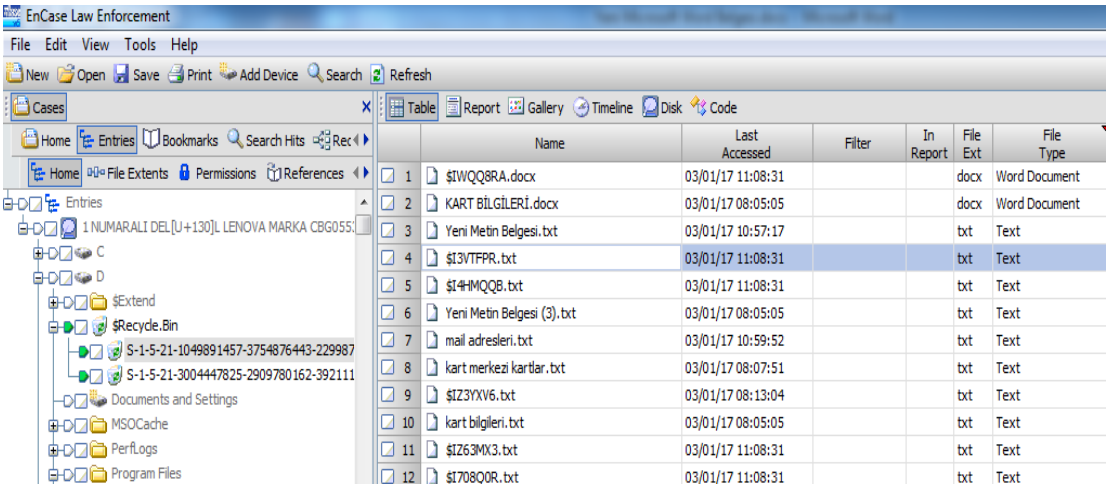
Şekil 4.15 EnCase Programı Silinmiş Belgelerde Arama Ekran Arama Yüzü 2

Silinmiş belgeler içerisinde yapılan fotoğraf aramalarında Kart bil.jpg, Kart bil2.jpg, Kart bil3.jpg, Kart bil4.png, Kart kopyalama.jpg, KartKopyalanacak444.jpg, Kart.jpg, Kart123.jpg, Karttt.jpeg, Kredi kartı kopyalama güvendemisin.com.flv, isimli fotoğraf ve video dosyalarına rastlanılmıştır. Şekil 4.16'da EnCase programı silinmiş belgeler fotoğraflar sonuç ekranı gösterilmiştir.



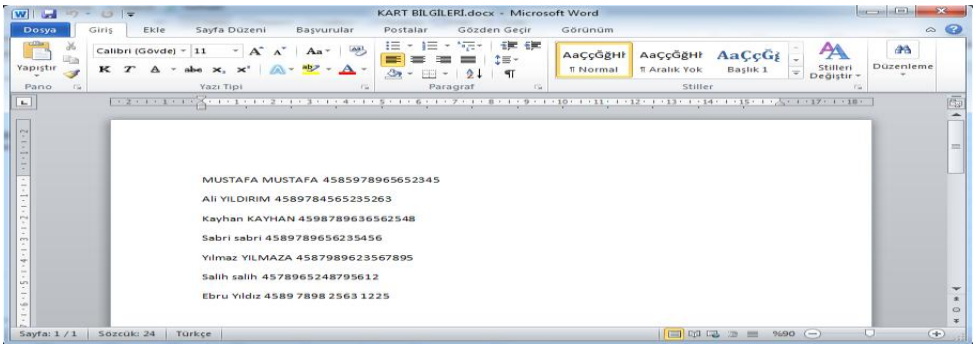
Şekil 4.16 EnCase Programı Silinmiş Belgeler Fotoğraflar Sonuç Ekranı 1

Silinmiş belgeler içerisinde yapılan metin KART BİLGİLERİ.docx, Kart bilgileri.txt, Kart merkezi kartlar.rar, Kart merkezi kartlar.txt, Mail adresleri.txt, Yeni Metin Belgesi(3).txt uzantılı dosyalara ulaşılmıştır. Şekil 4.17'de EnCase Programı Silinmiş Metin Belgeleri Sonuç Ekranı gösterilmiştir.



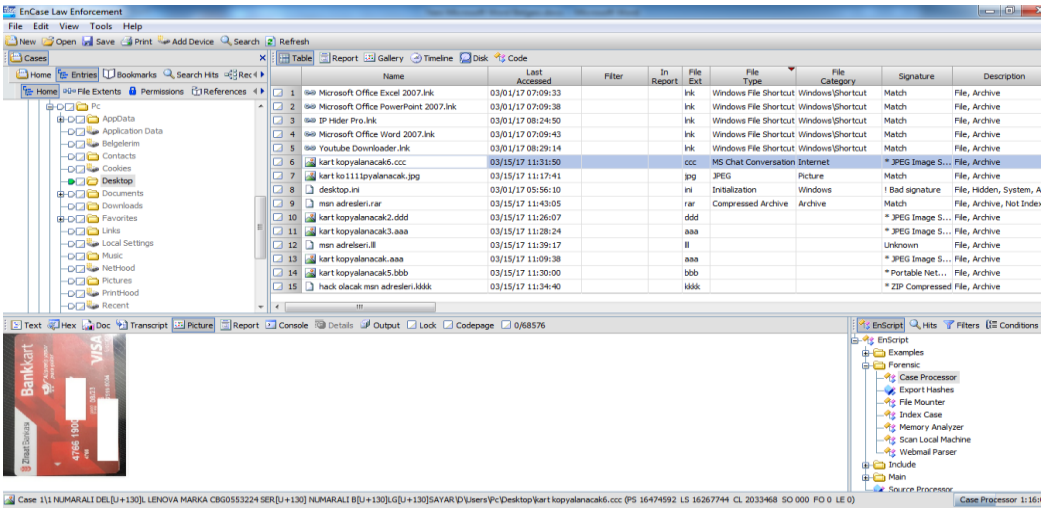
Şekil 4.17 EnCase Programı Silinmiş Belgeler Sonuç Ekranı

KART BİLGİLERİ.docx isimli klasör açıldığında içerisinde isimler ve kart numaraları olan bilgilere rastlanılmıştır. Şekil 4.18'de Kart bilgileri dosyanın açılmış hali verilmiştir.



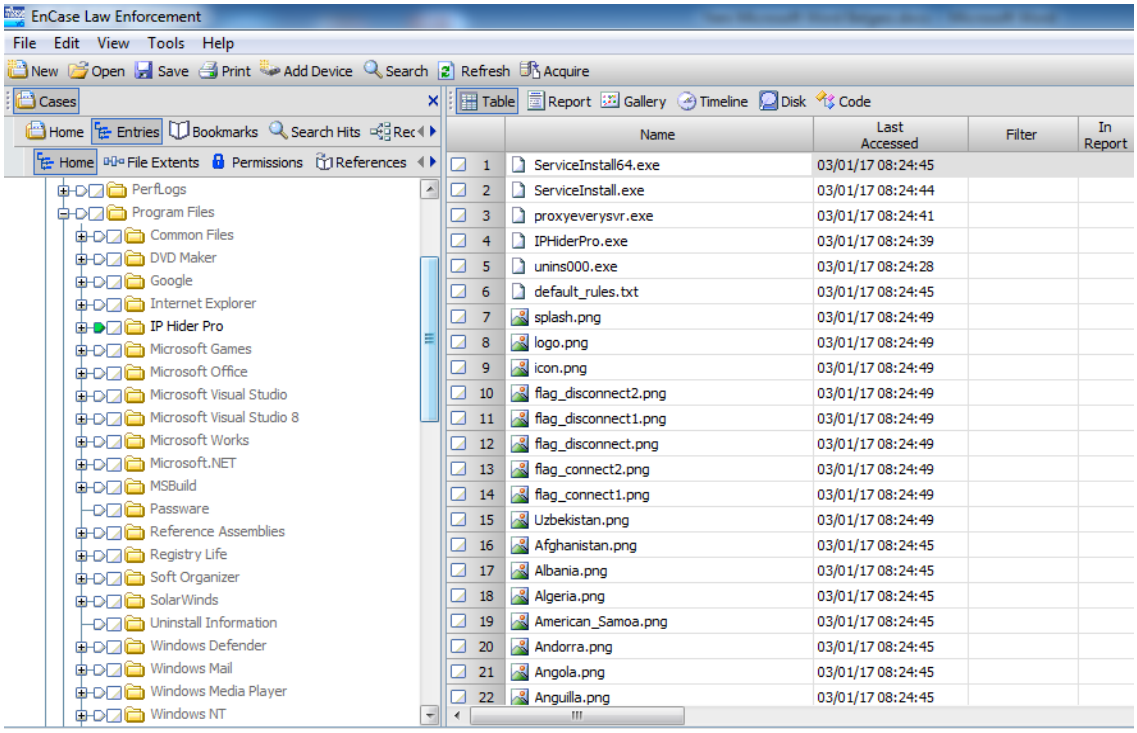
Şekil 4.18 Kart Bilgileri Dosyası

Bilgisayarın yapılan ayrıntılı incelemesinde kullanıcının masaüstünde kart kopyalanacak6.ccc, hack olacak msn adresleri.lll, kart ko1111pyalanacak.jpg, kart kopyalanacak.aaa, kart kopyalanacak2.ddd, kart kopyalanacak3.aaa, kart kopyalanacak5.bbb, msn adrelseri.lll isimli uzantıları değiştirilmiş dosyalara ulaşılmış Encase programı vasıtasıyla yapılan incelemede bu uzantıları değiştirilmiş dosyaların gerçek uzantıların JPEG fotoğraf belgesi olduğu anlaşılmıştır. Msn adresleri isimli klasörün gerçek uzantısının txt Hack olacak msn adresleri isimli dosyanın ise rar uzantılı dosya olduğu anlaşılmış ve şekil 4.19'da bu uzantısı değiştirilmiş dosyalar gösterilmiştir.



Şekil 4.19 Encase Dosya Uzantıları

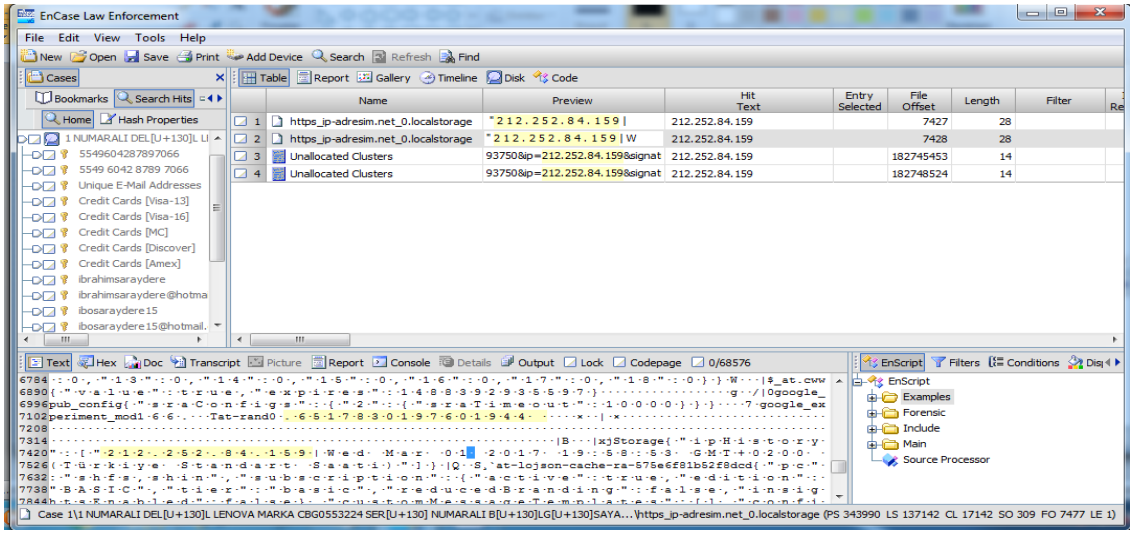
Bilgisayarın kullanıcı programları incelendiğinde bilgisayar kullanıcının İp adreslerini değiştirmek için kullandığı IP Hider Pro ve Hard disk temizleme internet geçmişini silmek için kullanılan Registry File isimli programlara rastlanılmış bu programların ekran görüntüsü aşağıya çıkartılmıştır. Şekil 4.20'de bilgisayar içerisinde kullanılan programlar verilmiştir.



Şekil 4.20 Bilgisayar İçerisinde Kullanılan Programların Ekran Görüntüsü

Bilgisayarın 212.252.84.159 IP adresini kullanıp kullanmadığı tespit edilmeye çalışılmış 212.252.84.159 IP numarasının bilgisayarda kullanıldığı tespit edilmiştir. Kelime (Keywords) yazma yöntemiyle 212.252.84.159 IP numarasının bilgisayarda kullanıldığı şekil 4.21'de verilmiştir.

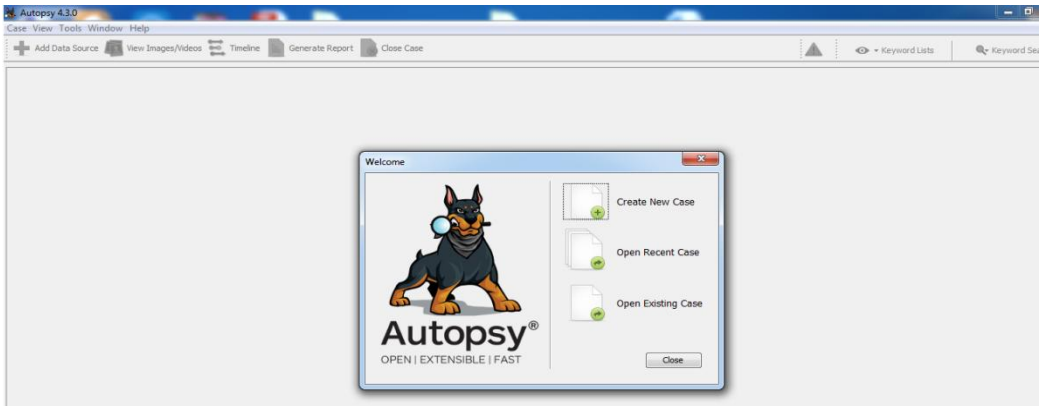
Bilgisayar içerisinde https_ip-adŞekil.net_0.localstorage log kayıtlarında 212.252.84.159 IP numarasına rastlanılmış ve bu IP adresinin bu bilgisayarda kullanıldığı tespit edilmiştir.



