SİBER SUÇ SORUŞTURMALARINDA

ADLİ BİLİŞİM İNCELEMELERİ

YÜKSEK LİSANS TEZİ

Yasin BAŞAR

DANIŞMAN
Doç. Dr. Fehmi AKIN

İNTERNET VE BİLİŞİM TEKNOLOJİLERİ YÖNETİMİ

Eylül, 2015

AFYON KOCATEPE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

SİBER SUÇ SORUŞTURMALARINDA ADLİ BİLİŞİM İNCELEMELERİ

Yasin BAŞAR

DANIŞMAN

Doç. Dr. Fehmi AKIN

İNTERNET VE BİLİŞİM TEKNOLOJİLERİ YÖNETİMİ

Eylül, 2015

TEZ ONAY SAYFASI

Yasin BAŞAR tarafından hazırlanan "**Siber Suç Soruşturmalarında Adli Bilişim İncelemeleri**" adlı tez çalışması lisansüstü eğitim ve öğretim yönetmeliğinin ilgili maddeleri uyarınca 04/09/2015 tarihinde aşağıdaki jüri tarafından oy birliği ile Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü İnternet ve Bilişim Teknolojileri Yönetimi **Anabilim Dalı'nda YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman : Doç. Dr. Fehmi AKIN

Başkan	: Doç. Dr. Veysel AĞCA AKÜ İktisadi ve İdari Bilimler Fakültesi	İmza
Üye	: Doç. Dr. Fehmi AKIN AKÜ İktisadi ve İdari Bilimler Fakültesi	İmza
Üye	: Yrd. Doç. Dr. Ramazan ARSLAN Uşak Üniversitesi İktisadi ve İdari Bilimler Fakültesi	İmza

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

.....
Prof. Dr. Hüseyin ENGİNAR
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.

03/09/2015

Yasin BAŞAR

ÖZET
Yüksek Lisans Tezi

SİBER SUÇ SORUŞTURMALARINDA ADLİ BİLİŞİM İNCELEMELERİ

Yasin BAŞAR
Afyon Kocatepe Üniversitesi
Fen Bilimleri Enstitüsü
İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı
Danışman: Doç. Dr. Fehmi AKIN

Bu araştırmada, siber suç soruşturmaları başta olmak üzere adli makamlarca yürütülmekte olan neredeyse tüm soruşturmalarda, adli bilişim incelemelerinin kullanılmasının soruşturmanın akıbeti açısından gerekliliği incelenmiştir. Çalışmada siber suç soruşturmalarında delil elde etme yöntemlerinde kullanılan adli bilişim teknolojisi ve incelemelerde kullanılan donanım ve yazılımlardan bahsettikten sonra, çalışma kapsamında bir senaryo oluşturulmuştur. Oluşturulan senaryo çerçevesinde Banka ve/veya Kredi Kartlarının Kötüye Kullanılması suçu soruşturması gerçekleştirildiği varsayılarak, soruşturma sonucunda tespit edilen şüphelinin adresinde arama ve el koyma işlemi gerçekleştirilmiş ve işlem neticesinde üç adet dijital materyal elde edilmiştir.

Dijital materyallerin asılları üzerinde inceleme işleminin yapılması delil bütünlüğünü bozacağından, elde edilen üç adet dijital materyalin adli kopyaları alınarak delil bütünlüğünün korunduğunu gösterir “hash değerleri” tespit edilmiş ve adli kopyalar üzerinde inceleme işlemi gerçekleştirilmiştir.

İnceleme işlemi neticesinde, senaryo kapsamında elde edilen ve üzerinde inceleme işlemi gerçekleştirilen dijital materyaller içerisinde Banka ve/veya Kredi Kartlarının Kötüye Kullanılması suçuna konu olan bilgi ve belgeler tespit edilmiştir. Tespit edilen bilgi ve belgelerin ayrıntılı bir şekilde belirtildiği inceleme raporu, anlaşılır bir dil

kullanılarak tanzim edilmiş ve adli makamlara teslim edilmeye hazır hale getirilerek çalışmaya son verilmiştir.

2015, xiv + 129 sayfa

Anahtar Kelimeler: Siber Suçlar, Adli Bilişim, Adli Kopya, Dijital Delil, Hash Algoritması,

ABSTRACT

M.Sc. Thesis

FORENSIC EXAMİNATİONS IN CYBER CRIME İNVESTİGATİONS

Yasin BAŞAR

Afyon Kocatepe University

Graduate School of Natural and Applied Sciences

Department of Internet and Information Technology Management

Supervisor: Assoc. Prof. Fehmi AKIN

In this study, nearly all the investigations being conducted by the judicial authorities, especially cyber crime investigation, forensics requirements in terms of the outcome of the investigation of the use of investigation have been examined. After working in talking about the technology used in computer forensics and analysis hardware and software used in the methods of obtaining evidence in cybercrime investigation, it has created a scenario under study. In the framework of scenario the bank and / or credit cards, assuming Abuse criminal investigation is carried out, the investigation resulted in the suspect's address detected was carried out search and seizure operations and in the process result obtained three pieces of digital material.

Would compromise the integrity of evidence made the review process on the originals of digital materials indicates that preserve the integrity of evidence on three digital material legal copy obtained "hash values" have been identified and the review process on forensic copies were carried out.

In the review process as a result, obtained under scenario and in the review process carried out by the Bank of digital materials and / or information and documents that are subject to the Credit Card Abuse of crime have been identified. A thorough examination of the detected information and documents that report stated, was

drawn up using a simple language and is no longer allowed to work by making ready to be delivered to judicial authorities.

2015, xiv + 129 pages

Key Words: Cybercrime, Forensics, Forensic İmage, Digital Evidence, Hash Algorithm,

TEŞEKKÜR

Bu araştırmanın konusu, deneysel çalışmaların yönlendirilmesi, sonuçların değerlendirilmesi ve yazımı aşamasında yapmış olduğu büyük katkılarından dolayı tez danışmanım Sayın Doç. Dr. Fehmi AKIN, araştırma ve yazım süresince yardımlarını esirgemeyen Emin GÜRSOY ve Ali BÜYÜKGÜLEN'e, her konuda öneri ve eleştirileriyle yardımlarını gördüğüm hocalarıma ve araştırma boyunca manevi desteklerini esirgemeyen eşim Semra BAŞAR'a teşekkür ederim.

Yasin BAŞAR

AFYONKARAHİSAR, 2015

İÇİNDEKİLER DİZİNİ

Sayfa

KISALTMALAR DİZİNİ

Kısaltmalar	
BKK	Banka Kartları ve Kredi Kartları Kanunu
BTK	Bilgi Teknolojileri Kurumu
CMK	Ceza Muhakemeleri Kanunu
EİK	Elektronik İmza Kanunu
FSEK	Fikir ve Sanat Eserleri Kanunu
FTK	Forensic Toolkit (Adli Bilişim Yazılımı)
IP	İnternet Protocol (İnternet Protokol)
ISS	İnternet Servis Sağlayıcı
LAN	Local Area Network (Yerel Alan Ağı)
RAM	Random Access Memory (Rastgele Erişimli Hafıza)
SLD	Second Level Domain (İkinci Derece Alan Adı)
TCK	Türk Ceza Kanunu
TDK	Türk Dil Kurumu
TLD	Top Level Domain (Birinci Derece Alan Adı)
TRABİS	.tr Ağ Bilgi Sistemi
USB	Universal Serial Bus (Evrensel Seri Yolu)
WAN	Wide Area Network (Geniş Alan Ağı)

ŞEKİLLER DİZİNİ

Sayfa

ÇİZELGELER DİZİNİ

Sayfa

RESİMLER DİZİNİ

Sayfa

1. GİRİŞ

Günümüzde bilişim ve teknoloji sistemlerinin hızla büyümesi, sürekli gelişmesi, toplum yaşamında giderek daha fazla yer alması ve kullanım alanının günden güne genişlemesi, doğal olarak bazı hukuki sorunları da beraberinde getirmiştir. Bu gelişme, bir yandan insan hayatını kolaylaştırmaya devam ederken, bir yandan da çözülmesi gereken birtakım problemlere yol açmaktadır. İnsanlık tarihi kadar eski bir kavram olan suçun önlenebilmesi için, toplum tarafından sürekli çözüm yolları aranmıştır. İnsanoğlunun var olduğu her dönemde, şartlara göre şekil alan suç ve suçlu kavramları günümüzdeki bilişim ve teknoloji sistemlerinin gelişime paralel olarak farklılık göstermektedir. Bilişim ve teknolojinin gelişmesi ve bilginin eskiye göre daha hızla yayılması, önem kazanması, bilginin ekonomik, sosyal, siyasal değerinin artması, bu değerler üzerinde kolay yoldan hak sahibi olmak isteyen kişileri, bilişim teknolojisi marifetiyle suç işler hale getirmiştir.

İnsanlar her gün yüzlerce internet sitesini ziyaret ediyor, onlarca elektronik posta okuyorlar. Kredi kartı ile internet üzerinde alışveriş yapıyor, internet bankacılığını kullanarak havale ve EFT işlemleri gerçekleştiriyorlar. Hastaneye gitmeden muayene sırası alıyor, ödeme günü gelen faturaları bankaya gitmeye gerek olmadan yatırıyorlar. Sosyal paylaşım sitelerini yoğun bir şekilde kullanarak gerek arkadaşlarıyla sohbet ediyor, gerekse kendileri ile ilgili resim ve video paylaşımlarında bulunuyorlar. Kişisel bilgilerinin yanı sıra kurumsal bilgilerini de internet ortamında aktif olarak kullanıyor ve ticari yazışmaların çoğunu yine internet üzerinden gerçekleştiriyorlar.

İnternetin sağladığı bütün bu faydalı işlemler ve teknoloji dünyasındaki hızlı gelişmeler hayatı her geçen gün biraz daha kolaylaştırmakta, ekonomik ve sosyal hayatta önemli değişikliklere neden olmaktadır. Bununla birlikte, insan ilişkileri de teknolojik ortamlara taşınmakta, suç işleme şekilleri de teknolojiye paralel olarak gelişmekte ve bilişim alanında yeni suç tipleri ve suç fail profilleri ortaya çıkmaktadır.

Ortaya çıkan bu yeni suç tipleri, ilk başlarda klasik suç olarak adlandırılan sahtecilik,

hırsızlık, dolandırıcılık vb. suçlar gibi değerlendirilirken, çok geçmeden bu suç tiplerinin klasik suçlardan işleniş şekilleri, suçun yeri ve zamanı, suçun şüphelisi ve mağduru gibi etkenlerde farklılık gösterdiği anlaşılmıştır. Sonrasında ise, bu suç tiplerine genel olarak bilişim suçları tanımlaması yapılarak klasik suçlardan ayrılmıştır.

Bilişim suçları soruşturması, bilişim sektöründe yaşanan gelişmeler sonucunda sürekli olarak çeşitlilik göstermekte ve işlenen suçlar günden güne artmaktadır. Bilişim ve teknoloji sınırları olmayan bir dünya olduğundan, bu dünyada suç işleyen suçluların tespit edilmesi, takip edilmesi, yakalanması ve yargılamanın yapılabilmesi için gerek araç ve gereç, gerekse personel eğitimi konusunda gelişmeye sürekli olarak açık olunması gerekmektedir.

Suçluların takibinin kolayca yapıldığı ve yakalanarak cezalandırıldığı bir toplumda insanlar daha huzurlu bir ortamda yaşayacak ve devletin otoritesine duyduğu saygınlığı artacaktır. Bu sebeple, bilişim suçlarıyla etkin olarak mücadele edilebilmesi ve bu suçların aydınlatılabilmesi için, suçluların kullandıkları yöntemler ile bu tür suçlarla mücadele yöntemlerinin bilinmesi, teknolojik gelişmelerden haberdar olunması, kolluk kuvvetlerinin bilişim suçları birimlerinde çalışan personel sayısının artırılması ve personelin bu yönde eğitilmesi gerekmektedir.

Bilişim suçları ve bilişim yoluyla işlenen suçlar ile daha etkin bir şekilde mücadele edilebilmesi için, suçların aydınlatılması ve suçluların adli makamlara teslim edilmesi sürecinde fiziksel delillerden çok, elektronik veya manyetik bir ortam üzerinden iletilen veya bu ortamlara kaydedilen delil niteliği taşıyan veri ve bilgiler olarak tanımlanan dijital delillere ihtiyaç duyulmaktadır.

Bu çalışmada, öncelikli olarak bilişim suçları, işleniş yöntemleri, hukukumuzdaki yeri ve bilişim suçları soruşturmasında olmazsa olmaz olarak kullanılan delil elde etme yöntemi olan adli bilişim teknolojisi araştırılmış ve banka ve/veya kredi kartlarının kötüye kullanılması suçu ile ilgili hazırlanan senaryo kapsamında adli bilişim aşamaları

uygulamalı olarak gösterilmiştir.

1.1 Araştırmanın Önemi

Bilişim suçları zaman, mekan ve mesafe kavramlarının anlamını yitirdiği suçlar olduğundan dolayı, klasik suçlara göre delil elde etme imkanı çok zor olan suçlardır. Adli bilişim ise, bilişim suçlarının soruşturulmasında kullanılan olmazsa olmaz denilebilecek kadar öneme sahip olan bir delil etme yöntemidir. Bu yöntemle elde edilen delile ise, dijital delil denmektedir. Dijital deliller kolaylıkla bozulabilir ve değiştirilebilir olduğundan, adli bilişimin her aşaması adli bilişim uzmanı tarafından yönetilmelidir.

Bu çalışmada, hazırlanan senaryo üzerinde adli bilişim incelemelerinin uygulamalı olarak gösterilmesi, kolluk kuvvetlerinin bilişim suçları birimlerinde çalışan personel başta olmak üzere, tüm kolluk kuvvetleri ile bu alana ilgi duyan kişilerin adli bilişim ile ilgili kendilerini geliştirmeleri açısından önemlidir.

1.2 Araştırmanın Amacı

Kolluk kuvvetlerince yürütülmekte olan bilişim suçları ve bilişim yoluyla işlenen suç soruşturmalarında adli bilişim yöntemlerinin kullanılması gerekmektedir. Bu yöntemlerin kullanılmadığı takdirde soruşturma eksik kalacak, mağdurun mağduriyeti giderilemeyecek ve suçlu da cezalandırılamayacaktır.

Adli bilişim incelemelerinde kullanılan yöntemler gelişen teknolojiye bağlı olarak değişim gösterdiğinden, teknolojinin sağladığı yeni yöntemlerin adli bilişim alanında çalışan uzman personel tarafından biliniyor ve uygulanıyor olması gerekmektedir. Bu çalışma, özellikle kolluk kuvvetlerinin bilişim suçları ve adli bilişim alanında çalışan personel tarafından eksiksiz bir soruşturma yürütülmesini, personelin kendisini yenilemesini ve geliştirmesini sağlayacak bir kılavuz olmayı amaçlamaktadır.

1.3 Araştırmanın Kapsamı

Özellikle bilişim suçları ile mücadele eden kolluk kuvvetleri başta olmak üzere, diğer adli soruşturmalarda çalışmakta olan kolluk kuvvetleri ile özel sektörde bilişim alanında çalışanlar, bilişim suçları ve adli bilişim alanına ilgi duyan kişiler ve adli mercilerde bilirkişi görevi yapmak isteyen herkesi kapsamaktadır.

Adli bilişimde inceleme işlemi, söz konusu olay odaklı olması gerekmektedir. Yani her olay için gerçekleştirilen inceleme işlemi esnasında kullanılan yöntem farklılık göstermektedir. Bu çalışma kapsamında uygulanan senaryoda, sadece banka ve/veya kredi kartlarının kötüye kullanılması suçu üzerinde inceleme işlemi gerçekleştirildiğinden, diğer suç türlerinde yapılması gereken adli bilişim yöntemlerinden bahsedilememiş olması araştırmanın kapsamını daraltmaktadır.

1.4 Araştırmanın Yöntemi ve Aşamaları

Bu araştırmada, uygulamalı tanıtsal araştırma yöntemi kullanılmış ve araştırma verileri literatür taraması yapılarak elde edilmiştir. Çalışmanın ilk kısmı olan giriş bölümünde araştırmanın önemi, amacı ve kapsamı ile çalışma hakkında genel bir bilgilendirme yapılmıştır. Bilgisayar, internet ve bilişim suçları ile ilgili temel kavramlar başlıklı ikinci bölümde araştırma konusu ile ilgili literatür taraması yapılarak bilişim sistemlerinin kullanıldığı suçlar ve bu suçu işleyen suçluların kullanmakta oldukları yöntemler hakkında bilgi verilmiştir. 5237 sayılı Türk Ceza Kanununda (TCK) siber suçlar başlıklı üçüncü bölümde, Türk hukuk sisteminde yer alan siber suçlar ve bilişim sistemleri kullanılmak suretiyle işlenen suçlardan bahsedilmiş ve dördüncü bölümde ise, daha çok siber suç soruşturmalarında kullanılan ve Ceza Muhakemesi Kanununun (CMK) 134. maddesinde bahsi geçen delil elde yöntemi olan adli bilişim ve bu alanda kullanılmakta olan cihaz, yazılım ve yöntemler anlatılmıştır.

Çalışmanın materyal ve metot başlıklı beşinci bölümünde, oluşturulan bir senaryo kapsamında siber suç soruşturması yürütüldüğü varsayılarak, IP numarası tespitinin

yapıldığı, yapılan tespit neticesinde şüpheli şahsın adresinde arama yapıldığı ve yapılan aramada 3 (üç) adet dijital materyale incelenmek üzere el konulduğu yönündeki kurgu sonrasında, el konulan dijital delillere uygulanan adli bilişim aşamaları anlatılmış, altıncı bölümde senaryo gereği yapılan inceleme neticesinde tespiti yapılan dijital delillerin değerlendirmesi yapılmış ve son olarak yedinci bölümde ise, adli bilişim kapsamında yaşanan hukuki ve teknik sorunlar tartışıldıktan sonra çalışma sonlandırılmıştır.

1.5 Araştırmanın Kısıtlılıkları

Adli bilişim teknolojisinde kullanılan yöntemler her suç için farklılık gösterdiğinden dolayı, bu araştırma adli bilişim açısından Banka ve/veya Kredi Kartlarının Kötüye Kullanılması suçu ile kısıtlıdır.

2. BİLGİSAYAR, İNTERNET VE BİLİŞİM SUÇLARI İLE İLGİLİ TEMEL KAVRAMLAR

Gelişen ve sürekli yenilenen bilişim teknolojileri ile birlikte, klasik suç olarak tabir edilen ve yasa koyucular tarafından kanunlarla suç olarak tanımlanan dolandırıcılık, tehdit, taciz ve şantaj gibi birçok suçun büyük bir kısmı, artık doğrudan bilgisayar ve internet ortamında ya da bilgisayar ve internet araç olarak kullanılması suretiyle yaygınlaşarak işlenmeye devam etmektedir. "Bilişim teknolojileri bazı klasik suçların daha kolay işlenmesine imkan vermesinin yanında, yeni tip suçların da ortaya çıkmasını sağlamıştır (Başıbüyük ve Hekim 2013)."

Bilgisayarın suçta doğrudan ya da dolaylı yoldan kullanılması, teknolojinin gelişme hızı ile doğru orantılı bir şekilde artış gösterdiğinden bu suç türlerinin daha anlaşılır bir şekilde açıklanabilmesi için, öncelikle bilgisayar ve internetin doğru bir biçimde anlaşılması gerekmektedir. Bu sebeple bilgisayar, internet ve bilişim suçları ile ilgili temel kavramlar aşağıda ayrıntılı bir şekilde açıklanmıştır.

2.1 Bilgisayar

Kendisine verilen bilgileri istediğimizde saklayabilen, istediğimizde geri verebilen cihaz olarak adlandırılan bilgisayarın günümüzde, neredeyse kullanılmadığı hiçbir alanın olmadığı açıkça görülmektedir (İnt.Kyn.1).

Bilgisayar, Türk Dil Kurumu'nun Güncel Türkçe Sözlüğünde "Çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin" olarak tanımlanmıştır (İnt.Kyn.2).

Yine bilgisayar başka bir kaynakta ise "kendine önceden yüklenmiş program gereğince çeşitli bilgileri-verileri uygun ortamlarda saklayan ve istenildiğinde geri getiren, çeşitli aritmetik ve mantıksal işlemler yapan; çok hızlı çalışan elektronik bir cihaz" şeklinde tanımlanmıştır (İnt.Kyn.3).

Belli kuralları dahilinde çalışan, verileri işleyerek sonuçlar elde eden, problem çözen ve bir veya birden fazla görevi yerine getirmek üzere meydana getirilmiş parçalar bütünü (Topaloğlu 2014) olan bilgisayar, günümüzde çok farklı alanlarda kullanılmaya başlandığından "monitör, kasa, klavye ve fare gibi temel donanım unsurlarından" oluşmayan ancak, özellikleri nedeniyle içlerinde bilgisayarların bir kısım özelliklerini barındıran ya da bilgisayarların yaptığı bir takım işleri yapan makineler üretilmeye ve kullanılmaya başlanmıştır (Dülger 2013).

Bilgisayarın hayatın her alanında farklı şekillerde kullanılmaya başlaması bilgisayar ile ilgili yapılan tanımlamalarda da farklılıklar meydana getirdiği görülmektedir. Çizelge - 2.1'de belirtilen bilgisayarın değişmeyen 4 donanım unsuru (İnt.Kyn.3) göz önünde bulundurularak bir tanımlama yapmak gerekirse;

Bilgisayar; belirli kurallar dahilinde çalışan, kendisine giriş birimleri tarafından aktarılan bilgiyi saklayabilen, işleyebilen ve sonuçlandırabilen elektronik makine olarak adlandırılabilir.

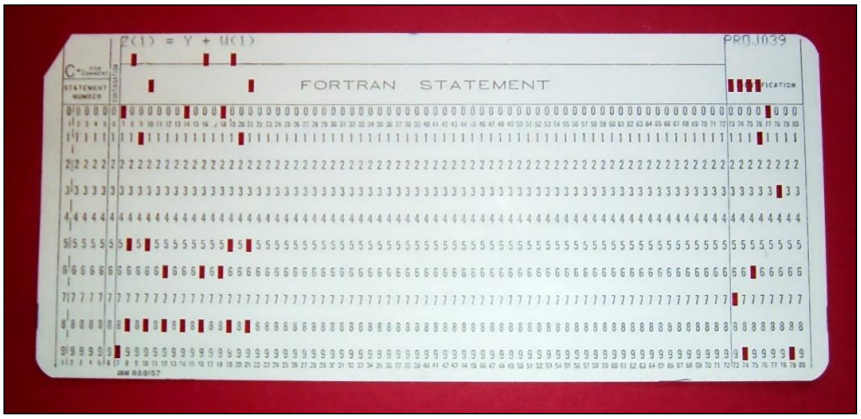
Çizelge 2.1 Bilgisayarın Değişmeyen Donanım Unsurları.

1. Unsur	Bilginin Girişi	**Giriş Birimleri:** Klavye, Fare, Kamera, Tarayıcı, Fax-Modem vb.
2. Unsur	Bilginin Saklanması	**Hafıza:** Harddisk, CD/DVD vb.
3. Unsur	Bilginin İşlenmesi	**Beyin:** CPU (Central Processing Unit - Merkezi İşlem Birimi) vb.
4. Unsur	Bilginin Çıkışı	**Çıkış Birimleri:** Ekran, Yazıcı, Çizici, Modem vb.

2.1.1 Bilgisayarın Tarihi Gelişimi

Geçmişte "bilgisayar" olarak bilinen birçok aygıt yazılımlanabilir olmamaları nedeniyle günümüz ölçütlerine göre bu tanımı hak etmemektedirler. 1801 yılında Joseph Marie Jacquard'ın dokuma tezgâhındaki işlemi otomatikleştirmek adına ürettiği delikli kartlar ise bilgisayarların gelişme sürecindeki, kısıtlı da olsa, ilk yazılımlanabilme izlerinden sayılmaktadır. Kullanıcının sağladığı bu kartlar sayesinde, dokuma tezgahı kart

üzerindeki delikler ile tarif edilen çizme işleyişini uyarlayabiliyordu (İnt.Kyn.1). Resim 2.1'de örnek bir delikli kart gösterilmiştir.

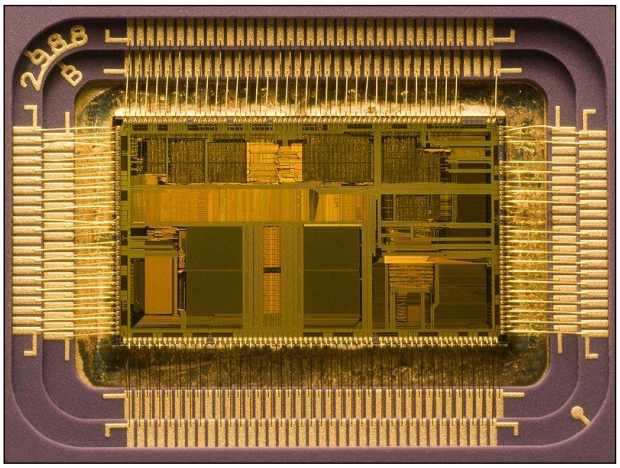


Resim 2.1 Delikli Kart (İnt.Kyn.1).

1946 yılında Amerika Birleşik Devletleri Ordusu tarafından geliştirilen ENIAC, onluk sayı tabanına dayalı olan ilk genel kullanım amaçlı elektronik bilgisayar unvanına sahiptir (İnt.Kyn.1). Resim 2.2'de ilk bilgisayar olan ENIAC gösterilmiştir.

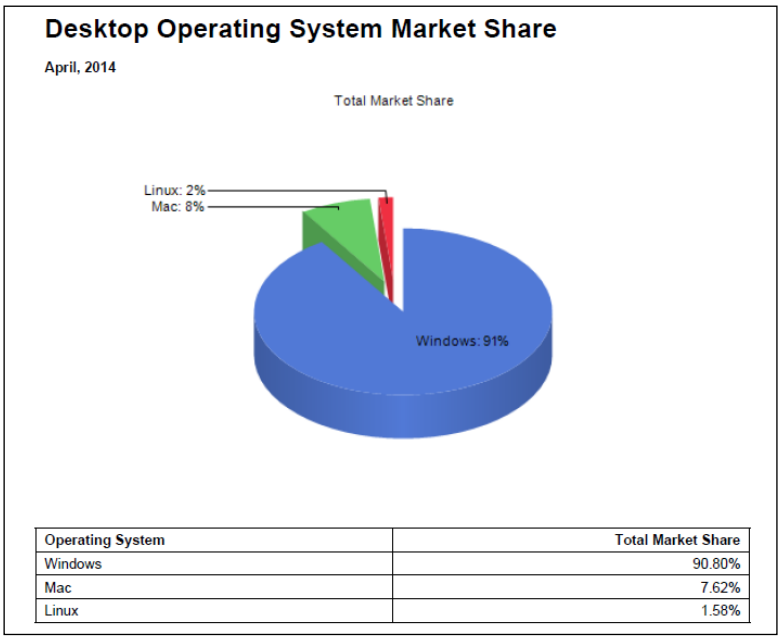
Resim 2.2 ENIAC İsimli Bilgisayar (İnt.Kyn.1).

1960'larda daha hızlı ve ucuz olan transistor (geçirgeç) tabanlı bilgisayarlar yaygınlık kazandı ve bilgisayarların daha önce görülmemiş bir düzeyde toplu üretimine geçildi. 1970'lere varıldığında ise, tümleşik devre teknolojisi ve İntel 4004 gibi mikroişlemcilerin geliştirilmesi sayesinde bir kez daha büyük bir başarım ve güvenilirlik artışının yanı sıra, maliyet düşüşü de yaşandı (İnt.Kyn.1). Resim 2.3'de İntel firmasına ait bir mikroişlemci gösterilmiştir.



Resim 2.3 Mikroişlemci (İnt.Kyn.1).

Bir ABD şirketi olan IBM (International Business Machines; Uluslararası İş Makineleri), 1981 yılında ilk kişisel bilgisayarı ürettikten kısa bir süre sonra diğer bilgisayar şirketleri, IBM gibi kendi bilgisayarlarını tasarlamaya başladılar. Apple isimli şirket 1983 yılında faresi olan bir bilgisayar olan Macinmtosh'u üretmesi ile birlikte bilgisayar grafiksel kullanılmaya başlandı. 1986 yılında Microsoft isimli şirket, Windows 1.0'ı piyasaya sürmesi ile birlikte dünyada en çok kullanılan işletim sisteminin (İnt.Kyn.4) hikayesi başlamış oldu (İnt.Kyn.1).