Şekil 4.21 IP Tesbit Ekran Görüntüsü

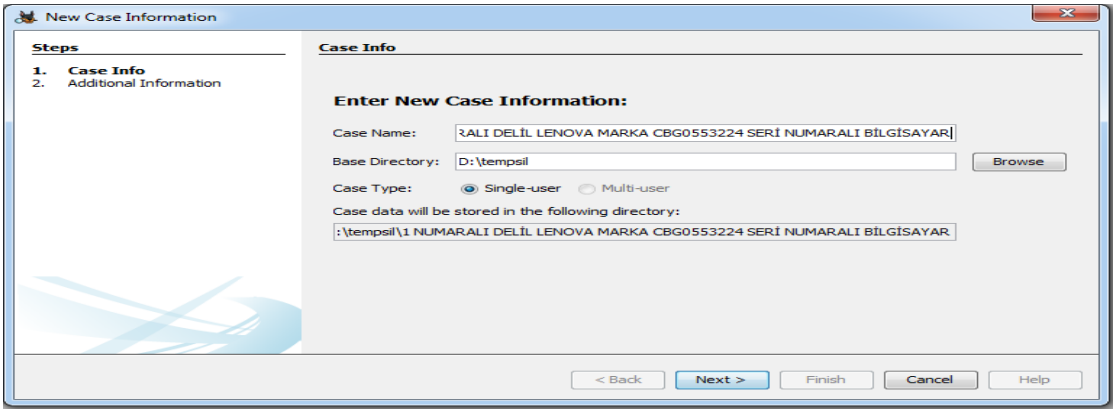
4.2 Autopsy Ücretsiz Adli İnceleme Yazılımı ile Hard Disk İnceleme

Autopsy yazılımı daha çok Linux işletim sistemlerinde çalışan açık kaynak kodlu geliştirilebilir adli bilişim inceleme yazılımıdır. Geliştiriciler son zamanlarda Windows versiyonunu da piyasaya sürmüştür. Autopsy yazılımın inceleme mantığı indeksleme sistemi ile çalışmaktadır. İndeksleme mantığı ise hard diskin program tarafından tüm bilgilerin çıkartılarak programa tanıtılmasıdır. Sonra programın belirli sekmeleri vasıtasıyla istediğimiz işlemlere tıklayarak program yapılmak istenilen bilgileri program vakit kaybetmeksizin çıkartmaktadır. Autopsy yazılımı imaj alma işlemi yapamamakta sadece incelme yapmaktadır. Aşağıda senaryo gereği Autopsy yazılımı ile hard disk incelenmiş ve sonuçları çıkartılmıştır. Autopsy yazılımın ekran görüntüsü Şekil 4.22'da gösterilmiştir.



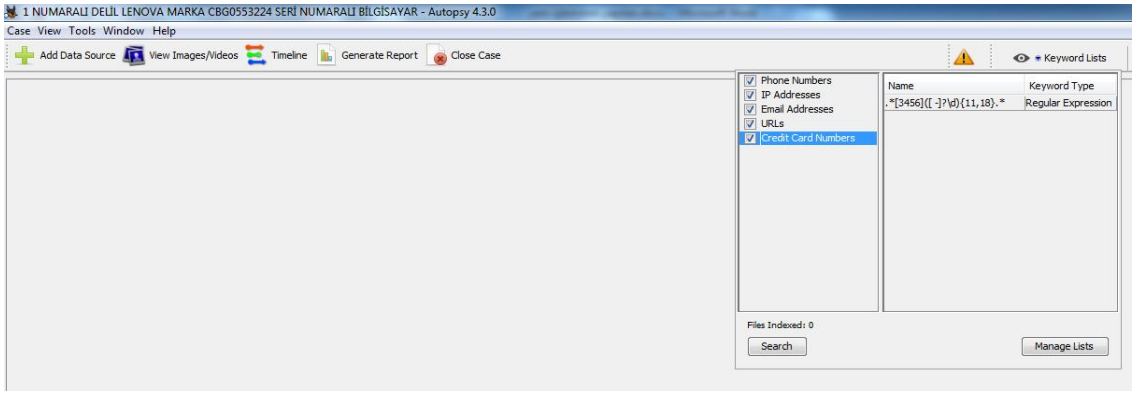
Şekil 4.22 Autos Yazılımın Ana Ekran Ara Yüz Görüntüsü

Yeni Olay Yarat (Create New Case) sekmesine tıklanarak yeni olayı oluşturulur. Şekil 4.23'de Yeni Olay Yaratma Ara Yüz Görüntüsü verilmiştir.

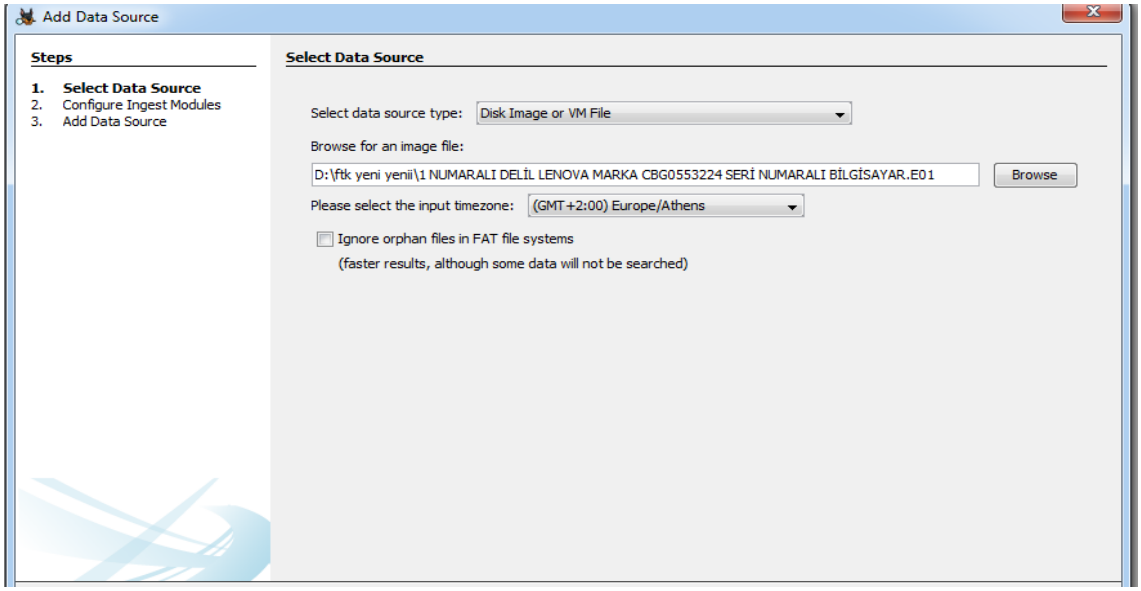


Şekil 4.23 Yeni Olay Yaratma Ara Yüz Görüntüsü

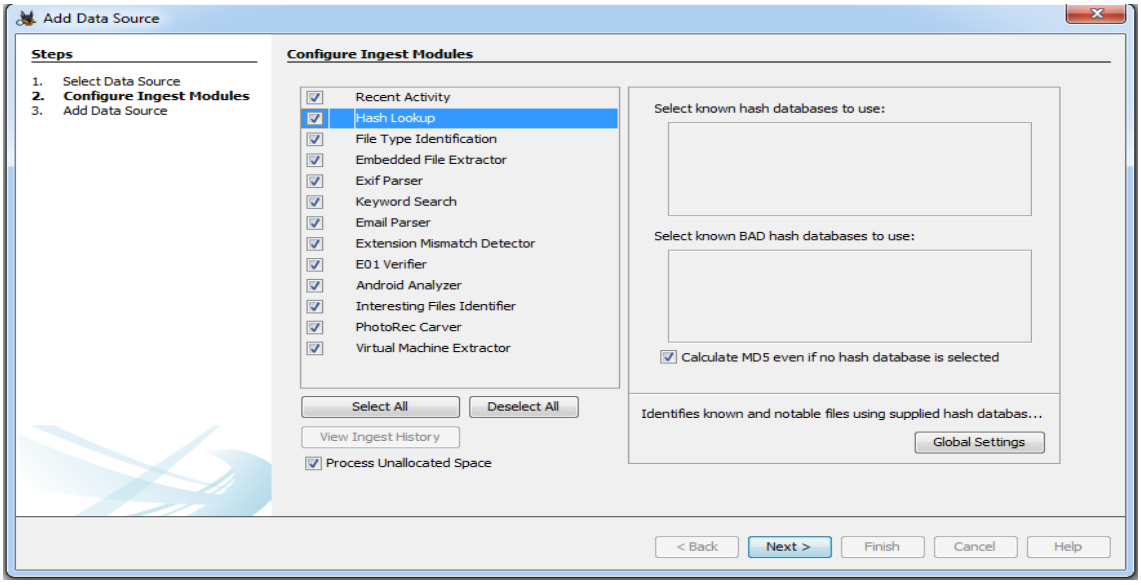
Bilgileri girdikten sonra İleri (Next) sekmesine tıklanarak programda yeni dava olay oluşturulur. Programı açıldıktan sonra sağ üst köşede bulunan Anahtar Kelime Listesi (Keyword List) tıklanır ve içerisinden Telefon Numarası (Phone Number), İp Adresi (Ip Addreses), E mail adresi (Email Addreses), İnternet Geçmişi (Urls), Kredi Kartı Numaraları (Credit Card Number) çentiklerinin hepsi tıklanır. Sonra Programın sol üst köşesinde bulunan veri kaynağı ekle (Add Data Source) kısmından daha önce aldığımız E.01 uzantılı imajı programa tanıtıyoruz. İleri (Next) sekmesi tıklanarak programda ne aratmak istediğimiz sekmesi gelir ve hepsine çentik atarak ilerlenir ve Bitiş (Finish) sekmesi tıklanarak programda indeksleme işlemine başlanır. Şekil 4.24 4.25 ve 4.26'de indeksleme işlemi ekran görüntüsü verilmiştir.



Şekil 4.24 İndeksleme İşlemi Ekran Görüntüsü-1



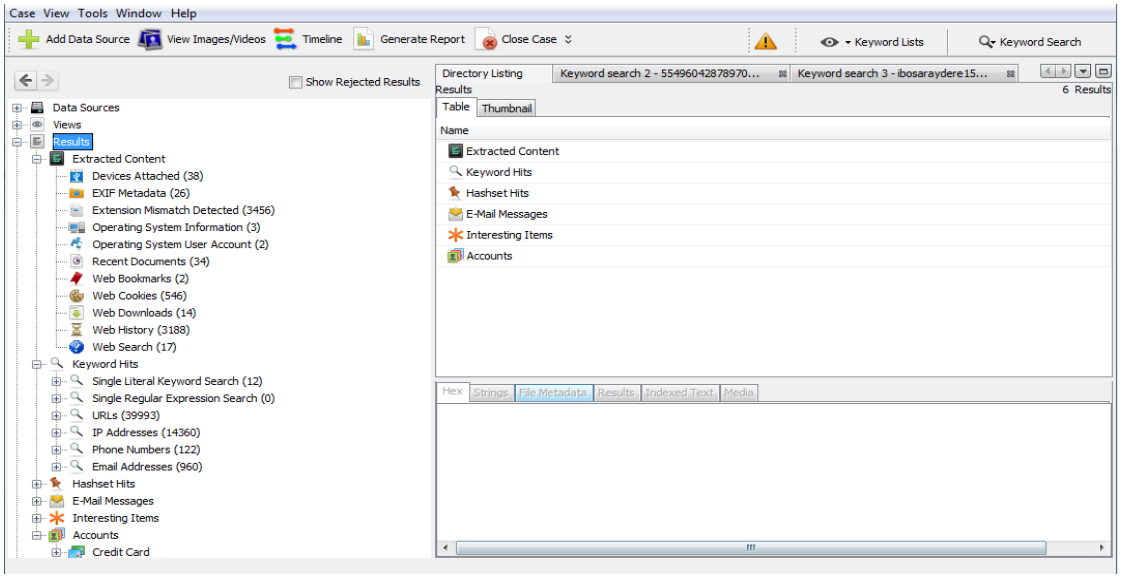
Şekil 4.25 İndeksleme İşlemi Ekran Görüntüsü-2



Şekil 4.26 İndeksleme İşlemi Ekran Görüntüsü-3

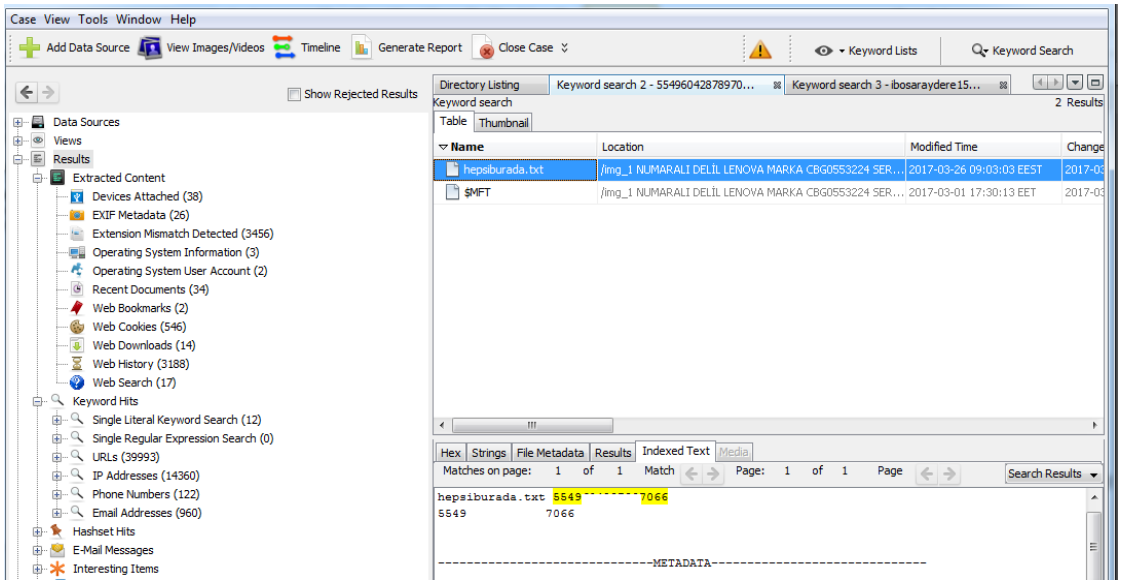
İndeksleme işlemi bittikten sonra seçmek artık işleme yazılımın sağ tarafında bulunan sekmelerinden yola çıkarak devam edilecektir.

Aşağıda gösterilen Şekilde Anahtar Kelime Aramasına (Keyword Search) kısmına tıklanarak ibosaraydere@hotmail.com ve 5549 **** *** 7066 numaralı kart bilgisi aranmış ve çıkan sonuçlarda bu bilgisayarda bu mail adresi ve kart bilgisinin kullanıldığı tespit edilmiştir. Şekil 4.27'de arama ekran görüntüsü verilmiştir.