Operating System	Total Market Share
Windows	90.80%
Mac	7.62%
Linux	1.58%

Şekil 2.1 Masaüstü Bilgisayar İşletim Sistemi Kullanım Oranı (İnt.Kyn.4).

1980'lerde artık bilgisayarlar, çamaşır makinesi, telefon ve televizyon gibi günlük hayat kullanımındaki birçok makinesel aygıtın yerlerini almaya başlamışlardı. Yine aynı dönemde, kişisel bilgisayarlar yaygınlık kazanıyorlardı. Son olarak 1990'lardaki internetin hızlı gelişimi ile de bilgisayarlar televizyon ve telefon gibi alışılmış birer aygıt haline gelmişlerdir (İnt.Kyn.1). Resim 2.4'de 1980 yıllarında IBM firması tarafından üretilen bir bilgisayar gösterilmiştir.

Resim 2.4 1980'li Yıllarda Bir Bilgisayar (İnt.Kyn.1).

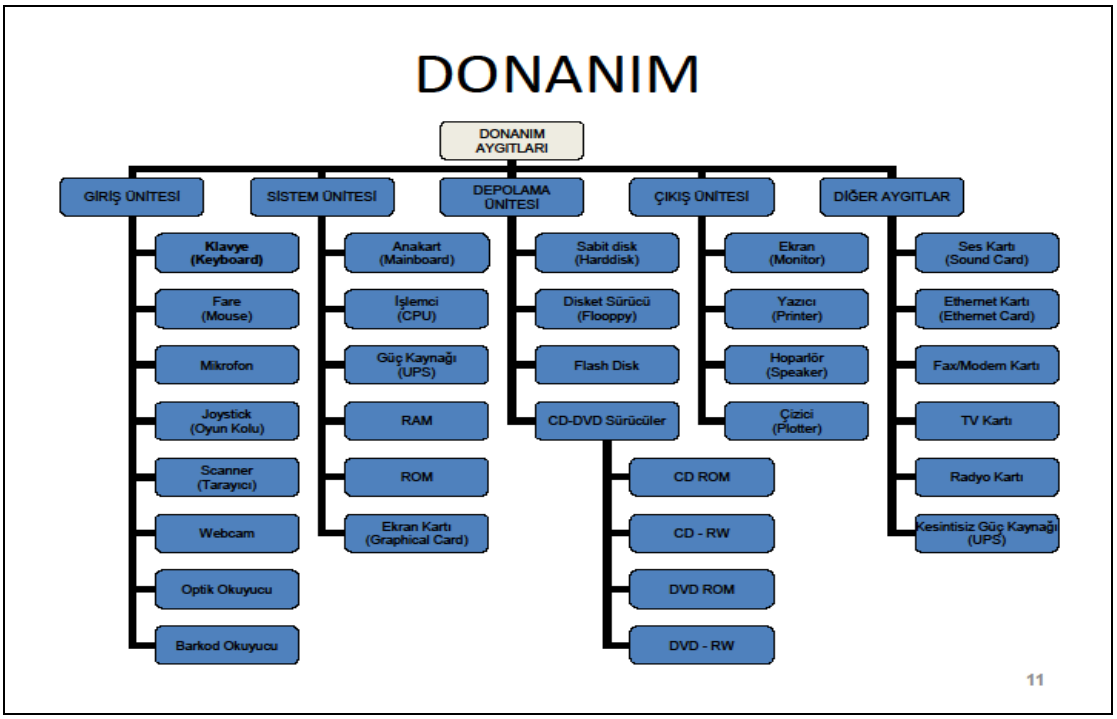
Günümüzde ise bilgisayarlar hayatın her alanına girmiş olmakla birlikte, bilgisayarın yerini almaya başlayan tabletler ve smart phone (akıllı telefon)'lar, klasik olarak bilgisayarın yaptığı sayısal ve mantıksal veri işlemin yanı sıra görsel, işitsel ve temasa dayalı veri girdilerinin de yüksek hızlarda işlenmesi ile kullanıcıya kullanım kolaylığı ve eğlence imkânı sağlamaktadır.

2.1.2 Bilgisayarı Oluşturan Unsurlar

Genel olarak bilgisayar donanım ve yazılım olmak üzere iki ana unsurdan oluşur. "Bilgisayarın elektronik kısmına donanım (hardware), program kısmına ise yazılım (software) denir (İnt.Kyn.3)."

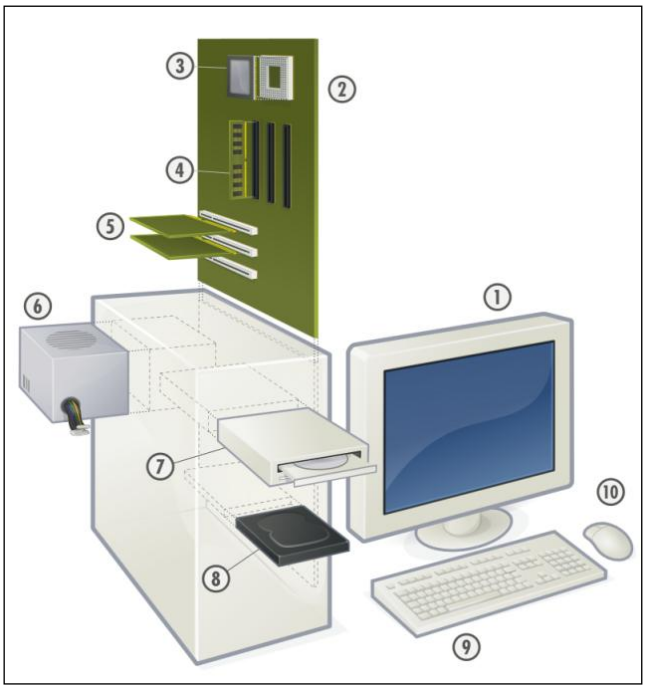
2.1.2.1 Donanım

Fiziksel olarak bilgisayarı oluşturan parçaların tümü donanım olarak adlandırılmaktadır. Elle tutulup gözle görülen elektronik devrelerden oluşmaktadır. Ekran (monitör), klavye (keyboard), sabit disk (harddisk), fare (mause), yazıcı (printer), bellek (RAM) ve işlemci (CPU) gibi bileşenler donanıma örnek olarak verilebilir. Donanım aygıtları giriş ünitesi, sistem ünitesi, depolama ünitesi ve çıkış ünitesi olarak sınıflandırılabilir. Şekil 2.2'de donanım aygıtları ayrıntılı bir şekilde görülmektedir (İnt.Kyn.5).



Şekil 2.2 Bilgisayarın Donanım Birimleri (İnt.Kyn.5).

Aşağıdaki Şekil 2.3'de bir kişisel bilgisayarda bulunan donanımlar gösterilmektedir. (1) Ekran, (2) Ana kart, (3) İşlemci (CPU), (4) Bellek (RAM), (5) Genişletme Kartları (PCI-X, AGP, v.b.), (6) Güç Kaynağı, (7) Optik Disk Sürücü (DVD, CD, v.b.), (8) Sabit Disk, (9) Klavye ve (10) Faredir (İnt.Kyn.1).



Şekil 2.3 Kişisel Bilgisayarda Bulunan Donanımlar (İnt.Kyn.1).

2.1.2.2 Yazılım

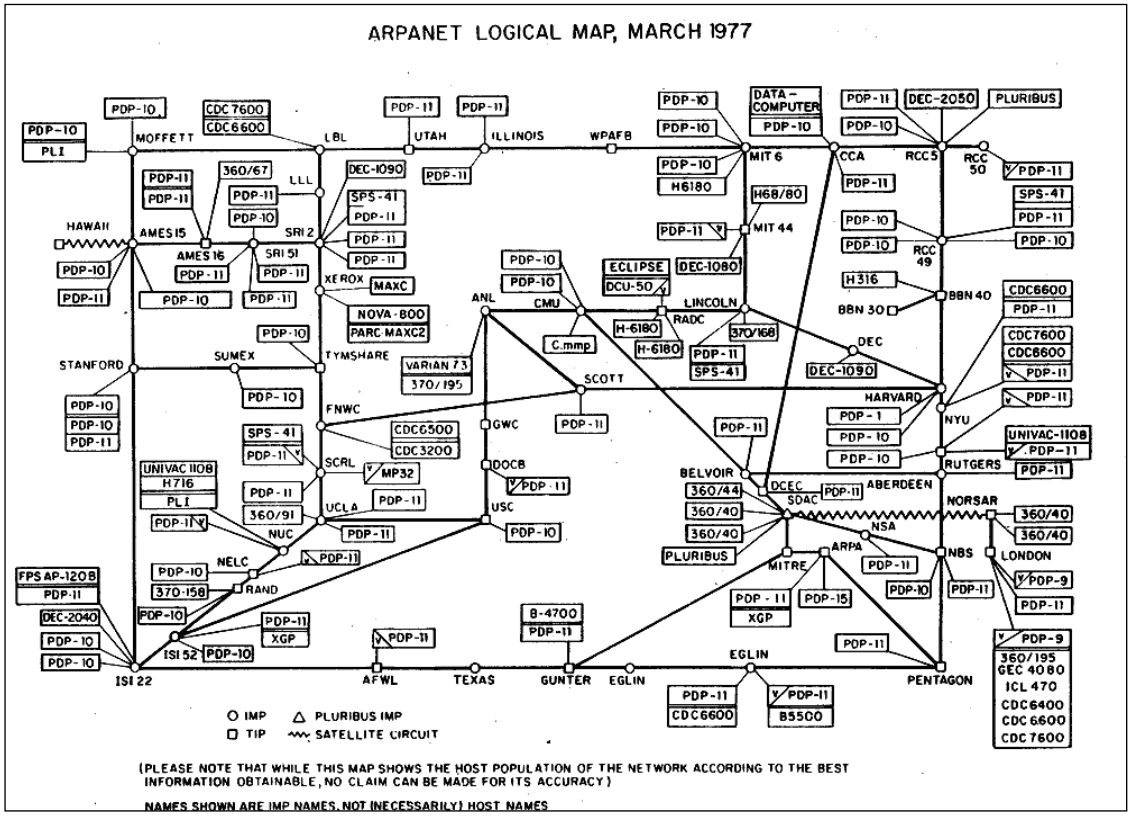
Donanım insanın vücuduna benzetilecek olursa; yazılım onun ruhudur. Yazılımlar, bir bilgisayar dili (kodlama) ile yazılmış programlardır. Yazılım program ve veri olmak üzere iki unsurdan oluşur. Program bilgisayarın sıralı olarak yapması gereken işlemleri belirleyen bir komutlar zinciri iken, veri ise bilgisayarın herhangi bir konuyu işleyerek, istenilen sonucu vermesi için uygulanan ön bilgilerdir (İnt.Kyn.5).

Yazılım, sistem yazılımları ve uygulama yazılımları olarak ikiye ayrılır. Sistem yazılımlarına, Microsoft şirketine ait Windows 8 işletim sistemi, Apple şirketine ait Macintosh (MacOS X) işletim sistemi, açık kaynak kodlu Linux işletim sistemi vb. örnek olarak verilebilirken, uygulama yazılımlarına ise, antivirüs programları, ticari yazılımlar, oyunlar, veri tabanı yazılımları, ofis yazılımları vb. örnek olarak verilebilir.

2.1.3 Bilgisayar Ağları

Vikipedi Özgür Ansiklopedi'de bilgisayar ağı "Birden fazla bilgisayar veya iletişim cihazını, bilgi alışverişi yapabilmeleri ve farklı kaynakları paylaşabilmeleri için, kablolar veya radyo dalgaları kanalıyla birbirine bağlayan yapıya "ağ" denir." şeklinde tanımlanmaktadır ve iki bilgisayarın birbirine kablo yardımıyla bağlanmasıyla en basit bilgisayar ağı oluşmaktadır (İnt.Kyn.6).

Bilgisayarlar 1950`lerden beri çoklu ortamlar arasında bilgi koordinasyonu kurmak amacıyla kullanılmıştı, ancak 1970'lerde ABD'li mühendisler ordu içerisinde yürütülen bir tasarı çerçevesinde bilgisayarları birbirleri ile bağlayıp (ARPANET), günümüzde bilgisayar ağı olarak bilinen yapının temelleri atılmış oldu. ABD ordusunun sistemi bu tür sistemlerin geniş kapsamlı ilk örneğiydi ve bu sistem birçok özel amaçlı ticari sistemlere öncülük etmiştir (İnt.Kyn.1).



Şekil 2.4 ARPANET'in Mantıksal Haritası (İnt.Kyn.1).

1990'lara gelindiğinde ise, İsviçre'nin CERN araştırma merkezinde geliştirilen küresel ağ (World Wide Web, www) adlı iletişim kuralları, e-posta gibi uygulamalar ve ethernet (ağ bağdaştırıcısı) gibi ucuz donanımsal çözümler ile bilgisayar ağlarının kullanılmasında yaygınlık kazandırmıştır (İnt.Kyn.1).

En çok bilinen bilgisayar ağları büyüklüklerine göre PAN (Personal Area Network; Kişisel Alan Ağı), LAN (Local Area Network; Yerel Alan Ağı), MAN (Metropolitan Area Network; Şehir Alan Ağı), WAN (Wide Area Network; Geniş Alan Ağı), VPN (Virtual Private Network; Sanal Özel Ağ), CAN (Controller Area Network; Kontrolör Alan Ağı) ve SAN (Storage Area Network; Depolama Alan Ağı)'dır (İnt.Kyn.6).

Günümüzde en çok bilinen ve yaygın olarak kullanılan ağların başında LAN ve WAN ağları gelmektedir.

2.1.3.1 Yerel Alan Ağı (LAN)

Küçük alanları (bina, firma, departman, oda vb.) kapsayan yüksek hızlı bir veri ağıdır. Yerel ağ içinde bilgisayarlar, workstation (iş istasyonu), yazıcılar, çiziciler ve diğer çevre birimleri yer alabilir. LAN, bilgisayar kullanıcılarına uygulamalara ve cihazlara ulaşım, bağlı kullanıcılar arasında dosya değişimi, elektronik posta ve diğer uygulamalar yoluyla haberleşme gibi çeşitli avantajlar sağlarlar. Fakat LAN, yapısı itibarı ile yerel bir ağ olduğu için, ancak bir bina veya bir kat içerisinde kurulabildiğinden kapsama alanı dardır (İnt.Kyn.7).

2.1.3.2 Geniş Alan Ağı (WAN)

Coğrafi olarak birbirinden uzak yerlerdeki (şehirlerarası/ülkelerarası) bilgisayar sistemlerinin veya yerel bilgisayar ağlarının birbirleri iletişimini sağlayan ağlardır. Genellikle kablo ya da uydular aracılığı ile uzak yerleşimlerle iletişimin kurulduğu bu

ağlarda çok sayıda iş istasyonu kullanılır. WAN'lar üzerinde on binlerce kullanıcı ve bilgisayar çalışabilir (İnt.Kyn.7).

Bilgisayar ağlarından tam anlamıyla faydalanmak, coğrafi olarak nerde olursa olsun, fiziksel olarak nasıl ayrılırsa ayrılsın, birbirinden ayrı LAN'ların tüm çalışanları ve bilgi işlem kaynaklarını bir araya getirecek şekilde bağlanmasıyla gerçekleşir (İnt.Kyn.7). Bunu da sağlayan WAN'ın en meşhur olanı, neredeyse tüm bilgisayar kullanıcılarının kullanıldığı internettir (İnt.Kyn.6).

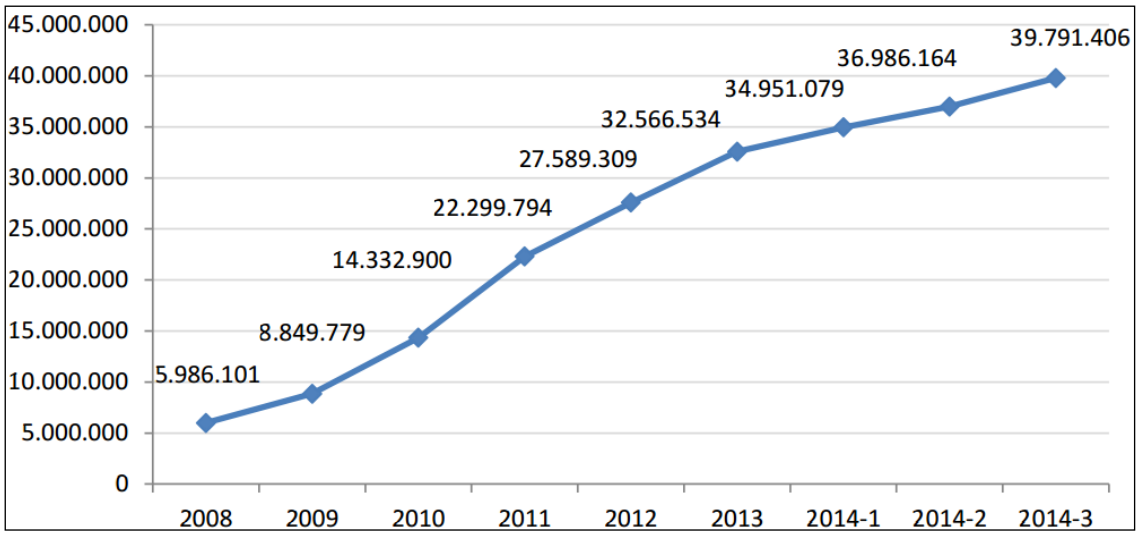
2.2 İnternet

İnternet, dünya çapında herkese açık bir haberleşme ağıdır. Çok sayıda bilgisayarı birbirine bağlayarak iş dünyası, devlet kuruluşları ve eğitim kuruluşları arasında dünya çapında iletişim yapma olanağı sağlayan uluslararası bir bilgisayar ağıdır. Ancak hiçbir organizasyon internetin sahibi değildir ve onu kontrol etmemektedir. Bu yapının parçaları olan ağlar, devlet kuruluşları, üniversiteler, gönüllü organizasyonlar ve ticari kuruluşlar tarafından çalıştırılmaktadır (Seferoglu 2006).

Çok protokollü bir ağ olup birbirine bağlı bilgisayar ağlarının tümünü ifade eden internet, binlerce akademik ve ticari ağla devlet ve serbest bilgisayar ağının birbirine bağlanmasıyla oluşmuş bir ağdır (İnt.Kyn.8).

"İnternetin insan hayatında önemli role sahip olması ile aynı zamanda birçok fırsat sunması, internet kullanımının gün geçtikçe artmasına olanak tanımıştır (Çubukçu 2014)."

Bilgi Teknolojileri ve İletişim Kurumu (BTK) verilerine göre, Türkiye'de 2008 yılında 6 milyon genişbant (sabit, mobil, kablo, fiber vb.) internet abonesi bulunurken, altı yıl gibi bir sürede altı katı aşan artışla, 2014 yılı üçüncü çeyrek sonu itibarıyla genişbant internet abone sayısı 40 milyona yaklaşmıştır (BTK 2014).



Şekil 2.5 Genişbant İnternet Abone Sayısı (BTK 2014).

Türkiye'de internet kullanımının bu denli artması, klasik suç olarak adlandırılan dolandırıcılık, hırsızlık, sahtecilik vb. suç türlerinin bilgisayar ve internet vasıtasıyla işlenmesi olasılığını da artırmaktadır.

2014 yılı üçüncü çeyrekte 3G (3. Nesil) abone sayısı yaklaşık 57 milyona ulaşırken, 3G hizmetiyle birlikte mobil bilgisayarlardan ve cep telefonundan internet hizmeti alan mobil abone sayısı ise, 31 milyonu geçmiştir (BTK 2014).

Çizelge 2.2 3G Hizmeti Kullanıcı Verileri (BTK 2014).

	2013-3	**2013-4**	**2014-1**	**2014-2**	**2014-3**
3G Abone Sayısı	47.533.786	49.266.163	51.023.960	53.385.734	59.780.787
Mobil Bilgisayardan İnternet	1.742.995	1.701.014	1.541.425	1.379.300	1.277.070
Mobil Cepten İnternet	21.099.677	22.472.129	24.902.507	27.066.363	29.826.976
Mobil İnternet Kullanım Miktarı TByte	38.944	43.686	52.359	61.913	84.940

3G internet teknolojisi ile birlikte, internetin bilgisayarlar dışında akıllı cep telefonları ve tablet bilgisayarlar tarafından her geçen gün artarak kullanılması, bilişim suçlarının

işlenme metotlarında yenilikler getirmektedir. Bu sebeple de, suçla mücadele eden kurumlar suçluyu yakalamakta ve suçu delillendirmede zorluk yaşamaktadırlar. Dolayısıyla, bilişim yoluyla işlenen suçlar ve bilişim suçlarında bilgisayar kullanılması zorunluluğu ortadan kalkacak, böylece suçlular suç işlemek için çok uzağa gitmek zorunda kalmadan elinde bulunan cihazlar sayesinde kendisini gizleyerek suç işleyecekler.

İnterneti oluşturan ve bilişim suçu soruşturmaları kapsamında bilinmesi gereken en temel kavramlara bakacak olursak, IP (Internet Protocol) numarası en ön sırada yer alacaktır. Sonrasında ise, alan adı (domain), yer sağlayıcı (hosting) ve internet servis sağlayıcı (ISS) gelmektedir. Bu kavramların açıklamaları aşağıda başlıklar halinde yer almaktadır.

2.2.1 IP Numarası Nedir?

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanuna dayanak olarak hazırlanan 30.10.2007 tarih ve 26716 sayılı Resmi Gazete'de yayımlanan İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelikte, IP adresi "Belirli bir ağa bağlı cihazların birbirini tanımak, birbirleriyle iletişim kurmak ve birbirlerine veri yollamak için kullandıkları, İnternet Protokolü standartlarına göre verilen adres" şeklinde tanımlanmıştır.

İnternet Kontrol Protokolü standardını kullanan bir ağdaki cihazların birbirini tanımak, birbirleriyle iletişim kurmak ve veri alışverişinde bulunmak için kullanılan benzersiz bir numara olan IP adresi ya da numarası, bugün suçluların takibinden online satış ve pazarlamaya kadar çok çeşitli alanlarda yaygın olarak yararlanılan bir veridir. IP numarasına bakarak kullanıcının bulunduğu ülkeyi, kenti, enlem ve boylamı ve ISS'nı belirlemek mümkündür (İnt.Kyn.9).

IP numarası, bilişim suç soruşturmalarında kolluk kuvvetleri tarafından bilişim

suçlusunun tespit edilebilmesi için temel delil niteliğinde değerlendirilmektedir. Ancak IP numarası adli makamlarca tek başına delil kabul edilmediğinden, delil niteliğinden çok suçlunun tespitine yönelik yapılan çalışmada kullanılan yöntem olarak kullanılmaktadır. IP numarası tespiti sonrasında şüpheli şahsın kullanmakta olduğu bilgisayar/bilgisayar kütükleri ve dijital materyaller üzerinden arama, elkoyma ve inceleme işlemlerinin yapılması gerekmekte, inceleme neticesinde suça ilişkin delil elde edilmesi halinde IP numarası delil olarak değerlendirilecektir. Aksi takdirde yalnız IP numarası tespiti ile bir şahsın cezalandırılması hukuki olmayacaktır.

IP numarası, internet ortamından çok kolay bir şekilde temin edilen programlar ve zararlı yazılımlar vasıtası ile değiştirilebilmekte ve suça karışan şahıslar kendilerini bu yöntem ile kolaylıkla gizleyebilmektedirler.

2.2.2 Alan Adı Nedir?

5809 sayılı Elektronik Haberleşme Kanununun 5 inci, 34 üncü ve 35 inci maddelerine dayanak olarak hazırlanan 07.10.2010 tarih ve 27752 sayılı Resmi Gazete'de yayımlanan İnternet Alan Adları Yönetmeliğinde, internet alan adı "İnternet üzerinde bulunan bilgisayar veya internet sitelerinin adresini belirlemek için kullanılan internet protokol adresini tanımlayan adlar" şeklinde tanımlanmıştır.

Alan adı, ingilizce "domain" kelimesinden gelmekte ve bir web sitesinin internetteki adı ve adresi olarak tanımlanmaktadır. Alan adları IP adresinin daha basitleştirilmiş ve akılda kalması için kelimelerle ifade edilmiş halidir (İnt.Kyn.10). Örneğin; Afyon Kocatepe Üniversitesinin alan adı, 193.255.51.101 IP numarasına karşılık gelen www.aku.edu.tr, Yükseköğretim Kurulu Başkanlığının alan adı ise, 193.140.255.1 IP numarasına karşılık gelen www.yok.gov.tr'dir.

Hiyerarşik bir yapıya sahip olan alan adlarında nokta ile ayrılan bölümler soldan sağa doğru artan düzeyde bir önem sırasına sahiptir. Alan adları TLD (Top Level Domain –

Birinci Derece Alan Adı) ve SLD (Second Level Domain – İkinci Derece Alan Adı) olmak üzere en az iki kısımdan oluşmaktadır. www.btk.gov.tr alan adında en sağdaki bölüm "gov.tr" TLD, ortadaki "btk" ise SLD'dir (İnt.Kyn.26).

1980'lerde oluşturulan ".com, .edu, .gov, .int, .mil, .net ve .org" olmak üzere toplam yedi adet TLD'den ".com, .net ve .org" kısıtlama olmaksızın herkes tarafından tescil edilebilmektedir (İnt.Kyn.11). 5809 sayılı Elektronik Haberleşme Kanununun İnternet Alan Adları Yönetmeliğinde belgeli tahsis edilen alan adları aşağıda bulunan Çizelge 2.3'deki gibi tanımlanmıştır.

Çizelge 2.3 Alan Adları ve Tahsisine Yetkili Olan Kurumlar.

Alan Adı	Tahsis Edilecek Taraf
.av	Türkiye Barolar Birliğine kayıtlı serbest avukatlar, hukuk büroları ve avukatlık ortaklıkları.
.bel	İçişleri Bakanlığı kayıtlarında yer alan belediyeler.
.dr	Türk Tabipler Birliğine kayıtlı tıp doktorları, doktor ortaklıkları, hastaneler ve Sağlık Bakanlığı birinci basamak sağlık kuruluşları.
.edu	T.C. Yüksek Öğretim Kurumu (YÖK) tarafından tanınan yüksek eğitim kurumları.
.gov	Kamu kurum ve kuruluşları.
.pol	Emniyet Genel Müdürlüğü ve bünyesindeki birimler.
.k12	Milli Eğitim Bakanlığı (MEB) tarafından onaylanmış okul öncesi eğitim veren kreş, anaokulu, ilköğretim, lise ve dengi öğretim kurumları.
.tsk	Türk Silahlı Kuvvetleri bünyesinde yer alan birimler.

Kısıtlama olmaksızın herkes tarafından tescil edilebilen ve en çok kullanılan ".com" uzantılı web siteler üzerinde herhangi bir denetleme söz konusu değildir. Kişi kendisinin isteği doğrultusunda kullanmayı arzuladığı herhangi bir ismi kullanabilmektedir. Ancak ".com" uzantısından sonra ".tr" kullanmak istenildiğinde ise, Bilgi Teknolojileri ve İletişim Kurumu tarafından belirlenen belgelerin tamamlanması gerekmektedir. Gerekli belgeleri tamamlayanlar Orta Doğu Teknik Üniversitesi bünyesinde bulunan Nic.tr (".tr" Alan Adları Yönetimi)'ye yaptıkları başvuruları kabul edildikten sonra ".com.tr" uzantılı alan adını kullanabilmektedirler.

5809 sayılı Elektronik Haberleşme Kanununun 07.10.2010 tarih ve 27752 sayılı Resmi Gazete'de yayımlanan İnternet Alan Adları Yönetmeliğinde tanımlanan, alan adı tahsisi ile yetkili kayıt kuruluşlarının yükümlülüklerinden bazıları aşağıda belirtilmiştir.