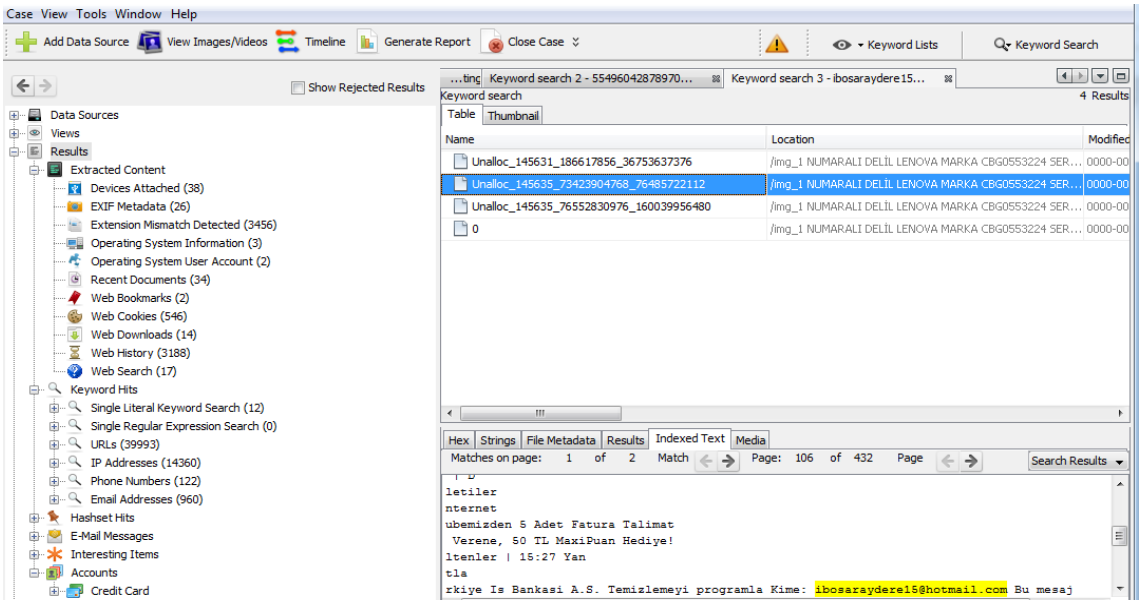
Şekil 4.27 Arama Ekran Görüntüsü

5549 **** *** 7066 numaralı kart bilgisin ekran görüntüsü Şekil 4.24'de verilmiştir.



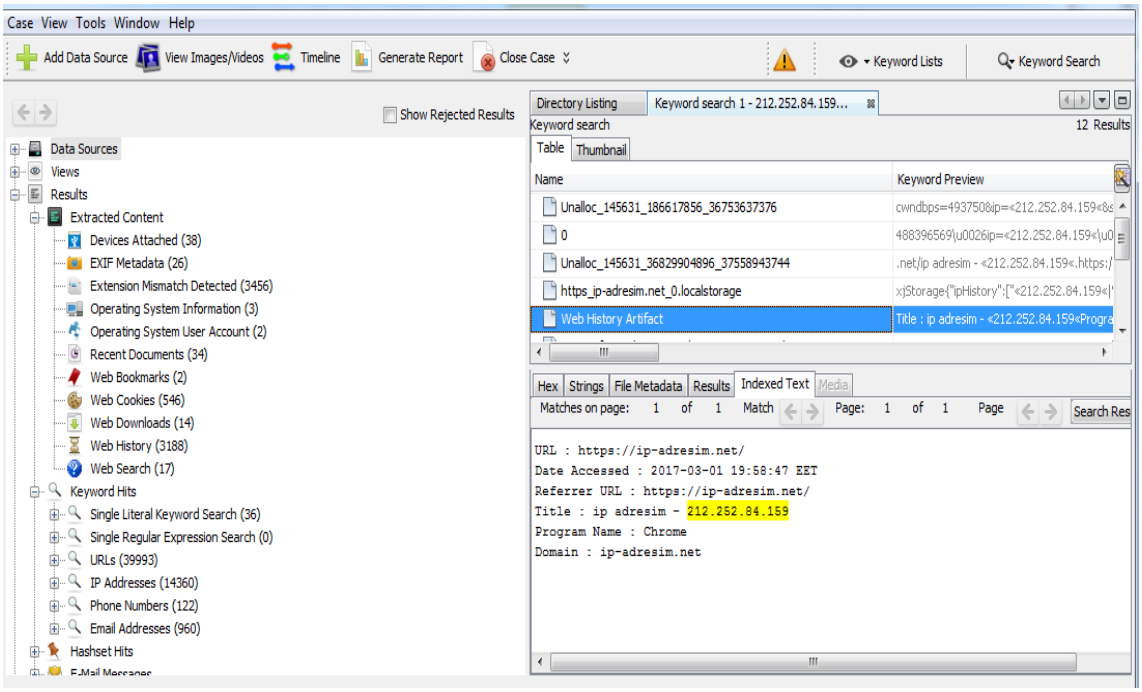
Şekil 4.28 Kart Bilgisi Ekran Görüntüsü

ibosaraydere@hotmail.com mail adresinin ekran görüntüsü şekil 4.29'da verilmiştir.



Şekil 4.29 Mail Adresi Ekran Görüntüsü

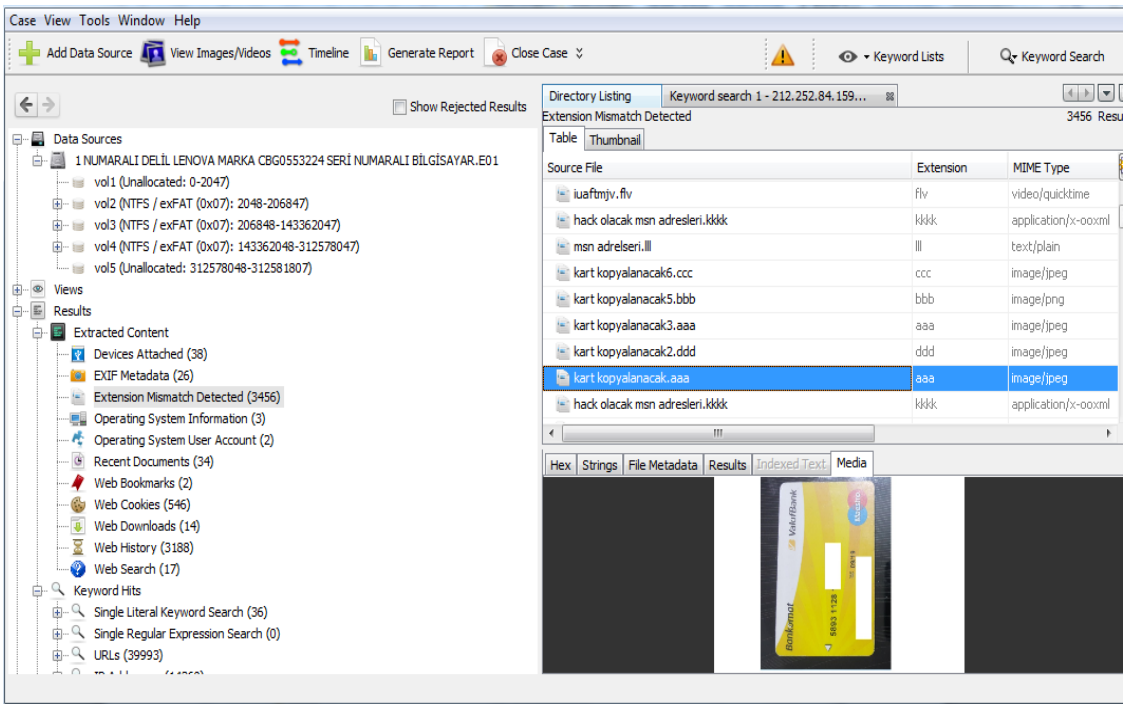
Bilgisayar içerisinde 212.252.84.159 IP numarasına web geçmiş izleri nde (Web History Artifact) rastlanılmış ve bu IP adresinin bu bilgisayarda kullanıldığı tespit edilmiştir. Şekil 4.30'da Ip adresi tespit ekranı görüntüsü verilmiştir.



Şekil 4.30 IP Adresi Tesbiti Ekran Görüntüsü

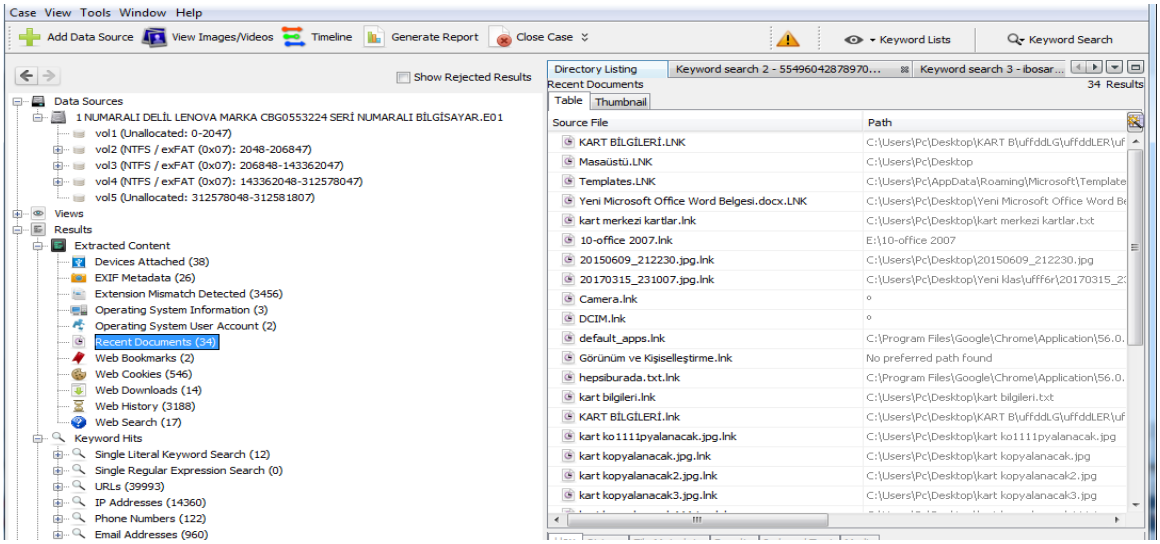
Sağ taraftaki bulunan Uzantı Uyumsuzluğu Tespiti (Extension mismatch detec) kısmında uzantısı değiştirilmiş olan kart kopyalanacak6.ccc, hack olacak msn

adresleri.lll, kart ko1111pyalanacak.jpg, kart kopyalanacak.aaa, kart kopyalanacak2.ddd, kart kopyalanacak3.aaa, kart kopyalanacak5.bbb, isimli uzantıları değiştirilmiş dosyalara ulaşılmış Autopsy programı vasıtasıyla yapılan incelemede bu uzantıları değiştirilmiş dosyaların gerçek uzantıların JPEG fotoğraf belgesi olduğu anlaşılmıştır. Msn adresleri isimli klasörün gerçek uzantısının txt, Hack olacak msn adresleri isimli dosyanın ise rar uzantılı dosya olduğu anlaşılmış bulunan ekran görüntüleri aşağıya çıkartılmıştır. Şekil 4.31'de uzantısı değiştirilmiş belgeler ekran görüntüsü verilmiştir.



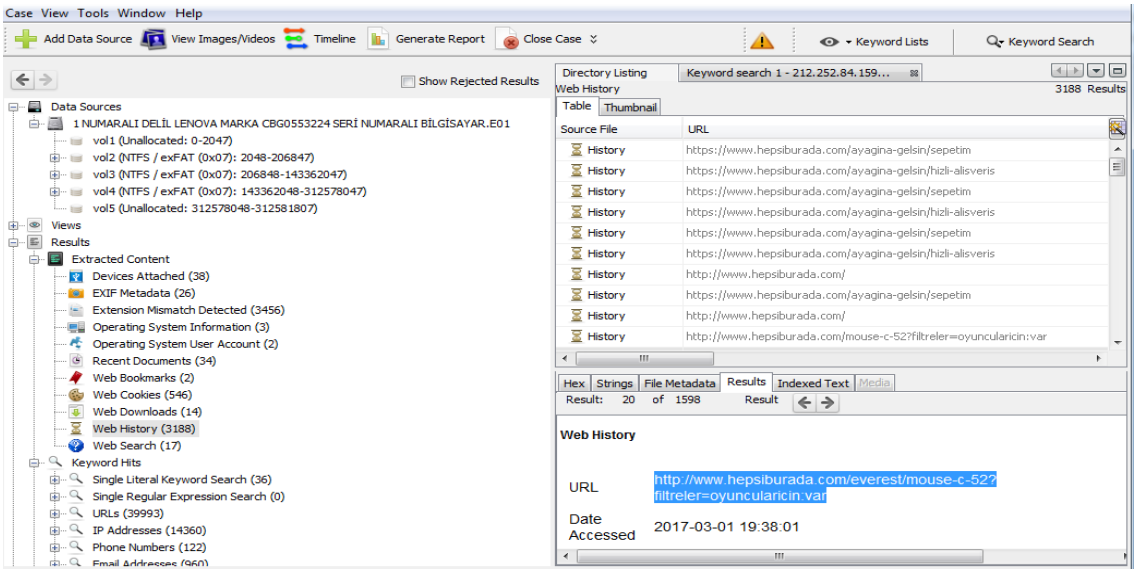
Şekil 4.31 Uzantısı Değiştirilmiş Belgeler Ekran Görüntüsü

Sağ taraftaki bulunan Son Dökümanlar (Recent Documents) kısmında bilgisayar içerisinden silinmiş belgeler olan Kart bil.jpg,Kart bil2.jpg,Kart bil3.jpg,Kart bil4.png, ,Kart kopyalama.jpg,KartKopyalanacak444.jpg ,Kart.jpg, Kart123.jpg, Karttt.jpeg,Kredi kartı kopyalama güvendemisin.com.flv, isimli fotoğraf, video dosyasına KART BİLGİLERİ.docx, Kart bilgileri.txt, Kart merkezi kartlar.rar, Kart merkezi kartlar.txt, Mail adresleri.txt,Yeni Metin Belgesi(3).txt uzantılı metin dosyalara ulaşılmıştır.Şekil 4.32'de silinmiş belgeler ekran görüntüsü verilmiştir.



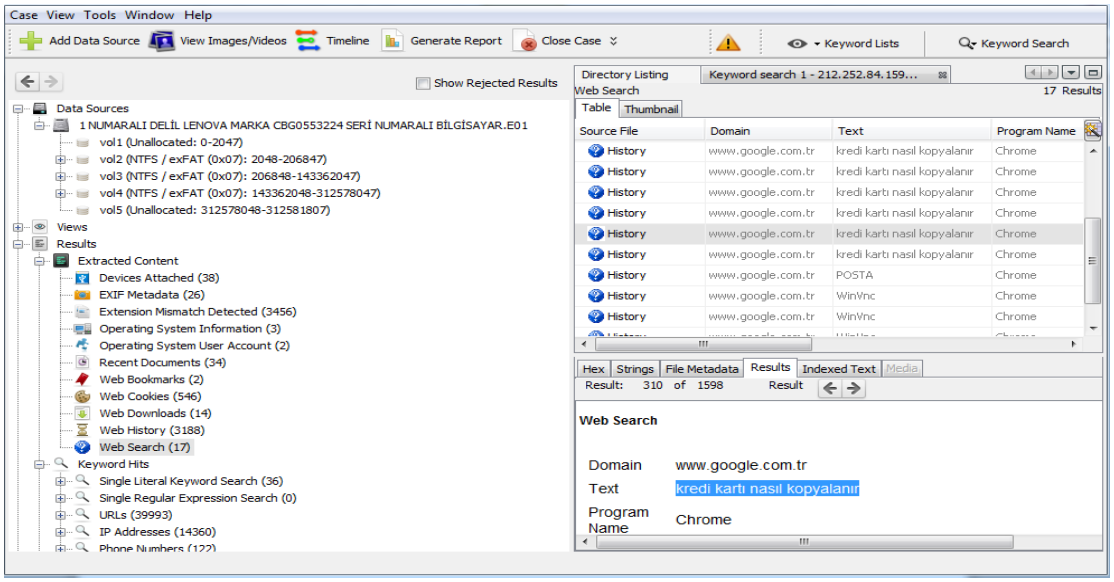
Şekil 4.32 Silinmiş Belgeler Ekran Görüntüsü

Sağ taraftaki bulunan İnternet Geçmişi (Web History) kısmında http://www.hepsiburada.com/ everest/mouse -c-52?filtreler=oyuncularicin:var isimli web sitesine giriş yapıldığı tespit edilmiştir. Şekil 4.33'de sitelere erişim ekran görüntüsü verilmiştir.



Şekil 4.33 Sitelere Erişim Ekran Görüntüsü-1

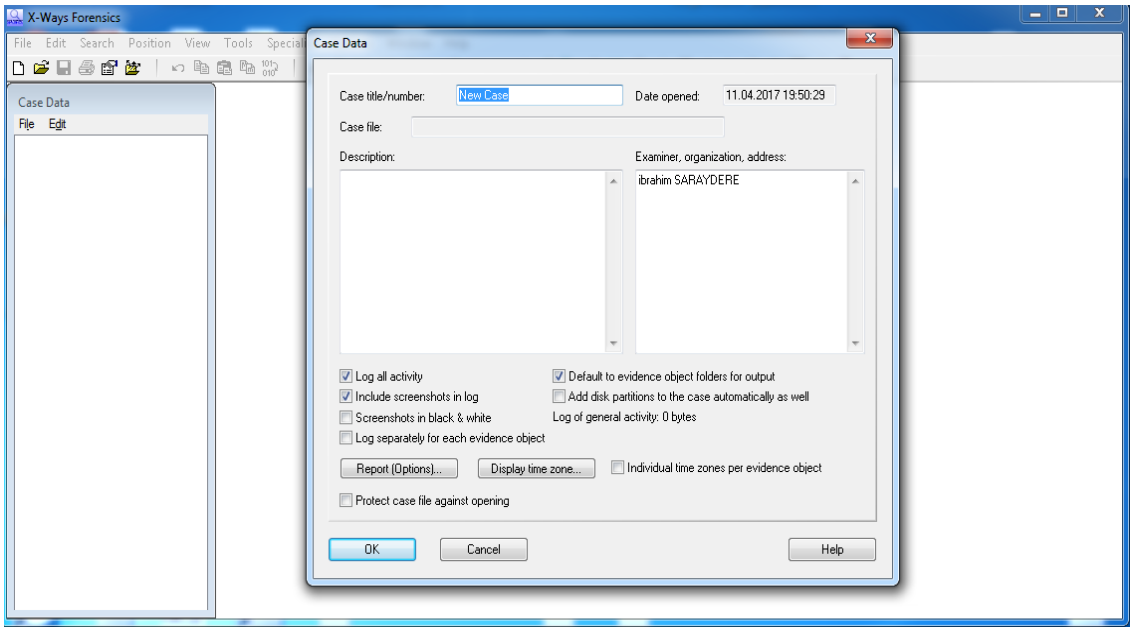
Sağ taraftaki bulunan İnternette Arama (Web Search) kısmında bilgisayar kullanıcısının internet tarayıcısı olan Google Crome da aranan kelimeler kısmında 'kredi kartı nasıl kopyalanır' şeklinde arama yapıldığı tespit edilmiştir. Şekil 4.34'de sitelere erişim ekran görüntüsü verilmiştir.



Şekil 4.34 Sitelere Erişim Ekran Görüntüsü-2

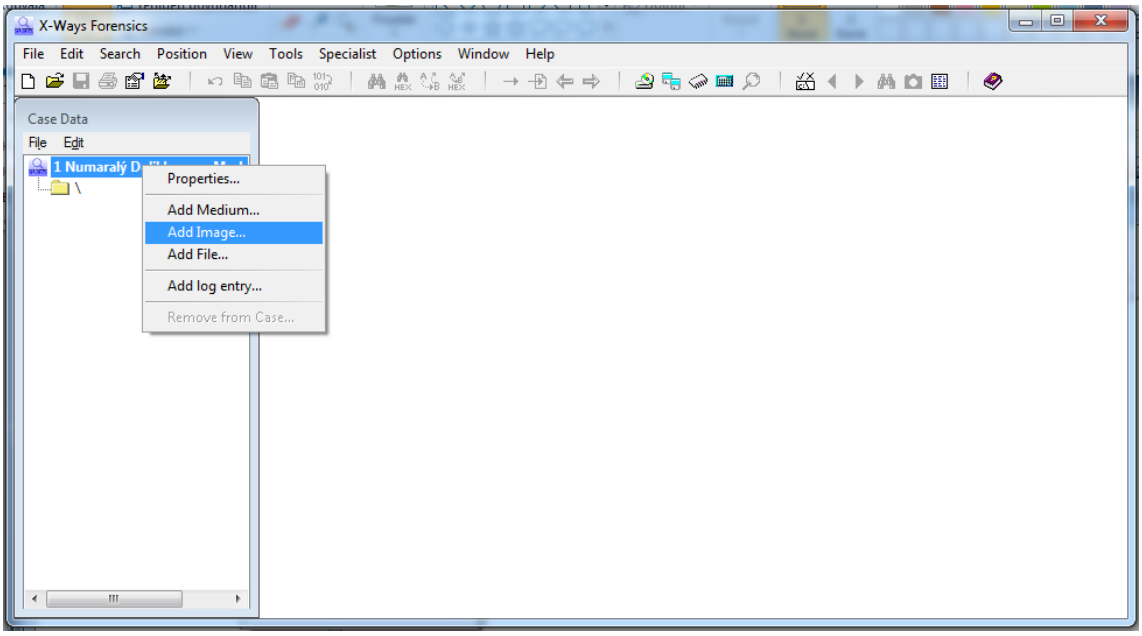
4.3 X WAYS Yazılımı

X ways yazılımı açıldıktan sonra sol üstte bulunan Dosya (File) sekmesinden Yeni Olay Oluştur (Create New Case) tıklanır. Sonra Vaka Numarası(Case the/number) kısmı ve İnceleyen(Examiner, Organization,) kısmı doldurulur. Tamam (Ok) kısmına tıklanarak yeni olay oluşturulur. X-Ways yazılımın ekran görüntüsü Şekil 4.35'da gösterilmiştir.



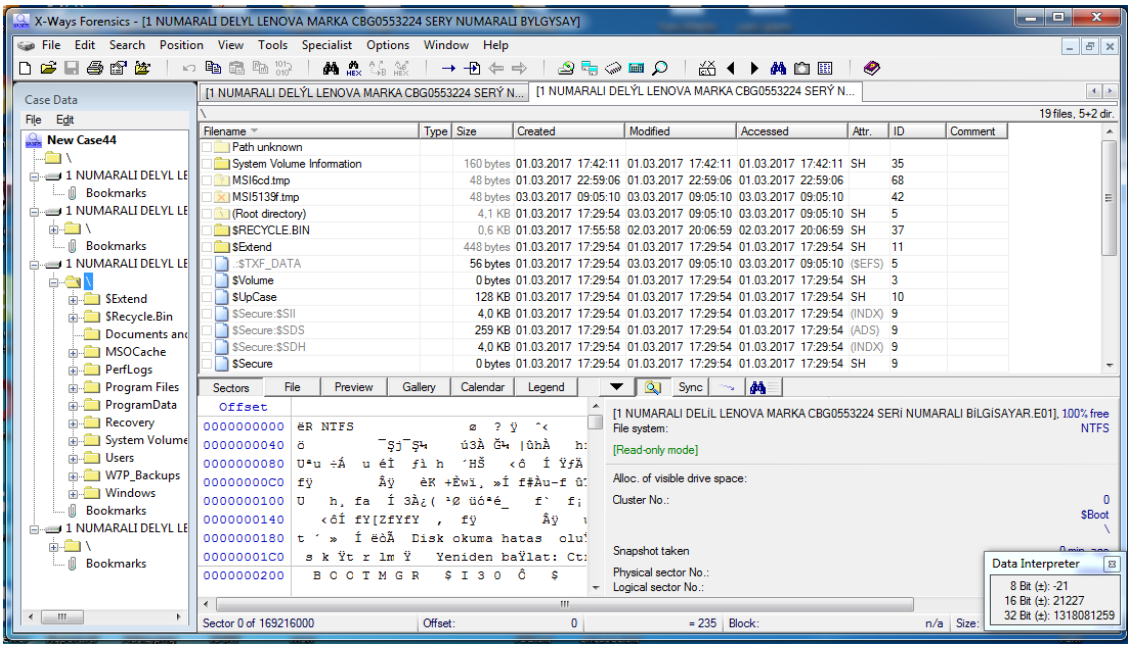
Şekil 4.35 X Ways Yazılımı Yeni Olay Oluşturma Ekran Ara Yüzü

Oluşturulan olayın üzerine sağ tıklanarak İmaj Ekle (Add İmage) kısmı tıklanır ve alınan imaj yazılıma eklenir. Şekil 4.36'da X Ways Yazılımı İmaj Ekleme Ekran Ara Yüzü verilmiştir.



Şekil 4.36 X Ways Yazılımı İmaj Ekleme Ekran Ara Yüzü

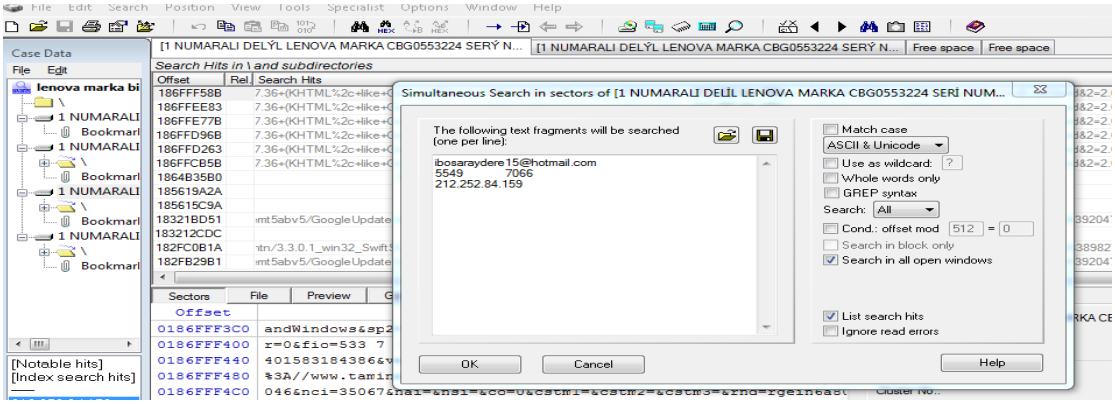
X WAYS yazılımına imaj açılmış ekran görüntüsü şekil 4.37'de verilmiştir.



Şekil 4.37 X Ways Yazılımı İmaj Açılmış Ekran Ara Yüzü

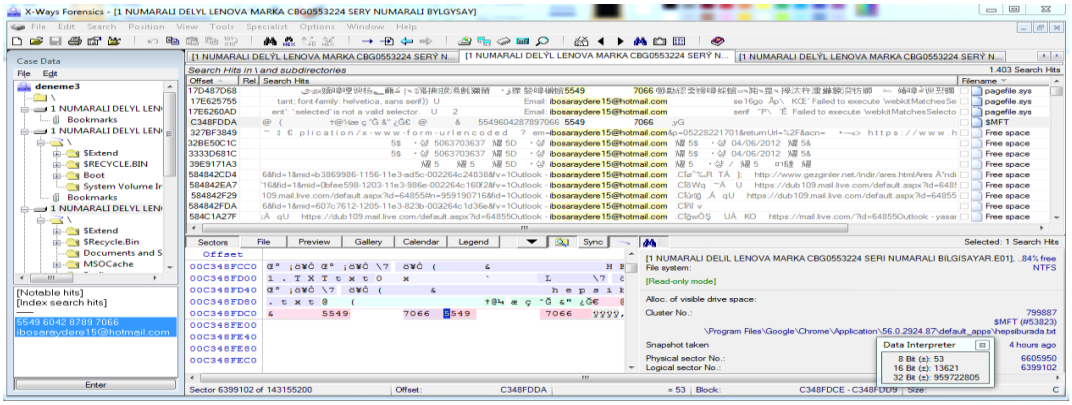
Xways Yazılımın Anahtar Kelime (Keywords) taraması yapılarak 5549 **** **** 7066 numaralı kart bilgisinin ekran görüntü şekil 4.38' de verilmiştir.

Xways yazılımının üst sekmesinde bulunan Arama(Search) kısmına tıklanır. Sonra çıkan Sektörler içerisinde Anlık Arama (Simultaneus Search In Sectors Of) kısmına tıklanır. Çıkan boşluk alana aratmak istenilen kelimeler yazılarak tamam (Ok) kısmına tıklanarak arama işlemine başlanır.



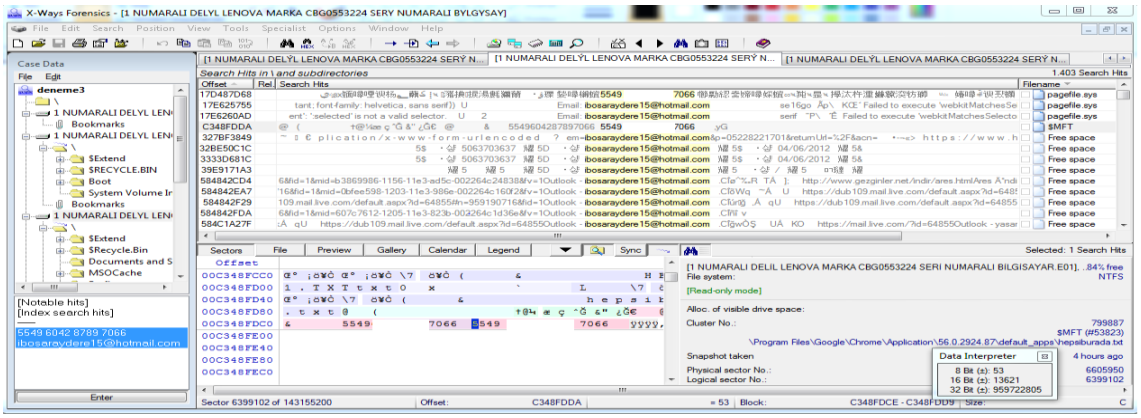
Şekil 4.38 X Ways Yazılımı Kelime Aratma Ekran Ara Yüzü

5549 **** **** 7066 isimli kart numaraları program vasıtasıyla taratılmış ve MFT kayıt tablosunda 5549 **** *** 7066 numaralara rastlanılmıştır. MFT kayıt tablosu ise Master File Tablo kelimelerinin kısalmasıdır. Yani bir bilgisayar sistemi içerisinde NFTS dosya sistemi içerisinde tüm dosyaların izlemesini yapar. Dosyalara ait konum bilgilerini hangi dizine ait fiziksel metadataları içerir. Şekil 4.39'da X Ways Yazılımı kredi kartı Sonuç Ekran Ara Yüzü verilmiştir.