- İlgili mevzuata uymak,
- Sundukları hizmetlerin erişilebilirliğini, güvenliğini, güvenilirliğini ve bütünlüğünü sağlamak,
- Sundukları hizmetlerin kalitesi ve sürekliliği ile ilgili bir aksamanın yaşanmamasını sağlamak ve gerekli teknik donanıma sahip olmak,
- 7 gün 24 saat eşit erişim imkânı sağlamak,
- Alan adı başvurusu ve diğer işlemler sırasında kişilerden tam ve doğru bilgiler almak, bilgilerin güvenliğini, gizliliğini ve güncelliğini sağlamak, bu bilgileri Bilgi Teknolojileri ve İletişim Kurumu ve yasal olarak yetkili kılınan taraflar haricinde hiçbir tarafa vermemek ve alınma amaçları dışında kullanmamak,
- Kendilerine yapılan alan adına ilişkin tahsis, yenileme, iptal gibi talepleri gerçek zamanlı ve TRABİS (.tr ağ bilgi sistemi)'te uygulanan yazılım standartlarına uygun olarak TRABİS'e iletmek,
- TRABİS üzerinden yürüttükleri alan adına ilişkin işlemlerde gerekli özeni göstermek,
- Kendilerinden hizmet alan ve almak isteyen kişileri; alan adına ilişkin başvuru, tahsis, yenileme, iptal ve transfer gibi işlemlerle ilgili olarak bilgilendirmek,
- Rehberlik hizmetine kendi İnternet siteleri üzerinden ücretsiz erişim imkanı sağlamak,
- Alan adı ile ilgili işlemlere ait bilgi ve belgeleri alan adının kullanımının sona ermesinden itibaren en az 10 yıl süre ile saklamak,
- Faaliyetleri sona ereceği zaman kayıt kuruluşu arası transfer işlemleri çerçevesinde gerekenleri yapmakla ve elindeki bilgi ve belgeleri Bilgi Teknolojileri ve İletişim Kurumuna tam ve doğru olarak zamanında teslim etmek,
- Her yıl Mart ayı sonuna kadar bir önceki yıla ait faaliyet raporunu Bilgi Teknolojileri ve İletişim Kurumuna sunmak,

- Tanıtıcı bilgilerini, ilgili mevzuatı ve başvuru formunun örneğini kendisine ait ".tr" uzantılı alan adına sahip internet sitesinde ilgili tarafların ulaşabileceği şekilde ve güncel olarak bulundurmakla yükümlüdür.

2.2.3 Yer Sağlayıcı Nedir?

Yer sağlayıcı, ingilizce "hosting" kelimesinden gelmekte ve bir web sitesinde yayınlanmak istenen sayfaların, resimlerin veya dokümanların internet kullanıcıları tarafından erişebileceği bir sunucu (server) bilgisayarda tutulmasıdır (İnt.Kyn.12).

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun "Tanımlar" başlığı altındaki 2. Maddesinde yer sağlayıcı, "Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişiler" şeklinde tanımlanmıştır.

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun 5. Maddesinde tanımlanan, yer sağlayıcının yükümlülükleri aşağıda belirtilmiştir.

- Yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir.
- Yer sağladığı hukuka aykırı içeriği haberdar edilmesi halinde yayından çıkarmakla yükümlüdür.
- Yer sağladığı hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdür.
- Telekomünikasyon İletişim Başkanlığının talep ettiği bilgileri talep edilen şekilde Telekomünikasyon İletişim Başkanlığına teslim etmekle ve bildirilen tedbirleri almakla yükümlüdür.

- Yer sağlayıcılık bildiriminde bulunmayan veya yükümlülüklerini yerine getirmeyen yer sağlayıcı hakkında Telekomünikasyon İletişim Başkanlığı tarafından on bin Türk Lirasından yüz bin Türk Lirasına kadar idari para cezası verilir.

Yer sağlayıcı, kimi zaman kamu kuruluşu, kimi zaman ticari şirket, kimi zaman da ileri seviyede bir bilgisayar kullanıcısı olabilmektedir. İyi seviyede bir bilgisayar kullanıcısı, kendi kullandığı kişisel bilgisayarını sunucu olarak kullanabilir ve sabit IP numarası üzerinden kendisine ait web sitelerini dünyaya yayın yapabilir. Bunun için, alan adı tahsis firmasından satın alacağı alan adı ve kullanmakta olduğu kişisel bilgisayarının 24 saat erişime açık olması yeterli olacaktır.

2.2.4 Erişim Sağlayıcı

5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun "Tanımlar" başlıklı 2. maddesinde erişim sağlayıcı, "Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişiler" olarak tanımlanmıştır.

Telekomünikasyon İletişim Başkanlığında kayıtlı 353 erişim sağlayıcı bilgisinin olduğu, bunlardan 86'sının değişik zamanlarda iptal edildiği, 267'sinin ise halen aktif olarak hizmet sunduğu görülmektedir (İnt.Kyn.13). Aktif olarak internet hizmeti sunmaya devam eden erişim sağlayıcılara TTNet, Süperonline, Smile, Biri, Millenicom, Doping vb. tüzel kişilikler örnek olarak verilebilir.

2.2.5 İçerik Sağlayıcı

5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun "Tanımlar" başlıklı 2. maddesinde içerik sağlayıcı, "İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişiler" olarak

tanımlanmıştır.

Vikipedi Özgür Ansiklopedi de içerik sağlayıcı, “radyo-televizyon yayını ya da internet gibi bir iletişim yolu aracılığıyla, ses, görüntü, bilgisayar yazılımı veya oyun gibi çoklu ortam içeriklerini sağlayan ileticidir.” şeklinde tanımlama yapılmıştır (İnt.Kyn.14). İçerik sağlayıcı kimi zaman Afyon Kocatepe Üniversitesinin resmi web sitesi olan www.aku.edu.tr’ye veri girişi yapmaya yetkili kurumsal kimliğe sahip personeller olabileceği gibi, hobi ve çeşitli bilgiler paylaşmak amacıyla kurulan bir blog sitesine veri girişi yapan bir kişi de olabilmektedir.

2.3 Bilişim Suçları

Günümüzde bilgisayarın neredeyse kullanılmadığı bir alanın kalmaması, bilişim suçlarının ortaya çıkmasına ve etki sahasının inanılmaz şekilde artmasına sebep olmuştur (Karagülmez 2011).

5237 Sayılı TCK’nın 2. Maddesinin 1. Fıkrasında yer alan “Kanunun açıkça suç saymadığı bir fiil için kimseye ceza verilemez ve güvenlik tedbiri uygulanamaz. Kanunda yazılı cezalardan ve güvenlik tedbirlerinden başka bir ceza ve güvenlik tedbirine hükmolunamaz.” hükmünden de anlaşılacağı üzere suç kavramının eksiksiz ve tam olarak anlaşılır olması gerekmektedir. “Suç kavramını anlamak, bilişim suçu kavramını tanımlarken yardımcı olacaktır (Say 2006).” Bu nedenle, bilişim suçlarının sınırlarının ve kapsamının daha net bir şekilde anlaşılabilmesi için, öncelikle suç kavramının neleri ifade ettiğinin açıklanması, sonrasında ise bilişim suçlarının neler olduğunun anlatılması gerekmektedir.

2.2.1 Suç Nedir?

İnsanlık tarihi kadar eski olan suç, günümüz toplumları için çözüm bekleyen önemli bir sosyal problem haline gelmiştir (Burkay 2008). Suç, tarihin farklı zamanlarında değişik

şekillere girerek insanoğlunun karşısına sürekli çıkmaktadır. Tarihte yeni denebilecek kadar çok uzak geçmişi olmayan bilişim suçları, bilişim ve teknoloji sistemlerini kullanan gencinden yaşlısına, kadınından erkeğine herkesin karşısına çok ciddi bir tehdit olarak çıkmaktadır.

TDK Büyük Türkçe Sözlük'te suç "Bir toplumda haksız sayılıp, yazılı-yazısız kurallarla yasaklanan ve yaptırımlara bağlanan davranış ve eylem." ve "Devletçe yasalarla tanımlanıp yaptırıma bağlanmış olan kurallara aykırı davranış." olarak tanımlanmıştır (İnt.Kyn.15).

Vikipedi Özgür Ansiklopedi'de ise, "yanlış ya da zararlı olduğu için yasaklanan ve bazı durumlarda cezalandırılan davranış. Hukuki anlamda suç, bir toplumdaki hukuki kurumlar tarafından ceza veya güvenlik tedbiri yaptırımına bağlanmış fiildir." şeklinde açıklanmıştır (İnt.Kyn.16).

Kişi hak ve özgürlüklerini, kamu düzen ve güvenliğini, hukuk devletini, kamu sağlığını ve çevreyi, toplum barışını korumak, suç işlenmesini önlemek amacıyla çıkartılan 5237 Sayılı TCK'da suçlar, cezalar ve güvenlik tedbirlerinin türleri maddeler halinde düzenlenmiştir. Tez konusu ile ilgili suç türleri ileride yer alan bölümlerde ayrıntılı bir şekilde anlatılacaktır.

Kısaca suç, yazılı ya da yazılı olmayan kurallar ile yasaklanan ve sonucu kanunlar çerçevesinde bir yaptırıma bağlanmış fiili anlatmakta olup, bu fiili işleyen kişiye ise suçlu denilmektedir.

2.2.2 Bilişim Nedir?

Dil Derneği'nin Türkçe Sözlüğünde enformatik ve informatik olarak da adlandırılan bilişim, "Bilimsel, toplumsal, sanatsal, ekonomik ve teknik bilgilerin bilgisayarda değerlendirilmesi, bölümlendirilmesi, saklanması, erişilebilmesi ve yayılması

yöntemlerini konu edinen bilim dalı.” olarak tanımlanmaktadır (İnt.Kyn.17).

Dülger tarafından bilişim, “insanların 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).

Aydın (1992) ise, bilişim tanımını “Bilginin iletişim yapısı ve özellikleri; bilginin aktarılması, organize edilmesi, saklanması, tekrar elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemler ve öte yandan da; bilgiyi kaynağından alıp kullanıcıya aktaran ve genel sistem bilimi, sibernetik, otomasyon ile insanın çalışma çevrelerindeki yerinde ve zamanında kullanılan teknolojileri temel alan bilgi sistemleri, şebekeleri, işlevleri, süreçler ve etkinlikleridir.” şeklinde yapmıştır.

Avrupa Konseyi Siber Suç Sözleşmesinin 1/a maddesinde bilişim yerine, dar kapsamlı bir ifade olan “bilgisayar sistemi” ifadesi kullanılmış ve “bilgisayar sistemi, herhangi bir cihaz ve birbiriyle bağlantılı bir grup veya cihazlar yoluyla bir veya birden fazla program tarafından devam ettirilen verinin otomatik olarak işlenmesi, bu işlemin yerine getirilmesi” ifadesi kullanılmıştır.

5237 Sayılı TCK’nın yürürlüğe girmesi ile birlikte yürürlükten kalkan 765 Sayılı TCK’ya 6 Haziran 1991 tarihinde eklenen Bilişim Alanında Suçlar başlığı altındaki 525. Maddede bilişim kavramı yerine “Bilgileri otomatik işleme tabi tutmuş sistem” tabirinin kullanıldığı görülmüştür.

1 Haziran 2005 tarihinde yürürlüğe giren 5237 Sayılı TCK’da ise bilişim sistemi, 10. Bölümde Bilişim Alanında Suçlar başlığı altında yer alan Bilişim Sistemine Girme başlıklı 243. maddenin gerekçesinde “Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemlerdir.” şeklinde tanımlama yapıldığı görülmektedir.

2.2.3 Bilişim Suçu Nedir?

Bilişim sistemlerinin çok farklı tiplerde olmasından ve bu sistemler ile işlenebilecek suç türlerinin de çeşidinin çok fazla olmasından dolayı, bilişim suçlarının da birçok tanımı vardır. Kanunun açıkça suç saymadığı bir fiil için kimseye ceza verilemeyeceği için bilişim suçu olgusunun da her yönden ortaya konulması ve tanımlanması gerekmektedir (Say 2006).

Teknolojinin gelişimine bağlı olarak hayatın akışı kolaylaşırken, önemsenecek boyutlarda maddi ve manevi kayıplara neden olan bilişim suçlarının işlenme oranı ve suçtan mağdur olanların sayısı her geçen gün artış göstermektedir (Henkoğlu 2014).

Bilişim suçları temelde iki şekilde işlenebilmektedir. İlki bilişim sistemlerine karşı işlenen suçlar, diğeri ise bilişim sistemlerinin aracı olarak kullanılması suretiyle işlenen suçlardır (Aydın 1992).

Bilişim suçlarının Avrupa'daki ilk tanımı ise; Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun Mayıs 1983 yılında Paris Toplantısında "Bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanun, gayri ahlaki ve yetki dışı gerçekleştirilen her türlü davranıştır." şeklinde yapılmıştır.

Her geçen gün teknolojinin ve bu teknolojilere erişilebilirliğin artmasına paralel olarak bilişim sistemlerine yönelik işlenen suçların da artış gösterdiği belirtilen İstanbul Emniyet Müdürlüğü Siber Suçlarla Mücadele Şube Müdürlüğünün resmi internet sitesinde bilişim suçlarını, "Bir bilişim sisteminin güvenliğini, buna bağlı verileri ve kullanıcısını hedef alan ve bilişim sistemi kullanılarak işlenen suçlar" şeklinde tanımladıkları görülmektedir (İnt.Kyn.18).

Halk arasında elektronik suçlar, teknoloji suçları, bilgisayar suçları, internet suçları, dijital suçlar vb. birçok tanımlamalar şeklinde bilinen bilişim suçlarının genel kabul

görmüş İngilizce “cyber” kelimesinin karşılığı olarak “siber suçlar” olarak tercih edilmesi isabetli olacaktır (Aytekin, Kılıç ve Çakır 2014).

Siber suçlar tanımının kapsadığı geniş alan, siber suçların değişik şekil ve içeriklerde olabileceğini ve klasik suçların siber alan ile farklı biçim ve yoğunlukta temas ettiğinden (Başıbüyük ve Hekim 2013) ve uluslar arası literatürde bilişim suçları kavramı, siber suçlar olarak adlandırıldığından, çalışmanın bundan sonraki kısmında bilişim suçları yerine siber suçlar kavramı kullanılacaktır.

2.2.4 Siber Suç İşleniş Yöntemleri

Siber suçların hayatımızda yer almaya başlaması ve bizleri rahatsız etmesiyle beraber, siber suçları çeşitli yönleriyle düzenleme ve sınıflandırma gereği ortaya çıkmıştır. Ancak bilgisayar ağları alanındaki sorunların ve özellikle internetin tam olarak değerlendirilememesi, internetin sürekli gelişmesi ve her geçen gün biraz daha fazla insan hayatına girmesi, bunun sonucunda yeni suç tiplerinin ortaya çıkmasına sebep olduğundan siber suçları sınıflandırma çalışmaları farklılık arz etmektedir (Benzer 2014).

Halk arasında bu yeni tip suçları işleyen bilgisayar korsanları, “hacker” olarak adlandırılmaktadır. Siber suçların işlenebilmesi daha çok teknik bilgi gerektirdiğinden dolayı bilgisayar korsanları yazılım ve donanım bilgisi olarak ileri seviyede bilgiye sahip kişilerdir.