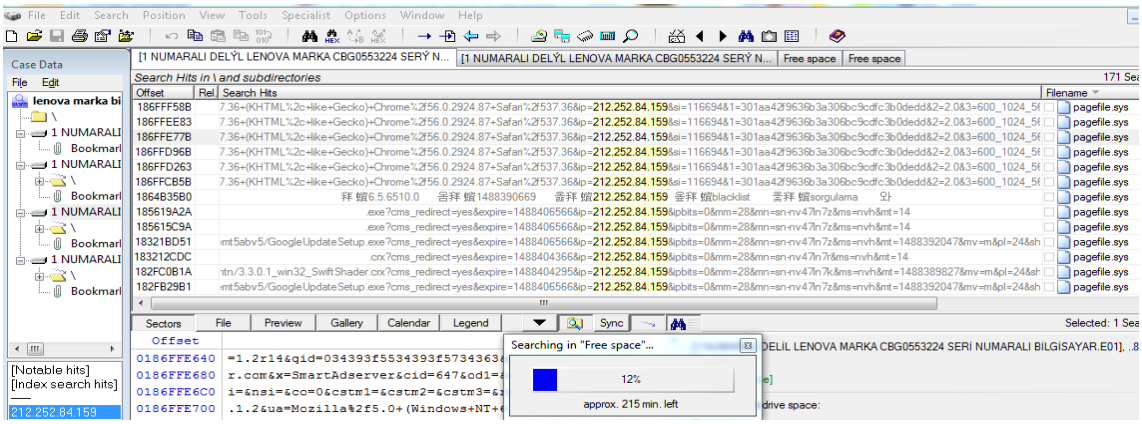
Şekil 4.39 X Ways Yazılımı Kredi Kartı Sonuç Ekran Ara Yüzü

Xways yazılımın Anahtar Kelime (Keywords) taraması yapılarak ibosaraydere15@hotmail.com elektronik posta adresi bilgisayar içerisinde bulunan pagefile.sys isimli alandan tespit edilmiş pagefile.sys (Pagefile.sys dosyası işletim sisteminin sanal bellek dosyasıdır. Sanal bellek dosyası, sabit diskin bir bölümünü bellek olarak kullanımı sağladığından gizli bir sistem dosyası olarak karşımıza çıkmaktadır). ibosaraydere15@hotmail.com isimli elektronik posta adreside bu bilgisayarda kullanıldığı tespit edilmiştir. Şekil 4.40'da X Ways yazılımı mail adresi sonuç ekran ara yüzü verilmiştir.



Şekil 4.40 X Ways Yazılımı Mail Adresi Sonuç Ekran Ara Yüzü

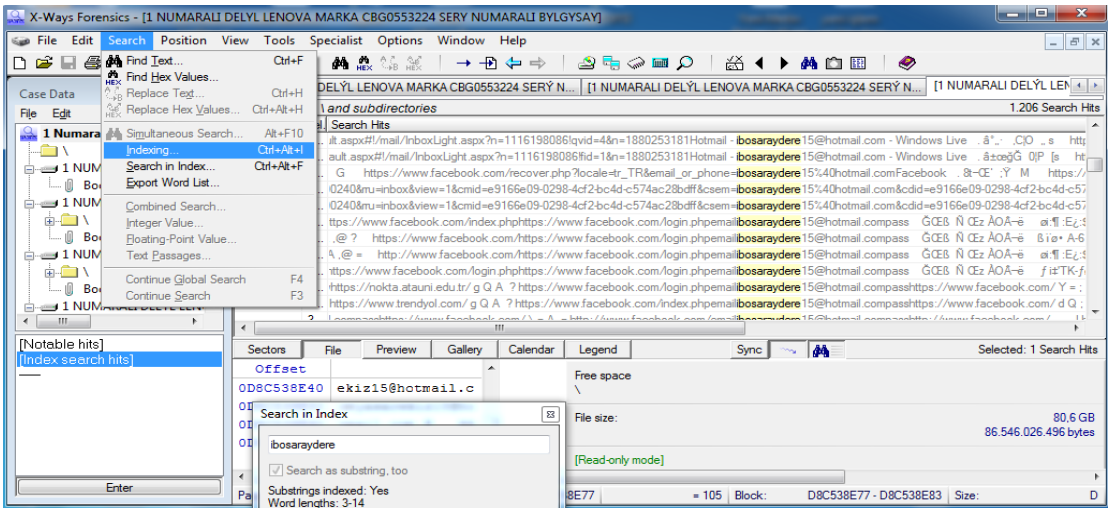
Xways Yazılımın Anahtar Kelime (Keywords) taraması yapılarak 212.252.84.159 Ip numarası taratılmış ve ip adresinin olduğu için 212.252.84.159 Ip adresinin bu bilgisayarda kullanıldığı tespit edilmiştir.Şekil 4.41'de X-Ways yazılımı ıp adresi sonuç ekran ara yüzü verilmiştir.



Şekil 4.41 X Ways Yazılımı IP Adresi Sonuç Ekran Ara Yüzü

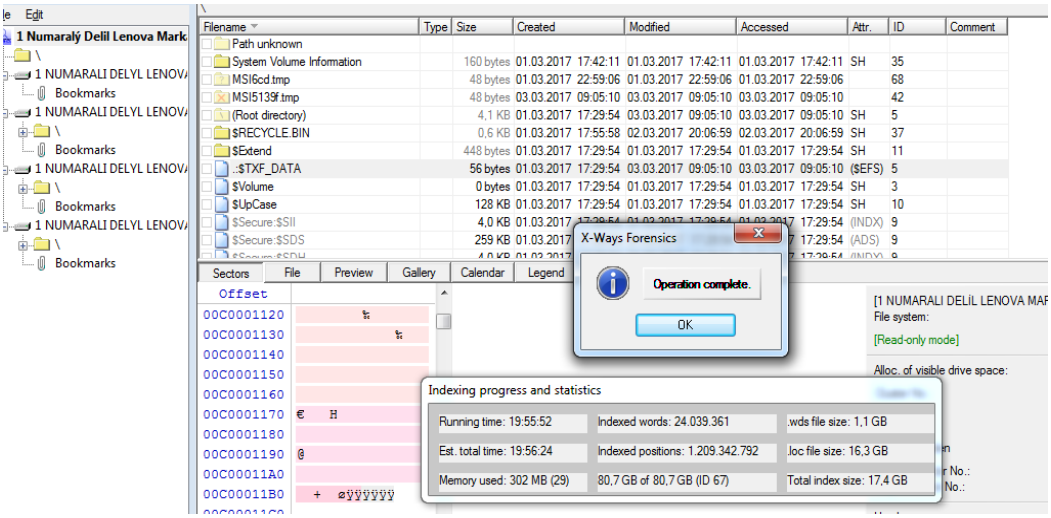
X Ways yazılımın indekleme işlemi ile de aratılma yapılmaktadır. İndeksleme işleminin aşamaları aşağıda gösterilmiştir.

X Ways yazılımın Arama (Search) kısmına tıkladıktan sonra alt bölmesinde bulunan İndeksleme (İndexing) kısmına tıklanarak indeksleme işlemine başlanır. Şekil 4.42'de X ways yazılımı indeksleme ekran görüntüsü verilmiştir.



Şekil 4.42 X Ways Yazılımı İndeksleme Ekran Görüntüsü

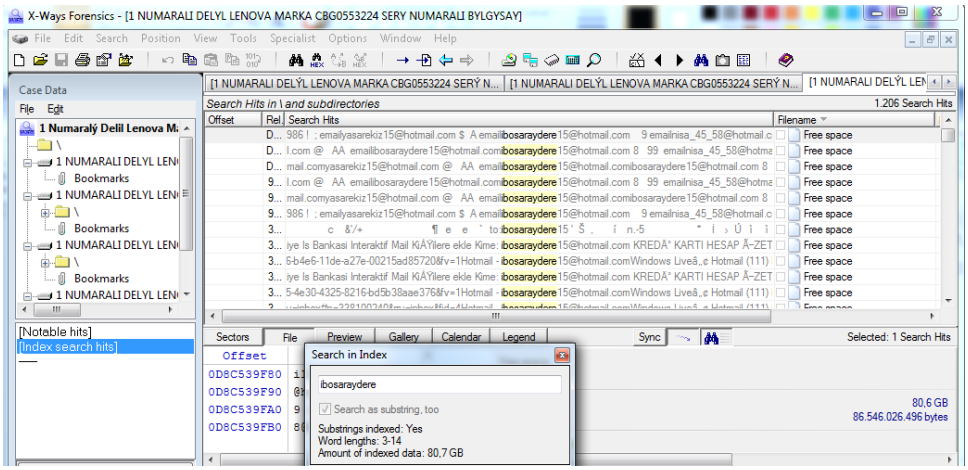
İndeksleme işlemi bittikten sonra çıkan sonuç aşağıya çıkartılmıştır. İndeksleme işlemi 29.56.24 saatte bittiği aşağıdaki çıkan raporda gösterilmiştir. Şekil 4.43'de X Ways yazılımı indeksleme bitiş ekran ara yüzü verilmiştir.



Şekil 4.43 X Ways Yazılımı İndeklesleme Bitiş Ekran Ara Yüzü

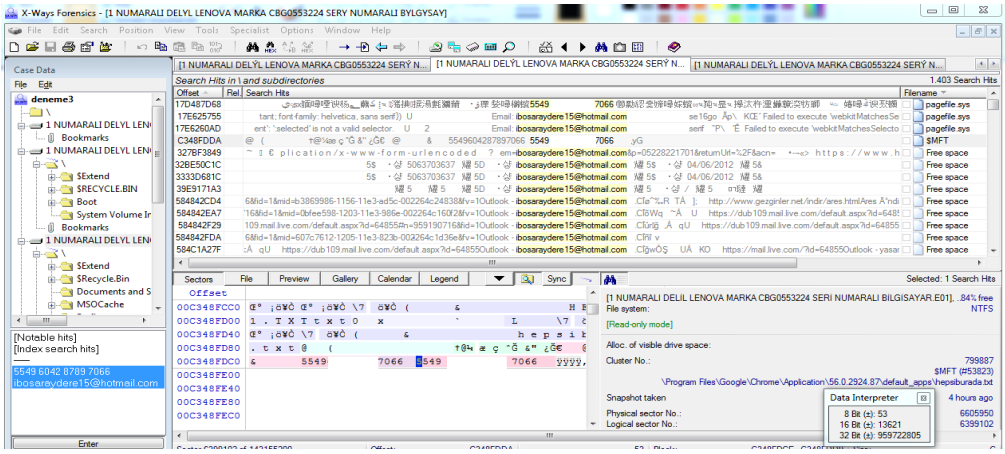
İndekleme işlemi bittikten sonra açılan İndekslerde Arama (Search in Index) kısmına aratmak istenilen kelimeleri yazarak hızlı bir şekilde aratmak istenilen kelimelere ulaşılır.

X-Ways Yazılımın İndekslerde Arama (Search in Index) kısmına ibosaraydere15@hotmail.com isimli msn adresini yazılır ve çıkan sonuç aşağıda gösterilmiştir. Şekil 4.44'de X Ways yazılımı indeksleme mail adresi Arama Sonuç Ekranı verilmiştir.



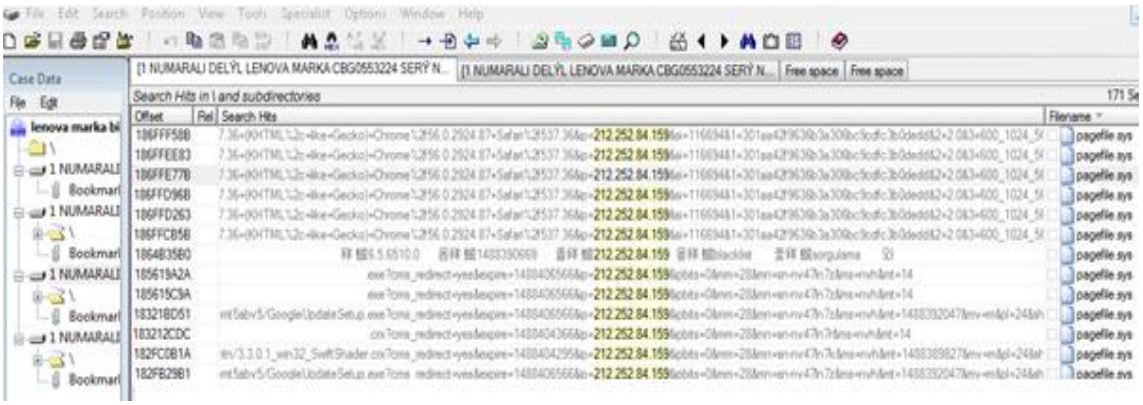
Şekil 4.44 X Ways Yazılımı İndeksleme Mail Adresi Arama Sonuç Ekranı

Xways Yazılımın İndeklerde Arama (Search in Index) kısmına 5549 **** **** 7066 kart numarası yazılarak çıkan sonuç aşağıda gösterilmiştir. Şekil X Ways yazılımı indeksleme kredi kartı numarası arama sonuç ekranı verilmiştir.



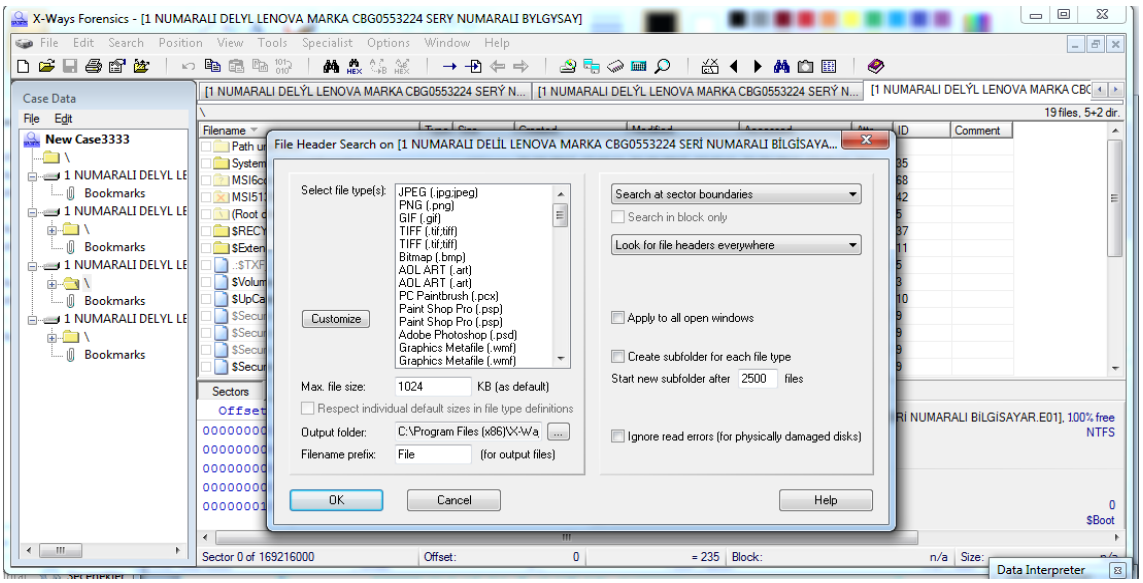
Şekil 4.45 X Ways Yazılımı İndeksleme Kredi Kartı Numarası Arama Sonuç Ekranı

Xways Yazılımın İndekslerde Arama (Search in Index) kısmına 212.252.84.159 Ip adresinin yazılarak çıkan sonuç aşağıda gösterilmiştir. Şekil 4.46'da X Ways yazılımı indeksleme IP numarası arama sonuç ekranı verilmiştir.