Hacker kelimesi ilk olarak 1960’lı yıllarda Massachusetts Institue of Technology (MIT) laboratuarlarında Fortran programlama dili ile yapılan yazılım ve sistemleri geliştiren araştırma görevlilerine verilen ad olarak kullanılmaya başlandı (Burlu 2012).

Hackerlar, internet dünyasında White Hat Hacker (Beyaz Şapkalı Hacker), Black Hat Hacker (Siyah Şapkalı Hacker) ve Grey Hat Hacker (Gri Şapkalı Hacker) olmak üzere üçe

ayrılırlar. Beyaz Şapkalı Hacker; temel amaçları bilişim teknolojileri ve sistemlerini geliştirmek ve güvenliğini sağlamak olan hacker tipidir. Güvenlik uzmanı diye de adlandırılmaktadırlar. Siyah Şapkalı Hacker; amaçları tamamen zarar vermek olan korsan diye de adlandırılan hacker türüdür. Kendi içlerinde vasıflarına göre Script Kiddies, Phreakers, Crackers vb. gruplara ayrılırlar. Gri Şapkalı Hacker; amacı sadece kazanç olan hem savunma hem de saldırı amaçlı çalışan hacker tipidir (Burlu 2012).

Yukarıda anlatılan hacker gruplarından beyaz şapkalı hackerlar, genellikle özel şirketlerde güvenlik uzmanı olarak çalışmaktadırlar ve suça karışmazlar. Gri şapkalı hackerlar için önemli olan menfaatleridir ve suça karışabilme potansiyeli vardır. Siyah şapkalı hackerlar ise, her an suç işleme potansiyeli olduğundan dolayı çok tehlikelidirler. Siber suçla mücadele eden kolluk kuvvetlerinin en sık karşılaşmış oldukları hacker tipidir. Halk arasında bilinen hacker kavramı, gri ve siyah şapkalı hackerları kapsamakta ve çalışmanın bundan sonraki kısımlarında bilgisayar korsanı olarak adlandırılacaktır.

Bilgisayar korsanı olacak kadar bilgiye sahip kullanıcılar, bu bilgilerini en kısa zamanda paraya dönüştürmeye çalışmakta ve bunun içinde önceliğin isimlerini duyurmak olduklarına inanmaktadırlar (Bilek 2012). Bu sebeple, sanal dünyada kendilerine vermiş oldukları takma isimler ile tanınırlar ve işledikleri suçlarda bu isimleri kullanmaktan kaçınmazlar.

Siber suçlar ile mücadele edebilmek için, öncelikle hackerların dilinden anlamak gerekir. Yani Hackerların kullandıkları yöntemler, suçun ortaya çıkartılmasında ve delil elde edilmesi aşamalarında çok önem arz etmektedir. Bu sebeple hackerların kullandığı yöntemleri bilmekte fayda vardır. Bu yöntemlerden en çok bilinen ve en sık karşılaşılanlar aşağıda açıklanmıştır.

2.2.4.1 Kötücül Yazılımlar (Malware)

İngilizce “malicious software” kavramının kısaltması olan “malware”, Türkçe’de kötü amaçlı yazılım olarak tanımlanmaktadır. Bilgisayar sistemlerine zarar vermek, bilgi çalmak veya kullanıcıları rahatsız etmek gibi amaçlarla hazırlanmış yazılımlara verilen genel addır. Bu yazılımlara örnek olarak virüsler, solucanlar, truva atları, rootkitler verilebilir (İnt.Kyn 19).

Bu yöntem, suçlular tarafından finansal bilgilerin çalınması ve kişisel bilgilerin ele geçirilmesi için aracı olarak kullanılmaktadır. Genellikle bilgisayarın ele geçirilmesi için aşağıda açıklanacak olan sosyal mühendislik yöntemlerinden veya sistem güvenlik açıklarından yararlanılmaktadır (Çakır ve Doğan 2014).

2.2.4.2 Sosyal Mühendislik

Bir bilişim sisteminin en zayıf halkası olarak adlandırılan insan unsuru, ağ filtreleme cihazları, antivirüs yazılımları ve tüm güvenlik sağlama sistemlerine rağmen en büyük tehlikelerden birisidir. Bu sebeple sosyal mühendislik, etkileme ve ikna etme yöntemlerini kullanarak kurbandan bilgi alma ya da istenilen işleri yapmasını sağlamaktır (Burlu 2012).

“Sosyal mühendislik saldırıları kişisel beceri ve kabiliyete dayaman, basit ama oldukça etkili saldırılardır. Sosyal mühendislik saldırılarında hedef kişi ya da kurumun yapısı, çalışanların/yöneticilerin kişisel bilgileri, şifreler ile birlikte saldırıda kullanılabilecek her türlü materyal toplanmaktadır. Elde edilen bu materyaller ile sistemlere izinsiz giriş yapılmakta, bilgiler çalınmakta, değiştirilmekte veyahut yok edilmekte, elde edilen bilgiler ile dolandırıcılık, endüstriyel casusluk ve kimlik hırsızlığı yapılmaktadır (Çakır ve Doğan 2014).”

Sosyal mühendislikte kullanılan yöntemler; bilgi toplama (fiziksel girişimler), güven

kazanma (psikolojik girişimler), güveni kötüye kullanma (bilgisayara komut gönderme ve program yüklettirme) ve saldırı yöntemidir (Çakır ve Doğan 2014). Bu yöntemlerden bilgi toplama aşamasında büyük küçük ne kadar çok bilgi toplanırsa, hedefe ulaşmak o kadar kolay olacağından dolayı sosyal mühendisliğin en önemli yöntemidir.

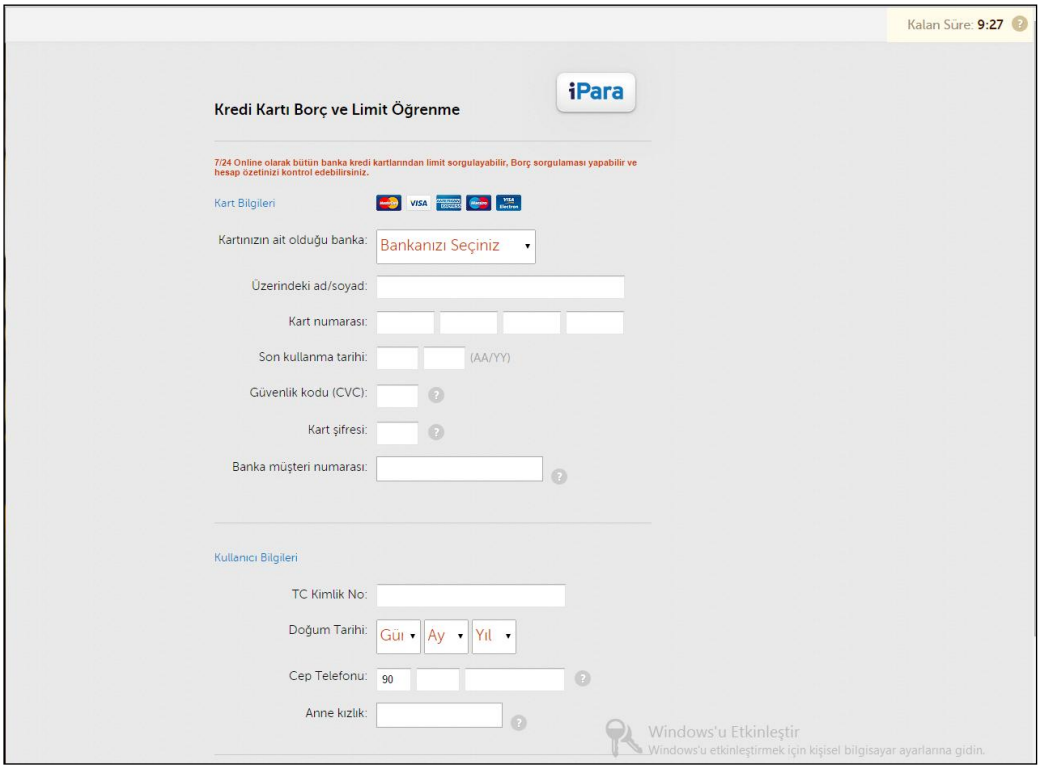
2.2.4.3 Oltalama (Fishing)

Oltalama, ingilizce password (şifre) ve fishing (balık avlamak) sözcüklerinin birleşmesiyle oluşturulmuş phishing ifadesinin Türkçe karşılığıdır. Dolandırıcılar, genelde e-posta gibi yollarla kişilere ulaşır ve onların kredi kartı gibi ayrıntılarını sanki resmi bir kurummuş gibi isterler, bu ava karşılık veren kullanıcıların hesap, şifre vb. özel bilgilerini çalmaktadırlar (İnt.Kyn.20).

Gönderilen e-postanın gerçek kuruluştan geldiğini göstermek için kuruluşa ait logo, gerçek web sayfasının birebir kopyası ve diğer sahte bilgiler kullanılabilmektedir. Diğer bir yöntemde zararlı yazılım içeren siteler yoluyla kişilerin bilgisayarlarına keylogger (tuş kaydedici), Trojan (truva atı) ve diğer casus yazılımları yükleyerek, zararlı programların kullanıcının dikkatini çekmek için isminin değiştirilip bilgisayara indirilmesi sağlanarak yapılmaktadır (Çubukçu ve Bayzan 2013).

Dolandırıcı, hazırlamış olduğu e-postaları daha önceden elinde hazır bulunan posta listelerine spam (İstem Dışı Alınan Elektronik Posta) olarak yollar. Bu postalarda banka/finans kuruluşunun sisteminde güncelleme yapılmakta olduğu ve sistemde eksik bilgilerin tamamlanması isteği belirtilir ve altına dolandırıcının daha önceden hazırladığı sitenin adresi belirli gizleme yöntemleri ile kurban aldatılacak şekilde konulur. Bu e-postaya inanan kullanıcı kendi elleri ile dolandırıcıya hesap, kredi kartı ve kişisel bilgilerini verir. Bundan sonra, dolandırıcıya sadece gelen bilgileri toplayıp bu bilgilerle maddi çıkar sağlamak kalmaktadır (Bilek 2012).

Resim 2.5'de kredi kartı borç ve limit bilgilerini öğrenmek isteyen kimselerin, dolandırıcılık amacıyla kredi kartı ve kişisel bilgilerini ele geçirmek için oluşturulmuş bir web sitesi görülmektedir. Bu tür web siteleri kısa süre yayında kalırlar ve arama motorlarında genellikle üst sıralarda çıkmak için reklam şirketlerinden faydalanırlar. Böylece arama motorlarında kredi kartı ile ilgili arama yapıldığında, arama sonuçlarının üst sıralarında çıktıklarından dolayı ziyaret edilme sayısı artacak ve çok fazla sayıda insan mağdur olması sağlanacaktır.



Resim 2.5 Sahte Web Sitesi.

2.2.4.4 Tuş Kaydediciler (Keylogger)

En temel işlevi bakımından, kullanıcının klavye kullanarak girdiği bilgileri yakalayıp, tutan ve bunları saldırgana gönderen casus yazılımlara denen keylogger, keycatcher (tuş yakalayıcı) ve screen scraper (ekran kazıyıcı) olarak da adlandırılmaktadır (Canbek 2005).

Keyloger internet üzerinde resim veya programların içerisine saklanarak kullanıcı bilgisayarına kullanıcının bilgisi dışında yüklenen programlardır. Program kullanıcının bilgisayarında aktif hale geldikten sonra klavye ile yazılan bütün bilgiler ve hatta fare ile tıklanan bölgelerin resimleri kaydedilerek rapor haline getirilir. Bu rapor bahse konu zararlı yazılımı yazan kişilerin e-posta adreslerine internet üzerinden gönderilir. Bu şekilde söz konusu yazılımı kullanıcının bilgisayarlarına bulaştırmak üzere yayan kişiler kullanıcının bilgisayarından yapılan bütün e-posta, bankacılık ve finans şifrelerini ele geçirebilmektedirler (Bilek 2012).

Keyloggerlar, bankacılık ve finans şifrelerini ele geçirebilmesinde etkin bir şekilde kullanıldığı gibi, sosyal paylaşım sitelerinde bulunan kullanıcı hesaplarının şifrelerini ele geçirmek için de çok sıklıkla kullanılmaktadır. Sosyal paylaşım hesabının şifresinin ele geçirilmesinden sonra ise, sosyal mühendislik yöntemleri kullanılarak hesapta kayıtlı olan arkadaş listesindeki kişilerle iletişime geçilmekte ve dolandırılmaya çalışılmaktadır.

2.2.4.5 Truva Atı (Trojan)

Mitolojideki truva atı nasıl bir armağan gibi görünüp, aslında Troya kentini ele geçirecek Yunan askerlerini taşıdıysa, günümüzün truva atları da bilgisayar kullanıcılarına kullanışlı ve eğlenceli gibi görünerek aslında çalıştığı sistemde önemli verilere ulaşıp, bunları dışarı gönderen casus yazılımdır (Burlu 2012).

Truva atları genellikle internetten indirilen müzik, dosya ve programlara iliştirilmiş olarak kullanıcıların bilgisayarlarına yüklenmekte veya e-posta aracılığıyla kullanıcılara ulaşmaktadır. Truva atları kullanıcıdan habersiz arka planda çalışarak internet bağlantısı sağlanması halinde dışarıya veri aktarımı yaparlar. Virüs ve solucanlardan farklı özelliği ise yayılmamalarıdır (Benzer 2014).

2.2.4.6 İstem Dışı Alınan Elektronik Postalar (Spam)

İstem dışı alınan elektronik posta olarak tabir edilen spam, internet üzerinde aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere zorlayıcı nitelikte gönderilmesine denilmektedir. Bu e-postaları gönderen kişilere ise "spammer" denilmektedir. Spammerlar oluşturdukları e-posta veritabanlarını kullanarak, ideolojik, pornografik, reklam ve her türlü ticari duyuru yapmak isteyen kişilerin, spam yardımıyla geniş kitlelere ulaşmasını sağlarlar. Spammerların e-posta elde etmek için en çok kullandıkları kaynaklar, forum siteleri, e-posta listeleri, haber grupları, tartışma grupları, yeniden iletilen e-postalar, web siteleri, sohbet odalarıdır (Benzer 2014).