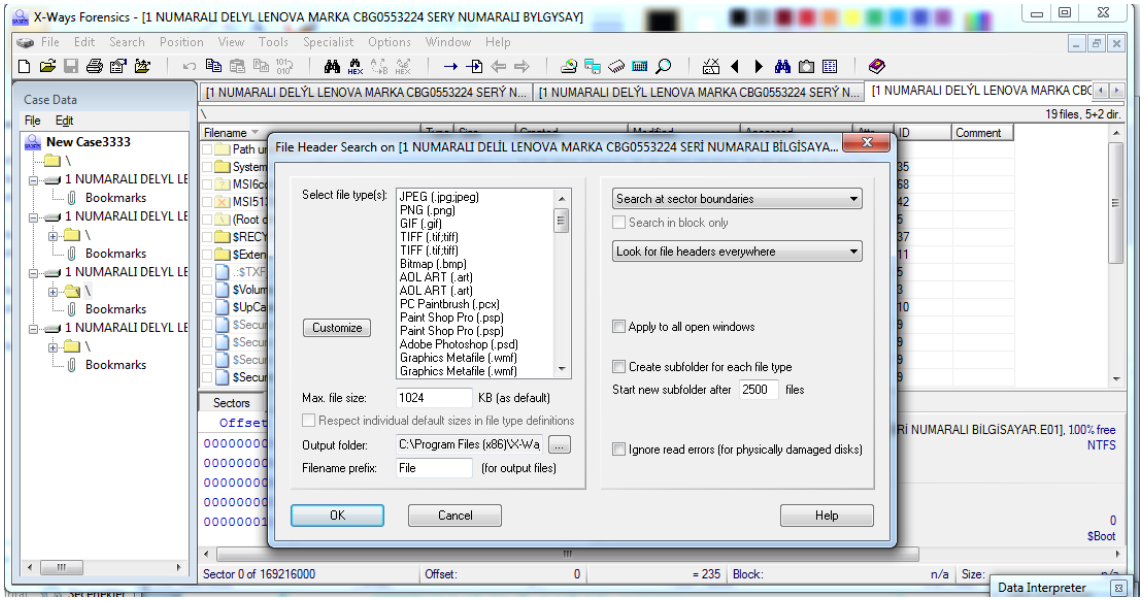


Şekil 4.46 X Ways Yazılımı İndeksleme Ip Numarası Arama Sonuç Ekranı

X Ways yazılımında silinmiş belgeleri Araçlar (Tools) kısmında bulunan Disk Araçları (Disk Tools) sekmesi altında bulunan Türe Göre Dosya Kurtarma (File Recovery By Type) sekmesi tıklanır ve kurtarmak istenilen uzantılar seçilir ve Tamam (Ok) sekmesine tıklanarak kurtarma işlemine başlanılır. Şekil 4.47'de X Ways yazılımı silinmiş belgeleri geri getirme ara yüzü ve Şekil 4.48'de X Ways yazılımı silinmiş belgeleri geri getirme dosya uzantısı seçme ekranı verilmiştir.

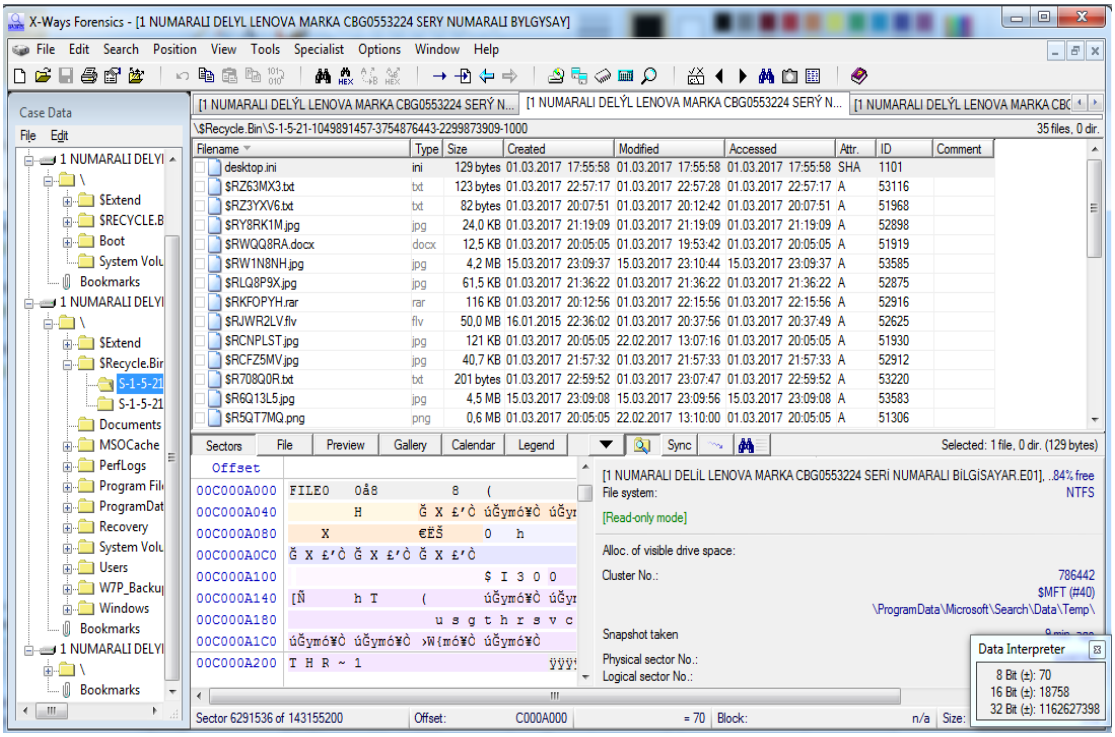


Şekil 4.47 X Ways Yazılımı Silinmiş Belgeleri Geri Getirme Ara Yüzü



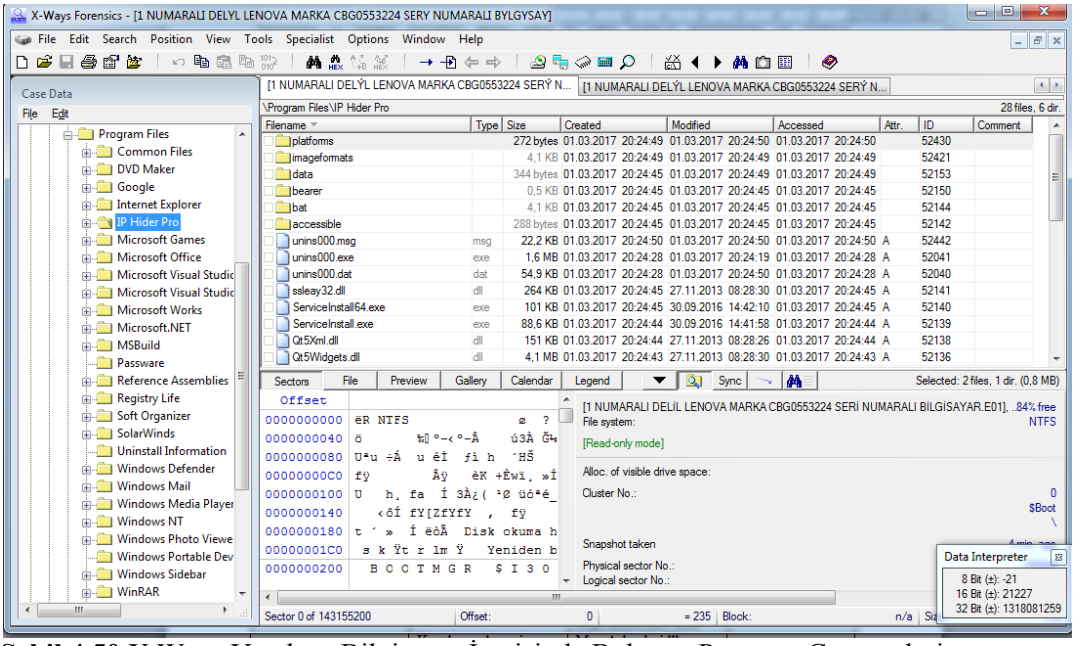
Şekil 4.48 X Ways yazılımı silinmiş belgeleri geri getirme dosya uzantısı seçme ekranı

Silinmiş belgeler taratıldıktan sonra çıkan sonuç ekranında $R4VCUAW.jpeg uzantılı dosyanın kredi kartı resmi olduğu dosya açılınca anlaşılmıştır. Şekil 4.49'da X Ways yazılımı silinmiş belgeler görüntü ekranı verilmiştir.



Şekil 4.49 X Ways yazılımı silinmiş belgeler görüntü ekranı

X WAYS Yazılımdan programlar içerisinde İP gizleme ve değiştirme programı (Ip Hider Pro) ve İnternet geçmişini silmek için kullanılan (Registry Life) programına rastlanılmış ve aşağıda gösterilmiştir. Şekil 4.50'de X Ways yazılımı bilgisayar içerisinde bulunan program görüntüleri ekranı verilmiştir.



Şekil 4.50 X Ways Yazılımı Bilgisayar İçerisinde Bulunan Program Görüntüleri

Çizelge 4.2'de 3 adet adli inceleme yazılımı ile imajı alınan hard disk incelenmiş ve inceleme sonucunda elde edilen bulgular kısaca tartışılmıştır. Encase yazılımının indeksleme yapmadığı 3 adet kelimeyi 120 dakikada bulduğu, kredi kartı bulucu sekmesinden ise kredi kartı numarasını 24 saatte bulduğu ve silinmiş belgelerde arama işlemini 25 saat gibi bir sürede tamamladığı görülmüştür.

Autopsy yazılımı ise indeksleme işlemi yaptığı bu indeksleme işlemini 35 saatte tamamladığı 3 adet kelimeyi, kredi kartı numaralarını, silinmiş belgeleri indeksleme işlemi yaptıktan sonra 1 dakika gibi bir sürede bulduğu görülmüştür.

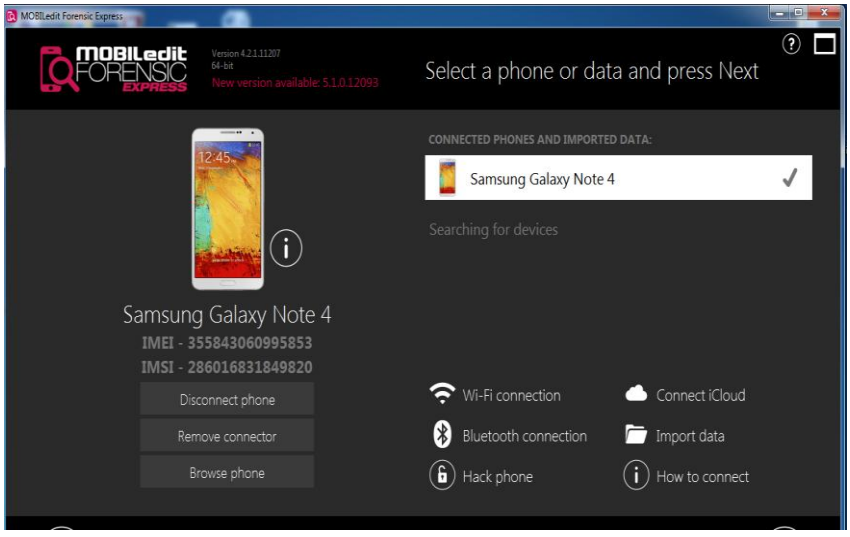
X-Ways yazılımının ise indeksleme işlemini 34 saatte tamamladığı 3 adet kelimeyi ve kredi kartı numaralarını indeksleme yolu ile 1 dakikada 3 adet kelimeyi ve kredi kartı numaralarını ise fiziksel olarak 150 dakikada ulaştığı, silinmiş bilgilere ise 26 saatte bulduğu görülmüştür.

Çizelge 4.2 İnceleme yazılımları performans karşılaştırmaları

İmaj Alma Yazılımı	İndeksleme Yapıp Yapmadığı	İndeksleme Zamanı	3 Adet Kelime Arama Zamanı	Kredi Kart Arama Zamanı	Silinmiş Belgelerde Arama Zamanı
Encase	Yapmıyor		120 Dakika	24 Saat	25 Saat
Autopsy	Yapıyor	35 Saat	Endeksleme ile 1 Dakika	Endeksleme ile 1 Dakika	Endeksleme ile 1 Dakika
X Ways	Yapıyor	34 Saat	150 Dakika veya Endeksleme ile 1 Dakika	İndeksleme ile 1 Dakika	26 Saat

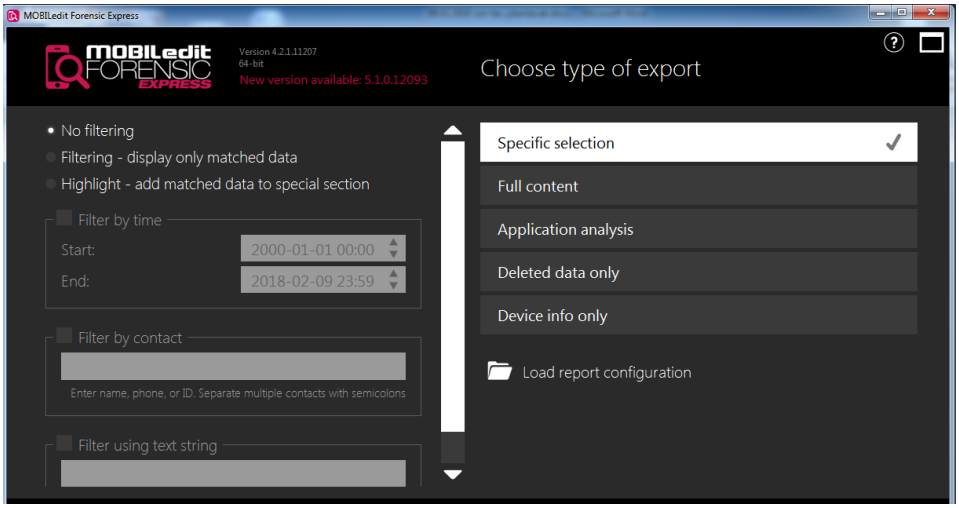
4.4 Mobil Cihazlarda İmaj Alma ve İnceleme

Suç unsura ikametten ele geçirilen Samsung Marka telefon Mobil Edit programı vasıtasıyla imaj alınmış ve incelenmiştir.Telefon Ultra Kit USB kablo vasıtasıyla bilgisayara bağlanır. Sonra program telefonu tanıyınca imaj alma ve inceleme işlemine geçilir. Mobil Edit Programı imaj alma işlemini 15 dakika silinmiş verileri 175 dakikada kurtarmıştır. Silinmiş verileri de programda bilgisayara tanımladığımız alana çıkartır ve oradan silinmiş verilere ulaşabiliriz. Mobil Edit programı başlatılır. İlk gelen ekranda telefon bilgileri IMEI ve IMSI numaraları ve telefonun modeli bulunur. Mobil Edit ilk ara yüz ekran görüntüsü Şekil 4.51'de gösterilmiştir.



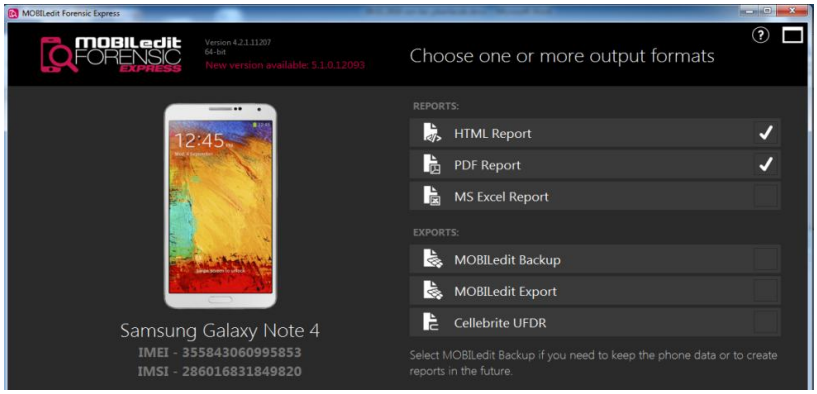
Şekil 4.51 Mobil Edit ilk ekran ara yüzü

İlk ekran geçildikten sonra Mobil Edit imaj alma ve silinmiş bilgileri kurtarma ekranı gelir. Bu ekran ara yüzünde bulunan Özel İçerik (Specific Selection) telefon içerisinde belirli tarihlerde arama yapma kısmı, Tam İçerik (Full Content) tam içerik yani telefon imaj alma kısmı, Uygulama Analizi (Application Analysis) kısmı ise telefon içerisinde yüklü bulunan uygulamaları analiz yapmak için kullanılır. Yalnızca Silinen Veriler (Deleted Data Only) kısmı telefon içerisinde silinmiş bilgi ve belgeleri kurtarmak için kulanılır.Yalnızca Cihaz Bilgileri (Device İnfo Only) kısmı ise telefonun bilgileri çıkarmak için kullanılan bölümdür.Mobil Edit menü bölümü şekil 4.52'de gösterilmiştir.



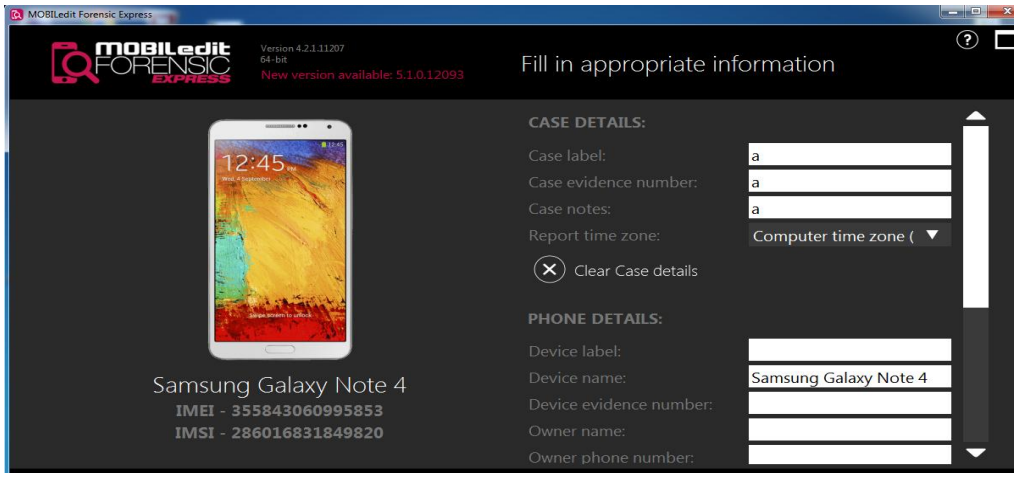
Şekil 4.52 Mobil Edit ilk Menüler ara yüzü

Mobil Edit programının 3. Ara yüzünde programın ne şekilde rapor vereceği şekil 4.53'de gösterilmiştir.



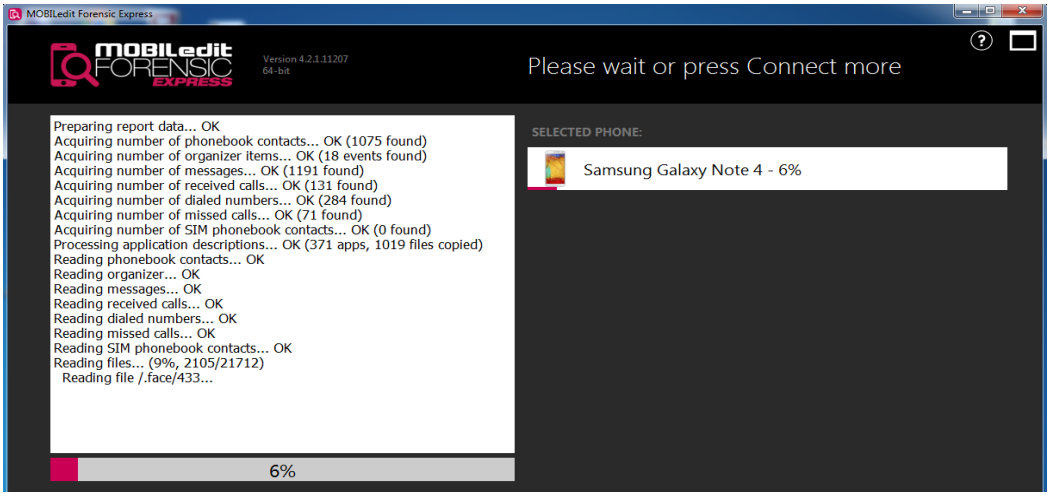
Şekil 4.53 Mobil Edit rapor ekranı

Mobil Edit programının 4. Ara yüzünde incelenen telefonun bilgileri kısmı yer almaktadır. Bu kısımda olay ile ilgili bilgiler Olay Etiketi (Case Label), Olay Kanıt Numarası (Case Evidence Number), Olay Notları (Case Notes) ve telefon bilgileri kısmında ise Cihaz Etiketi (Device Label), Cihaz Adı (Device Name), Cihaz Olay Numarası (Device Evidence Number), Cihaz Sahibi (Owner Name), Cihaz Sahibi Numarası (Owner Phone Number) kısımları yer almaktadır.Bu boşluklar doldurulduktan sonra inceleme işlemine geçilmektedir. Boşluk doldurma ekran görüntüsü şekil 4.54'de verilmiştir.



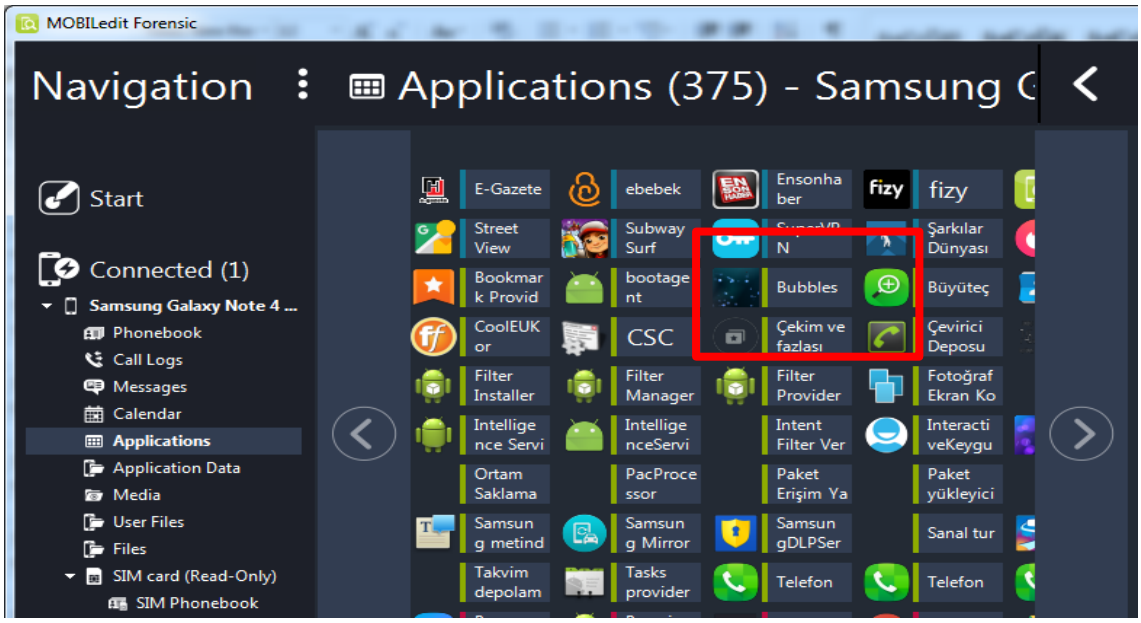
Şekil 4.54 Mobil Edit Boşluk Doldurma Ekranı

Boşluklar doldurulduktan sonra ileri sekmesine tıklanarak telefon inceleme ve imaj alma işlemine geçilmektedir. İmaj alma ekran ara yüzü şekil 4.55'de verilmiştir.



Şekil 4.55 Mobil Edit İmaj Alma ve İnceleme Ekranı

Mobil Edit programı Uygulamalar (Applications) kısmında cep telefonuna yükleniş olan Super Vpn Best Free Proxy pragramı ve Clean My Android programı şekil 4.56'de verilmiştir.



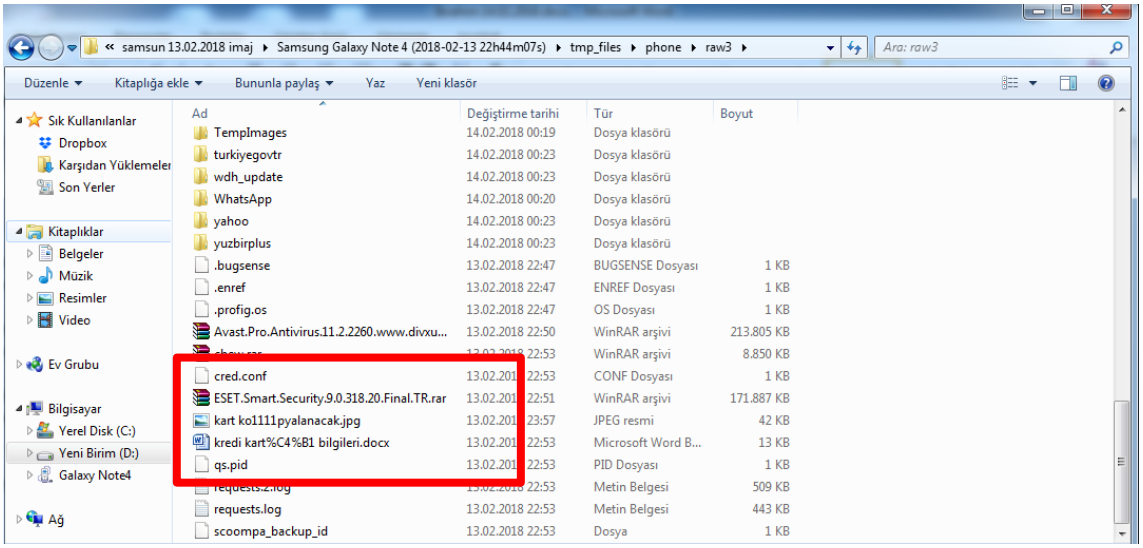
Şekil 4.56 Mobil Edit Uygulamalar Ekranı

Mobil Edit yazılımı cep telefonun imajını 15 dakikada silinmiş belgeleri ise 175 dakikada kurtarmıştır.Çizelge 4.3'de süreler verilmiştir.

Çizelge 4.3 Mobil edit kurtarma süreleri

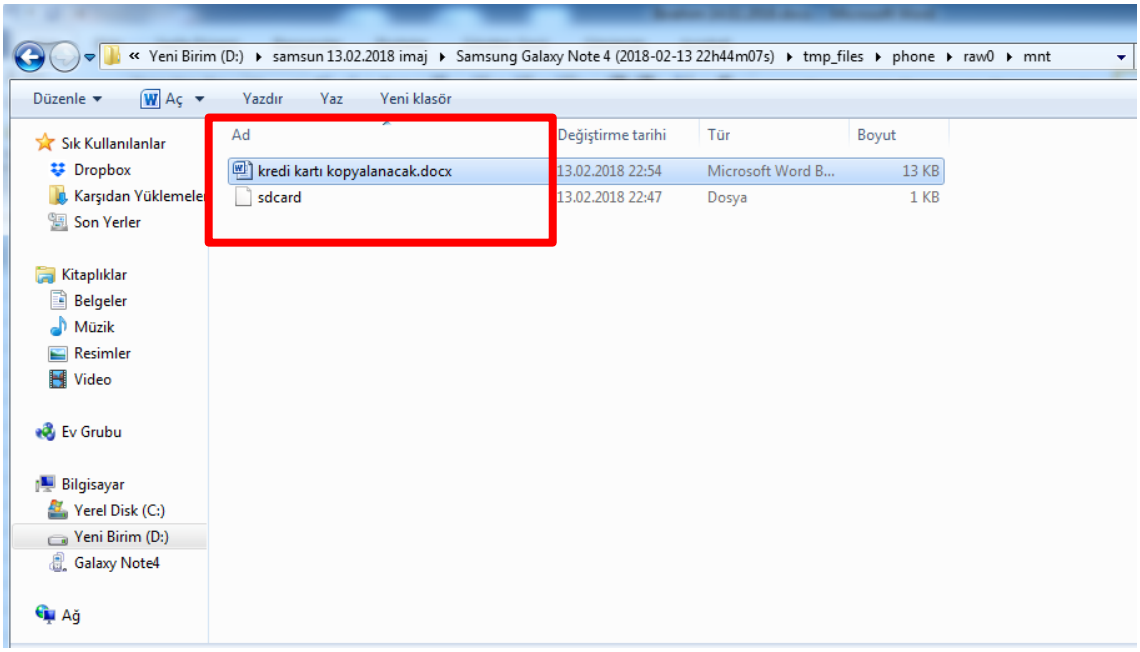
İmaj Alma Yazılımı	İmaj Alma Süresi	Silinmiş Bilgeler Kurtarma Süresi
Mobil Edit	15 Dakika	175 Dakika

Cep telefonuna mevcut yüklü olan belgeleri Mobil Edit programına tanımlamış olduğumuz yere gidip oradan çıkartabiliriz. Cep telefonunda mevcut yüklü olan belgeler Bilgisayarım, Samsung Galaxy Note 4 (2018-02-13 22h44m07s), tmp_files, phone. raw3, ekranında bulabiliriz. Cep telefonuna yüklü mevcut belgeler ekran görüntüsü Şekil 4.57'de verilmiştir.