Spam e-postalardan uzak kalabilmenin en iyi yolu e-posta filtresi kullanmaktır. Bu filtreler istenmeyen e-postaları kullanıcılara ulaşmadan doğrudan siler veya gereksiz e-posta kutusuna gönderirler (Bilek 2012).

2.2.4.7 Hizmet Engelleme Saldırısı (DOS Saldırısı)

DOS sistemin ya da servislerin aşırı yüklenme sebebiyle hizmet vermesi gereken kullanıcılara hizmet vermesini engellemek ya da yavaşlatmaktır. Genellikle saldırganlar bir sisteme yetkisiz giriş sağlayamazlar ise DOS saldırısı ile sisteme zarar vermeye çalışırlar (Burlu 2012).

DDOS (Distrubuted Denial of Service) ise DOS saldırısının yüzlerce, binlerce farklı sistemden yapılması şeklinde gerçekleşir. Genellikle taklit edilmiş IP adresleri ve köle bilgisayarlar kullanılır. Sistemde güvenlik açığı bulunamazsa zarar verme amaçlı politik sebeplerden ve ticari sebeplerle yapılabilir (Bilek 2012).

TC Ölçme, Seçme ve Yerleştirme Merkezinin resmi web sitesi olan www.osym.gov.tr'ye, üniversite sınav sonuçlarının açıklandığı zamanlarda erişebilmek

çok mümkün olmamaktadır. Burada da hizmet geçici bir süre engellenmekte, ancak saldırganlar tarafından bir DOS saldırısı şeklinde değil, sınav sonuçlarını öğrenmek isteyen milyon sayıdaki öğrencilerin web sitesine aynı anda giriş yapmaya çalışmaları şeklinde olmaktadır.

2.2.4.8 Diğer Yöntemler

Hackerların kullandıkları diğer yöntemler arasında Gizli Kapılar (Trap Doors), Mantık Bombaları (Logic Bombs), Salam Tekniği (Salami Techniques), Çöpe Dalma (Scavenging), Süper Darbe (Super Zapping), Eşzamansız Saldırılar (Asynchronous Attacks), Tarama (Scanning), Bukalemun (Chamelon), Sırtlama (Piggybacking) ve Yerine Geçme (Masquerading) gibi yöntemler bulunmaktadır (Benzer 2014).

3. 5237 SAYILI TÜRK CEZA KANUNUNDA SİBER SUÇLAR

Türkiye'de siber suçlar ile ilgili hukuki düzenleme TCK, İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, Elektronik İmza Kanunu (EİK), Fikir ve Sanat Eserleri Kanunu (FSEK) ve Banka Kartları ve Kredi Kartları Kanununda (BKK) yer almaktadır. Her ne kadar hukukumuzda internet kanunu olarak tabir edilse de, İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun siber suçlarla mücadele kapsamında çok büyük eksikliklerin olduğu görülmektedir.

Siber suçlar, yukarıda belirtilen kanunlardan, en kapsamlı ve uygulanabilir olarak TCK'da yer aldığı görülmektedir. Bu sebeple siber suçların mevzuattaki yeri anlatılırken daha çok 5237 Sayılı TCK üzerinde durulmuştur.

3.1 Bilişim Alanında Suçlar

Siber suçlar, TCK'nın ikinci kitabında "Topluma Karşı Suçlar" başlığını taşıyan üçüncü kısmının "Bilişim Alanında Suçlar" başlığını taşıyan onuncu bölümde düzenlenmiştir. Bilişim Alanında Suçlar başlığı altında ise, "Bilişim Sistemine Girme (Madde 243)", "Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme (Madde 244)", "Banka veya Kredi Kartlarının Kötüye Kullanılması (Madde 245)" ve "Tüzel Kişiler Hakkında Güvenlik Tedbiri Uygulanması (Madde 246)" olmak üzere dört madde şeklinde düzenlenmiştir.

26.09.2004 tarihinde kabul edilen ve 01.06.2005 tarihinde yürürlüğe giren 5237 sayılı TCK'da yer alan siber suçlar ile ilgili maddeler, 765 Sayılı TCK'daki gibi benzer yaklaşımda, ancak daha ayrıntılı şekilde ve ağırlıklı olarak yer almaktadır (Karagülmez 2011).

5237 Sayılı TCK'dan önce hukukumuzda siber suçlara ilk olarak, 1989 tarihli TCK Ön Tasarısında rastlanılmış, ancak 765 Sayılı TCK'da bilişim alanında suçları düzenleyen 525/a ile 525/d arasındaki madde metinlerinde bilişim kavramı, doğrudan belirtilmemekle birlikte ilgili maddelerin yer aldığı 11. bölüm isminde "Bilişim Alanında Suçlar" başlığıyla yer almıştır (Taşkın 2008).

3.1.1 Bilişim Sistemine Girme

Bilişim sistemlerine karşı suçların düzenlendiği bölümde yer alan 243. maddede bilişim sistemine girme fiili suç olarak tanımlanmış ve madde metninde "(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir. (2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir. (3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur." hükmüne yer verilmiştir.

Madde gerekçesinde, suçun oluşması için sisteme, doğal olarak, haksız ve kasten girilmiş olması yeterli görülmüş, suçun bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi, bu suç açısından daha az ceza ile cezalandırılmayı gerektirdiği belirtilmiş ve suçun işlenmesi nedeniyle sistemin içerdiği verilerin yok olması veya değişmesi halinde failin, suçun temel şekline nazaran daha ağır ceza ile cezalandırılması öngörülmektedir.

"Erdoğan (2010), bilişim suçlarının işlenebilmesi için öncelikle bilişim sistemine girmek gerektiğinden yetkisiz girişlerin suç olarak TCK'nın 243. maddesinde düzenlenmesinin son derece yerinde olduğunu belirtmiştir (Aytekin vd. 2014)."

3.1.2 Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme

Sistemi engelleme, bozma, verileri yok etme veya değiştirmenin suç olarak tanımlandığı 244. madde metninde, "(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır. (2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır. (3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır. (4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur." hükmüne yer verilmiştir.

Madde gerekçesinde, bilişim sisteminin işleyişini engelleme, bozma, sisteme hukuka aykırı olarak veri yerleştirme, var olan verileri başka bir yere gönderme, erişilmez kılma, değiştirme ve yok etme fiilleri suç olarak tanımlanmış, bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi hakkında işlenmesi halinde, verilecek cezanın artırılması öngörülmüş ve suç olarak tanımlanan fiillerin işlenmesi suretiyle kişinin kendisine veya başkasına yarar sağlaması ceza yaptırımına bağlanmıştır. Ancak cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerektiğini, aksi halde fiilin örneğin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturması halinde ise, cezaya hükmedilmeyeceği belirtilmiştir.

3.1.3 Banka veya Kredi Kartlarının Kötüye Kullanılması

Banka veya kredi kartlarının kötüye kullanılması suçunun tanımlandığı 245. madde metninde, "(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi

gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır. (2) Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adli para cezası ile cezalandırılır. (3) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır. (4) Birinci fıkrada yer alan suçun; haklarında ayrılık kararı verilmemiş eşlerden birinin, üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlatlığın, aynı konutta beraber yaşayan kardeşlerden birinin, zararına olarak işlenmesi halinde, ilgili akraba hakkında cezaya hükmolunmaz. (5) Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır." hükmüne yer verilmiştir.

Madde gerekçesinde, maddenin düzenlenme amacının banka veya kredi kartlarının hukuka aykırı olarak kullanılması suretiyle bankaların veya kredi sahiplerinin zarara sokulmasını, bu yolla çıkar sağlanmasını önlemek ve failleri cezalandırmak olduğu belirtilmiştir. Ayrıca, başkasına ait bir banka veya kredi kartının, ne şekilde olursa olsun ele geçirilmesinden sonra, sahibinin rızası dışında kullanılması veya kullandırılması ve bu şekilde failin kendisine veya başkasına haksız yarar sağlaması ile sahibine verilmesi gereken bir banka veya kredi kartının bunu elinde bulunduran kimse tarafından kullanılması veya kullandırılması madde kapsamında suç olarak değerlendirildiği görülmektedir. Suçun, oluşturulmuş sahte bir banka veya kredi kartını kullanmak suretiyle işlenmesi, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması halinde, daha ağır ceza ile cezalandırılmayı gerektirdiği, aksi halde cezaya hükmedilmeyeceği belirtilmiştir.

3.1.4 Tüzel Kişiler Hakkında Güvenlik Tedbiri Uygulanması

Tüzel kişiler hakkındaki düzenlemeye yer verilen 246. madde metninde, “Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.” hükmüne yer verilmiştir.

Madde gerekçesinde ise, bilişim alanında suçlar bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında da bunlara özgü güvenlik tedbirlerine hükmolunacağı düzenlenmiştir.

3.2 Bilişim Sistemi Kullanılmak Suretiyle İşlenen Suçlar

Teknolojinin gelişmesi klasik suç olarak tabir edilen suç türlerinin internet, bilgisayar ya da bilişim sistemleri kullanılarak işlenmesinde artış göstermektedir. İnsanoğlu, konusu suç oluşturan ya da oluşturmayan, sosyal hayatta gerçekleştiremediği hareketleri sanal dünyada gerçekleştirebilmektedir. Hatta sanal ortamda çaba sarf etmesine gerek kalmaksızın kolaylıkla suç işleyebilmekte ve hatta kendisini gizleyerek çoğu zaman farklı kimliklere bürünebilmektedirler.

Çalışmanın bu kısmında TCK’nın doğrudan bilişim alanında suçlar bölümünde yer almayan ancak, suç soruşturması aşamasında dijital delil haricinde başka bir delil elde etme imkânı olmayan ve dolaylı olarak bilişim sistemlerinin kullanıldığı suçlar anlatılmıştır.

3.2.1 Cinsel Dokunulmazlığa Karşı Suçlar

3.2.1.1 Çocukların Cinsel İstismarı

Çocukların cinsel istismarı suçu 103. maddede açıklanmış ve maddenin birinci fıkrasında, çocuğu cinsel yönden istismar eden kişinin, sekiz yıldan on beş yıla kadar

hapis cezası ile cezalandırılacağı, cinsel istismar deyiminden; on beş yaşını tamamlamamış veya tamamlamış olmakla birlikte fiilin hukuki anlam ve sonuçlarını algılama yeteneği gelişmemiş olan çocuklara karşı gerçekleştirilen her türlü cinsel davranış, diğer çocuklara karşı sadece cebir, tehdit, hile veya iradeyi etkileyen başka bir nedene dayalı olarak gerçekleştirilen cinsel davranışların anlaşılacağı hükmüne yer verilmiştir.

Madde gerekçesinde, on beş yaşını tamamlamamış veya tamamlamış olmakla birlikte maruz kaldığı fiilin hukuki anlam ve sonuçlarını algılama yeteneği gelişmemiş olan kişilere karşı gerçekleştirilen her türlü cinsel davranış, cinsel istismar olarak kabul edilmektedir. Aynı fiilin erişkin kişilere karşı işlenmesi halinde suçun tanımlamasında cinsel saldırı ifadesi kullanılmaktadır.

3.2.1.2 Cinsel Taciz

Cinsel taciz suçu 105. maddede açıklanmış ve madde metninde, bir kimseyi cinsel amaçlı olarak taciz eden kişinin, mağdurun şikayeti üzerine, üç aydan iki yıla kadar hapis cezası veya adli para cezası, fiilin çocuğa karşı işlenmesi halinde altı aydan üç yıla kadar hapis cezası ile cezalandırılacağı, suçun; posta veya elektronik haberleşme araçlarının sağladığı kolaylıktan faydalanmak suretiyle işlenmesi halinde verilecek cezanın yarı oranında artırılacağı hükmüne yer verilmiştir.

Madde gerekçesinde, cinsel yönden ahlak temizliğine aykırı olarak mağdurun rahatsız edilmesinden ibaret davranış olarak tanımlanan cinsel taciz, kişinin vücut dokunulmazlığının ihlali niteliği taşımayan cinsel davranışlarla gerçekleştirilebildiği ve suçun soruşturulması ve kovuşturulmasının mağdurun şikayetine bağlı tutulduğu belirtilmektedir.

Örneğin; mağdur kadının internet üzerindeki bir sosyal paylaşım sitesinde bulunan hesabına, fail tarafından ahlaka aykırı olan cinsel içerikli resim göndermesi, bu suçun

bilişim sistemleri kullanılmak suretiyle işlenmesidir.

3.2.2 Hürriyete Karşı Suçlar

3.2.2.1 Tehdit

Tehdit suçu 106. maddede açıklanmış ve maddenin birinci fıkrasında, bir başkasını, kendisinin veya yakınının hayatına, vücut veya cinsel dokunulmazlığına yönelik bir saldırı gerçekleştireceğinden bahisle tehdit eden kişinin, altı aydan iki yıla kadar hapis cezası ile cezalandırılacağı hükmüne yer verilmiştir.

Madde gerekçesinde, kişinin hayatının veya vücut bütünlüğünün tehlikeye maruz bırakılacağının, suç teşkil eden belli bir fiilin işleneceğinin, genel olarak kuvvet kullanılacağının veya herhangi bir kötülüğün, haksızlığın gerçekleştirileceğinin bildirilmesi tehdidin konusunu oluşturduğu belirtilmektedir.

Tehdit suçu, fail ile mağdurun yüz yüze geldiği zamanlarda ya da mağdura imzasız mektup gönderilmesi şeklinde işlenebileceği gibi son zamanlarda çok sıklıkla karşılaşılan işlenme şekli, internetin araç olarak kullanılmasıdır. Bu şekilde, fail imzasız mektup gönderilmesi mantığında yatan kendisini gizleme yöntemini daha rahat yapmakta, hatta çoğu zaman failin tespiti mümkün olmamaktadır. Bu da tehdit suçunu işleyen faillerin bu yöntemi tercih etmelerine sebep olmaktadır.

3.2.2.2 Şantaj

Şantaj suçu 107. maddede açıklanmış ve maddenin ikinci fıkrasında, bir kişinin şeref veya saygınlığına zarar verecek nitelikteki hususların açıklanacağı veya isnat edileceği tehdidinde bulunulması halinde bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılacağı hükmüne yer verilmiştir.

Madde gerekçesinde şantaj suçunun oluşabilmesi için, mağdurun zorlanmasının yeterli olacağı, zorlama karşısında mağdurun isteneni yapması suçun oluşması için gerekli olmadığı belirtilmiştir.