Şekil 4.57 Mobil Edit Mevcut Belgeler Ekranı

Cep telefonunda silinmiş olan belgeleri Mobil Edit programına tanımlamış olduğumuz yere gidip oradan çıkartabiliriz. Cep telefonunda silinmiş belgeler Bilgisayarım, Samsung Galaxy Note 4 (2018-02-13 22h44m07s), tmp_files, phone. raw0, mnt ekranında bulabiliriz. Cep telefonuna silinmiş belgeler ekran görüntüsü Şekil 4.56'de verilmiştir.



Şekil 4.58 Mobil Edit Silinmiş Belgeler Ekranı

5. TARTIŞMA ve SONUÇ

Adli bilişim tekniklerinin Ceza Kanunundaki tüm suç tiplerinde, mağdur ve şüphelisi bulunan tüm suçlarda, hukuk davalarında, kolluk kuvvetlerinin yürütmüş olduğu tüm soruşturmalarda soruşturmanın seyrini değiştirebilecek bilgilere ulaşılabilmesini sağlamaktadır. Örneğin bir cinayet suçunda şüphelinin veya maktulün dijital delillerinde yapılacak incelemede katilin yakalanılabilmesi veya suç ile ilgili olabilecek kişilerin tespit edilebilmesi sağlanmış olacaktır. Bu sebepten dolayı adli bilişim tekniklerinin kullanılmasının ne kadar önemli olduğu kolluk kuvvetleri tarafında bilinmesinde fayda vardır.

Adli Bilişim incelemeleri son zamanlarda popüler hale gelen bir inceleme alanı olmakla birlikte artık bu alanda üniversitelerde bölümler açılmaktadır. Dijital delilin somut olmaması inandırıcılığı ve güvenirliği açısından tereddütler oluşturmaktadır. Bu tereddütlerin ortadan kaldırılması ve suç işleyenlerin gerekli cezaları alması, adli makamlara bu adli bilişim sonrası düzenlenen raporların ayrıntılı ve anlaşılabilir bir şekilde izah edilmesi gerekmektedir.

İnceleme işlemleri sırasında kullanılan yazılımlar uluslararası adli bilişim standardına uygun bir şekilde yürütülmeli, incelemeyi yapan personel bu alanda uzman olmalı, kendisini bu alanda yenilikçi olmaya gayret göstermeli çünkü teknoloji sürekli geliştiği için yeni suç türleri ortaya çıktığından personelin bu değişime ayak uydurması gerekmektedir.

Adli bilişim incelemelerinin önemli ve ilk kısmını oluşturan imaj alma işleminin düzgün bir şekilde yapılması ve bu imaj alma işlemini tutanağa bağlanmasıdır. İmaj alma işlemi olay yerinde yapılmalı eğer olay yerinde imaj alma işlemi yapılamıyorsa el koyma işlemi sonrası laboratuvar ortamında yapılması gerekmektedir. Dijital materyaller çabuk bozulabilir ve etkilenebilir yapıda olduğundan dolayı hızlı ve çok kısa bir süre içerisinde geri getirilemez şekilde silebilecek ve soruşturma kapsamında dijital delil elde etme imkânı ortadan kalkacaktır.

Çalışma kapsamında dijital materyallere ilk müdahalenin nasıl yapılması gerektiği, dijital delillere ilk müdahalenin önemi, bu aşamada yapılacak bir hatanın tüm soruşturma aşamasını etkileyebileceği, yapılan senaryo gereği tespit edilen bilgiler neticesince el konulan ve incelenen bilgisayar kullanıcısın suçu işlediği yönünde kesin delillere ulaşılmıştır. Analizde kullanılan adli bilişim inceleme yazılımları ve teknik detaylar kullanılmamış olsaydı şüphelinin sadece ip adresi ile cezalandırılması hukuk kuralları ile bağdaşmayacağı için suçu işleyen cezasız kalacak ve bu suçu işlemeye devam edebilecekti.

Senaryo kapsamında dijital materyal üzerinde 5 yazılım ve 1 cihaz ile imaj alma işlemi yapılmış bu program ve cihaz ile ilgili imaj alma özellikleri imaj alma zamanları ve imaj alma aşamaları ayrıntılı olarak anlatılmış en hızlı sonucu Td1 diye tabir edilen imaj alma cihazı sağlamıştır.

İnceleme aşamasında ise, her soruşturmada olduğu gibi hash değerleri dikkate alınarak inceleme yapan uzman personel dışında delilin inceleme işlemi hiçbir personel tarafından ulaşılmaması gerekmektedir. Çünkü şüphelinin dijital materyalinde suç ile alakası olmayan ve şüphelinin özel hayatına ilişkin bilgi ve belgeler kullanmakta oldukları dijital materyallerde depolanmaktadır. İncelemeyi yapan uzman personel öncellikle suç ile ilgili bilgilere ulaşmalıdır. Adli bilişim yazılımlarının geneli İngilizce dilinde yazıldığından dolayı inceleme esnasında yazım karakterlerinden kaynaklı bir sıkıntı ile karşılaşmamak için, adli bilişimin her aşamasında Türkçe karakter kullanmaktan kaçınılmalıdır. Bu çalışma esnasında kullanılan ekran çıktılarından ve log dosyalarından da anlaşılacağı üzere çeşitli sıkıntılar ortaya çıkmıştır.

Senaryo gereği alınan imaj üzerinde 3 adet dijital inceleme yazılımı ile inceleme yapılmış bu yazılımlar vasıtasıyla şüphelinin bilgisayarı içerisinde suç ile ilgili olabileceği değerlendirilen şüphelinin kullanmış olduğu IP adresi, müştekinin kullanmış olduğu mail adresi ve müştekiye ait olan kredi kartı bilgisinin bu 3 yazılımda tespit etmiştir. İmaj alma yazılımları dikkate alındığında Ftk programı 58.02 dakikada imaj almayı bitirmiş, Encase yazılımı 1 saat 13 dakikada imaj almayı bitirmiş, X-Ways yazılımı 1 saat 15 dakikada bitirmiş, Helix yazılımı saat 28 dakikada bitirmiş, Tablue

İmager yazılımı 50.25 dakikada imaj almayı bitirmiş, Td1 cihazı ise 44.41 dakikada imaj almayı bitirmiştir. Burada en hızlı sonuca Td1 cihazı ile varılmıştır.Td1 cihazı imaj alma yazılımları içerisinde en hızlı imaj alan donanım olmuştur. Sonra ise Tablue İmager programı en hızlı yazılım olmuş fakat kullanım açısından Tableu İmager yazılımı Ultrakit olmadığında imaj almadığından dolayı çok tercih edilmemektedir. Sonra hızlı imaj alan yazılım olan Ftk yazılımı ise sık ve basit kullanılan bir yazılım olduğundan dolayı daha çok tercih edilmektedir. Sonra ise Encase yazılımı en kısa sürede imaj almış fakat Encase daha çok adli incelemede kullanıldığı için imaj alma yazılımı diğer programlara göre yavaş imaj almaktadır. Sonra ise genelde bir inceleme yazılımı olan x-Ways İnceleme yazılımı imaj almayı bitirmiştir. Son olarak ise Helix imaj alma yazılımı imaj almayı bitirmiştir. Genel olarak bakıldığında Td1 donanımı en hızlı sürede imaj alan donanım olmuş inceleme yazılımı olan programlar biraz daha geç sürede imaj almayı bitirmişlerdir. Adli inceleme yazılımları karşılaştırıldığında Encase yazılımı 3 adet kelime aramasını 120 dakikada, kredi kartı numaralarını 24 saatte silinmiş belglerde aramayı ise 25 saatte bitirmiştir. Autopsy yazılımı indeksleme mantığı ile çalıştığından dolayı indekslemeyi 35 saatte birimiş ve aranan kelimeleri indeksleme bittikten sonra 1 dakika gibi bir sürede çıkartmaktadır. X-Ways yazılımı hem indeksleme mantığı hemde normal arama yapabilme özelliğinden dolayı 34 saatte indekslemeyi bitirmiş,3 adet kelimeyi 150 dakika da bulmuş, silinmiş belgeleri de 26 saatte ulaşmıştır. Burada en hızlı şekilde sonuca ulaşan ve en hızlı şekilde verileri inceleyen Encase yazılımı olmuş, sonra indeksleme mantığından X-Ways yazılımı sonra da Autopsy yazılımı istenilen belgelere en hızlı sonuca ulaşmıştır. Mobil cihazlarda incelemede ise kullanılan Mobil Edit programı imaj alma süresini 15 dakika silinmiş bilgilerde kurtarma süresi ise 175 dakika olduğu görülmüştür.

6. KAYNAKLAR

Ayers, D. (2009). A second generation computer forensic analysis system. *Digital Investigation,* **3** : 21-23.

Çakır, H. ve Sert, E. (2013). Bilişim Suçları ve Delillendirme Süreci. *Örgütlü Suçlar ve Yeni Tredler,* **1** : 145-147.

Çatalkaya, H., Karaman, M. ve Koca, E. (2015). Elektronik Kopyanın (adli imaj) Alınmasında Açık Kaynak Uygulamalarının Güvenirliği. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, **2** : 15-19.

Daniel, L. (2011). Digital Forensic. *The Subdisciplines. Digital Forensic for Legal Professions*, **1 :** 17-23

Demirkaya, V. (2009). Delil Güvenliği. Yüksek Lisans Tezi, Polis Akademisi Güvenlik Bilimleri Enstitüsü, Ankara.

Dülger, M.V. (2013). Bilişim Suçları ve İnternet İletişim Hukuku. Seçkin Yayıncılık, 3. Baskı, Ankara.

Ekim A. (2013). Mobil Cihazlarda Adli Bilişim ve Malware Analizi, *1st International Symposium on Digital Forensics and Security,* **1** : 20-21

Ersoy Y (1994) Genel hukuki koruma çerçevesinde bilişim suçları. *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi,* **3 :** 49-151.

Garfinkel, S.L. (2010). Digital forensics research: The next 10 years. *Digital Investigation,* **7** : 25-27.

Henkoğlu, B., Turan, Y. ve Kutar, E. (2011). Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi. Pusula Yayıncılık, Ankara.

Hosmer, C. (2002). Proving the Integrity of Digital Evidence with Time, *International Journal of Digital Evidence,* **1** : 8-9.

IACIS. (2004). International Association of Computer Investigative Specialists, "Guide for Forensic Examinations. Digital Forensic, USA 55-56

Karagülmez, A. (2011). Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri. Seçkin Yayıncılık, 3. Baskı, Ankara.

Kılıç M.S. (2013). Bilişim Suçlarına İlişkin Elektronik Delil Etme Yöntemlerine Genel Bakış, *Polis Bilimleri Dergisi*, **24** : 11-13

Kılıç, M.S. (2014). Elektronik Deliller ve Yapısal Özellikleri. Seçkin Yayıncılık, Ankara.

Özbek, M. (2013). Adli Bilişim Uygulamalarında Orijinal Delil Üzerindeki Hash Sorunları. *1st International Symposium on Digital Forensics and Security*, **2 :** 1-7.

Özen, M. (2015). Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134), *Ankara Barosu Dergisi*, S.74.

Shinder, D.L. (2002). Scene of Cybercrime – Computer Forensics Syngress Publishing, USA Handbook, *Syngress Publishing,* 22-24

Srinivasan, S. (2007). Security and Privacy vs. Computer Forensics. *Capabilities Information Systems Control Journal*,45-46

Şamlı, R., Türk ve Dünya Hukukunda Bilişim Suçları, Akademik Bilişim'10 - XII. Akademik Bilişim Konferansı Bildirileri, Muğla Üniversitesi, Muğla, 2010, 22-24

Şirikçi, A.S. ve Cantürk, N. (2012). Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının Önemi. *Bilişim Teknolojileri Dergisi*, **5**: 29-34.

İnternet Kaynakları

1-) http://www.dersimiz.com/terimler-sozlugu/Bilisim-Nedir-13806.html#.WINP1lWL TIU, 10.01.2017

2-) http://www.ekizer.net/adli-bilisim-computer-forensics, 09.02.2017

3-) http://www.ekizer.net/adli-bilisim-computer-forensics, 13.02.2017

4-) https://cyberchefweb.wordpress.com/2017/03/16/dosya-imzasi-nedir-ne-ise-yarar/, 15.06.2017

5-) http://whatis.techtarget.com/definition/slack-space-file-slack-space, 15.06.2017

6-) https://www.guidancesoftware.com/encase-forensic-imager, 18.07.2018

7-) http://accessdata.com/product-download/digital-forensics/ftk-imager-version-3.4.2, 25.07.2018

8-) https://www.x-ways.net/replica.html, 11.11.2017

9-) https://www.guidancesoftware.com/tableau/download-center#tim, 10.12.2017

10-) http://www.e-fense.com/h3-enterprise.php, 10.12.2017

11-) https://www.logicube.com/shop/falcon/?v=ebe021079e5a, 10.12.2017

12-) https://tr.wikipedia.org/index.php?q=aHR0cHM6Ly90ci53aWtpcGVkaWEub3JnL3 dpa2kvU0hB LTE, 15.11.2016

13-) https://www.computerhope.com/jargon/s/slack-space.htm, 15.01.2018

ÖZGEÇMİŞ

Adı Soyadı : İbrahim SARAYDERE

Doğum Yeri ve Tarihi : Burdur 01.05.1988

Yabancı Dili : İngilizce

İletişim (Telefon/e-posta) : 0 506 370 36 37 ibrahimsaraydere@hotmail.com

Eğitim Durumu (Kurum ve Yıl)

Lise : Antalya Lisesi, (2002-2005)

Lisans : Aksaray Polis Meslek Yüksek Okulu (2007-2009), Anadolu Üniversitesi İşletme Fakültesi (2009-2012)

Çalıştığı Kurum/Kurumlar ve Yıl : Antalya İl Emniyet Müdürlüğü Kom Şube Müdürlüğü (2009-2012)

Sivas İl Emniyet Müdürlüğü Siber Suçlarla Mücadele Şube Müdürlüğü(2012-2015)

Antalya İl Emniyet Müdürlüğü Konyaaltı İlçe Emniyet Müdürlüğü (2015-Devam Ediyor)