Örneğin; fail erkeğin mağdur kadın ile birlikteliklerinde yaşadıkları özel bilgileri herhangi bir şeyi yaptırmaya zorlaması ya da bu bilgileri ailesi ile paylaşmaması karşılığında para talep etmek suretiyle haksız menfaat elde etmek istemesi, şantaj suçunun bilişim sistemleri kullanılmak suretiyle işlenmesidir.

3.2.2.3 Haberleşmenin Engellenmesi

Haberleşmenin engellenmesi suçu 124. maddede açıklanmış ve madde metninde, kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmesi halinde, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılacağı, her türlü basın ve yayın organının yayınının hukuka aykırı bir şekilde engellenmesi halinde ise, bir yıldan beş yıla kadar hapis cezası ile cezalandırılacağı hükmüne yer verilmiştir.

Madde gerekçesinde, haberleşmenin yapıldığı araç önemli olmaksızın, kişiler arasındaki haberleşmenin telefon hatlarının kesilmesi ve oluşturulan manyetik alanla telefon görüşmelerinin yapılamaz hale getirilmesi gibi fiiller ile engellenmesinin suçun konusunu oluşturduğu belirtilmiştir. Ayrıca her türlü basın ve yayın organının yayınının hukuka aykırı bir şekilde engellenmesi ayrı bir suç olarak tanımlanmıştır.

Örneğin; anayasa ve kanunlarda belirlenen koşullara uygun olarak, koruma veya güvenlik tedbiri uygulanması dışında, hukuka aykırı olarak bir bölgede oluşturulan manyetik alanla (jammer) telefon görüşmelerinin yapılmasının engellenmesi ya da ulusal veya yerel bir radyo şirketine tahsisli radyo frekansının, özel cihazlar kullanılmak suretiyle yerine geçilmesi ve reklam amaçlı yayınlar yapılarak haksız kazanç elde edilmesi, haberleşmenin engellenmesi suçunun bilişim sistemleri kullanılmak suretiyle işlenmesidir.

3.2.3 Şerefe Karşı Suçlar

3.2.3.1 Hakaret

Hakaret suçu 125. maddede açıklanmış ve madde metninde, bir kimseye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat eden kişinin, üç aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılacağı, fiilin sesli, yazılı veya görüntülü bir iletiyle işlenmesi halinde ise, aynı ceza ile cezalandırılacağı hükmüne yer verilmiştir.

Madde gerekçesinde, kişiye somut bir fiil veya olgu isnat edilmesi neticesinde hakaret suçunun oluştuğu ve hakaretin mağduru muhatap alan sesli, yazılı veya görüntülü bir mesajla yapılmasının huzurda hakaret olarak cezalandırılması gerektiği belirtilmiştir.

Örneğin; İnternet üzerinden yayın yapan bir internet gazetesinde yayınlanan haberin altına, haberde muhatap alınan şahıs hakkında hakaret içerikli yorum yapılması, her ne kadar madde metninde sesli, yazılı veya görüntülü bir iletiyle işlenmesi olarak tanımlansa da, bu olay hakaret suçunun bilişim sistemleri kullanılmak suretiyle işlenmesidir.

3.2.4 Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar

3.2.4.1 Haberleşmenin Gizliliğini İhlal

Haberleşmenin gizliliğini ihlal suçu 132. maddede açıklanmış ve madde metninde, kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimsenin, bir yıldan üç yıla kadar hapis cezası ile cezalandırılacağı, haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, verilecek cezanın bir kat artırılacağı, kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimsenin, iki yıldan beş yıla kadar hapis cezası ile cezalandırılacağı, kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası

olmaksızın hukuka aykırı olarak alenen ifşa eden kişinin, bir yıldan üç yıla kadar hapis cezası ile cezalandırılacağı hükmüne yer verilmiştir.

Madde gerekçesinde, kişiler arasındaki haberleşmenin ne suretle yapıldığının suçun oluşumu açısından önemi olmaksızın belirli kişiler arasındaki haberleşmenin içeriğinin öğrenilmesiyle işlenmekte olduğu ve söz konusu suçun, bu haberleşmenin tarafı olmayan kişi ya da kişiler tarafından da işlenebileceği belirtilmiştir. Ayrıca haberleşmenin gizliliğinin sadece dinlemek veya okumak suretiyle ihlal edilmesi, suçun temel şeklini oluşturduğu ancak, gizlilik ihlalinin haberleşme içeriklerinin kayda alınması suretiyle yapılmasının ise, haberleşmenin gizliliğini ihlal suçunun nitelikli şekli olarak tanımlandığı belirtilmiştir.

Haberleşmenin gizliliği Anayasa'nın 22. maddesi ile güvence altına alınmış ve kişiler arasındaki haberleşmeye müdahale edilmesi, ancak Anayasa'nın ilgili hükmü çerçevesinde, kanunlarla düzenlenen şekilde ve yetkili mahkeme kararı ile mümkün olmaktadır (Benzer 2014).

Kişiler arasındaki yazılı ya da sözlü haberleşme içeriklerinin, kanunların belirlediği koşullar dışında öğrenilmesi, dinlenilmesi veya kayda alınması bu suçu oluşturmaktadır. Bu suça konu fiilin gerçekleştirilebilmesi için ise, çoğu zaman bir bilişim sisteminden faydalanılması gerekmektedir. Haberleşmenin gizliliğini ihlal suçunun işlenmesi esnasında herhangi bir bilişim sistemi ya da bilgisayar yazılımı veya donanımının kullanılması, bu suçun bilişim sistemleri kullanılmak suretiyle işlenmesidir. Ayrıca, hukuka uygun olarak kayda alınmış bir haberleşme içeriğinin internet vasıtası ile çok büyük bir kitleye ifşa edilmesi, yine bu suçun bilişim sistemleri kullanılmak suretiyle işlenmesine girmektedir.

3.2.4.2 Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması

Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçu 133. maddede

açıklanmış ve madde metninde, kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişinin, iki yıldan beş yıla kadar hapis cezası ile cezalandırılacağı, katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişinin, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılacağı, kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişinin ise, iki yıldan beş yıla kadar hapis ve dört bin güne kadar adli para cezası ile cezalandırılacağı hükmüne yer verilmiştir.

Madde gerekçesinde, konuşmanın yapıldığı yerin önemi olmaksızın bir arada bulunan kişiler arasında yapılan konuşmanın aleni olmayan konuşma olarak kabul edildiği ve aleni olmayan konuşmanın bir aletle dinlenmesi veya bir ses alma cihazı ile kayda alınmasının, söyleşiye katılan kişilerden biri tarafından diğerlerinin rızası olmadan kayda alınmasının ve tanımlanan suçların işlenmesi suretiyle elde edildiği bilinen bilgilerden yarar sağlanması veya bunlardan diğer kişilerin bilgi edinmelerinin sağlanmasının bu suçu oluşturduğu belirtilmektedir.

Örneğin; kişiler arasında yapılan aleni olmayan görüşmelerin, taraflardan herhangi birisinin kullanmakta olduğu akıllı telefonuna bilgisi ve rızası dışında zararlı yazılım yüklenmesi vasıtasıyla, konuşmaya taraf olmayan üçüncü şahıs ya da şahıslar tarafından dinlenmesi, kayda alınması ve ifşa edilmesi, kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçunun bilişim sistemleri kullanılmak suretiyle işlenmesidir. Bu suçun madde metni ve gerekçesi incelendiğinde de, suça konu fiillerin gerçekleştirilebilmesi için, bilişim sistemlerinin kullanılmasının dışında başka bir yöntemin bulunmadığı muhakkaktır.

3.2.4.3 Özel Hayatın Gizliliğini İhlal

Özel hayatın gizliliğini ihlal suçu 134. maddede açıklanmış ve madde metninde, kişilerin

özel hayatının gizliliğini ihlal eden kimsenin, bir yıldan üç yıla kadar hapis cezası ile cezalandırılacağı, gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek cezanın bir kat artırılacağı, kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimsenin ise, iki yıldan beş yıla kadar hapis cezası ile cezalandırılacağı hükmüne yer verilmiştir.

Madde gerekçesinde, gizli yaşam alanına girerek veya başka suretle başkaları tarafından görülmesi mümkün olmayan bir özel yaşam olayının saptanması ve kaydedilmesi ile kişinin özel hayatına ilişkin görüntü veya seslerin hukuka aykırı olarak ifşa edilmesinin suç olarak tanımlandığı belirtilmiştir. Ayrıca, elde edilen saptama ve kayıtlardan herhangi bir suretle yarar sağlanması veya bunların başkalarına verilmesi veya diğer kimselerin bilgi edinmelerinin sağlanması veya basın ve yayın yoluyla açıklanmasının suçun ağırlaşmış şeklini oluşturduğu belirtilmiştir.

Örneğin; 04.12.2004 tarihinde kabul edilen 5271 Sayılı Ceza Muhakemesi Kanununun Genel Hükümler başlıklı Birinci Kitabının, Koruma Tedbirleri başlıklı Dördüncü Kısmının, Gizli Soruşturmacı ve Teknik Araçlarla İzleme başlıklı Altıncı Bölümünde yer alan Teknik Araçlarla İzleme başlığı altında bulunan 140. Maddesinin 5. fıkrasında Teknik Araçla İzleme madde hükümlerinin kişinin konutunda uygulanamayacağı hükmü bulunduğu halde, bir kolluk kuvvetinin soruşturma kapsamında takip ettiği şüphelinin konutunu, konutun içerisinde olan hareketleri görecek şekilde görüntü alması veya konut içerisinde konuşulanları teknik cihazlar marifetiyle dinlemesi ve kayda alması, bu suçu oluşturacaktır. Özel hayatı ihlal edilen şahıs hakkında herhangi bir soruşturmanın varlığı bu suçun işlenmediği anlamına gelmemektedir.

Aynı şekilde failin ikametinde bulunan kamera vasıtası ile karşı komşusunun penceresini yakınlaştırmak suretiyle konutun içerisinde olan hareketleri izlemesi ve kayda alması bu suçu oluşturacaktır. Özel hayatın gizliliğini ihlal suçunda bilişim sistemlerinin araç olarak kullanılması, daha çok bu suçun ifşa edilmesinde karşılaşılmaktadır.

3.2.4.4 Kişisel Verilerin Kaydedilmesi

Kişisel verilerin kaydedilmesi suçu 135. maddede açıklanmış ve madde metninde, hukuka aykırı olarak kişisel verileri kaydeden kimsenin bir yıldan üç yıla kadar hapis cezası ile cezalandırılacağı, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimsenin ise, yukarıdaki fıkra hükmüne göre cezalandırılacağı hükmüne yer verilmiştir.

Madde gerekçesinde, suçun oluşabilmesi için kişisel verilerin hukuka aykırı bir şekilde kayda alınmasının gerektiği vurgulanmış, kişisel verilerin bilgisayar ortamında veya kağıt üzerinde kayda alınması arasında herhangi bir ayırımın gözetilmediği ve söz konusu suç tanımı ile Avrupa Konseyi bünyesinde hazırlanan Türkiye'nin de 28 Ocak 1981 tarihinde imzalayarak taraf olduğu "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme"nin ilgili hükümlerine geçerlilik tanındığı belirtilmiştir.

Şirketlerin avantajlarından ve kampanyalarından yararlanmak amacıyla kişilerin kendi rızaları ile vermiş oldukları kişisel bilgiler elbette ki suç oluşturmamaktadır. Ancak bu toplanan kişisel bilgilerin üçüncü şirketlere haksız kazanç elde etmek amacıyla satılması kişisel verilerin kaydedilmesi suçunu oluşturacaktır. Örnek verecek olursak, bankalardan, finans kuruluşlarından ve telekomünikasyon şirketlerinden elde edilen kişisel bilgilerin, genellikle dolandırıcılık amacıyla kurulan üçüncü şirketlere aktarılması neticesinde, bu bilgileri kullanan dolandırıcılar insanları tuzaklarına düşürmekte ve çok büyük maddi zararlara neden olmaktadırlar. Günümüzde çok sık rastlanılan dolandırıcılık yöntemi olan telefon dolandırıcıları, aradıkları kişilerin daha önceden temin etmiş oldukları kişisel bilgileriyle ve kendilerini hakim, savcı, polis vb. gibi tanıtarak ikna etmekte ve insanları dolandırmaktadırlar. Burada oluşan suç her ne kadar dolandırıcılık suçu olmuş olsa da, suçun oluşumunda en önemli etken olarak bulunan kişisel verilerin kaydedilmesi suçundan da ayrıca soruşturma yürütülmesi

gerekmektedir.

3.2.4.5 Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme

Verileri hukuka aykırı olarak verme veya ele geçirme suçu 136. maddede açıklanmış ve madde metninde, kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişinin, iki yıldan dört yıla kadar hapis cezası ile cezalandırılacağı hükmüne yer verilmiştir.

Madde gerekçesinde, hukuka uygun olarak kaydedilmiş olsun veya olmasın, kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmenin, bağımsız bir suç olduğu belirtilmiştir.

Verileri hukuka aykırı olarak verme veya ele geçirme suçu, kanun koyucular tarafından her ne kadar bağımsız bir suç olarak tanımlansa da kişisel verilerin kaydedilmesi suçu ile ilintilidir. Yani bu suçun oluşabilmesi için, öncelikle kişisel verilerin kaydedilmesi suçunun oluşması gerekmektedir. Yani yukarıda verilen dolandırıcılık suçu ile ilgili örnek bu suç içinde verilebilir.

3.2.4.6 Verileri Yok Etmeme

Verileri yok etmeme suçu 138. maddede açıklanmış ve madde metninde, kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası ile cezalandırılacağı hükmüne yer verilmiştir.

Madde gerekçesinde, hukuka uygun olarak kaydedilmiş olan kişisel verilerin kanunların belirlediği sürelerin geçmiş olmasına rağmen yok edilmemesi, Verileri hukuka aykırı olarak verme veya ele geçirme suçu gibi bağımsız bir suç olarak tanımlandığı belirtilmiştir.

3.2.5 Malvarlığına Karşı Suçlar

3.2.5.1 Nitelikli Hırsızlık

Bilişim sistemleri kullanılmak suretiyle hırsızlık suçu nitelikli hırsızlık suçunun tanımlandığı 142. maddenin 2. fıkrasının e bendinde yer almaktadır. Madde metninde hırsızlık suçunun bilişim sistemlerinin kullanılması suretiyle işlenmesi halinde, beş yıldan on yıla kadar hapis cezasına hükmolunacağı hükmüne yer verilmiştir.

Madde gerekçesinde, hırsızlık suçunun bilişim sistemlerinin kullanılması suretiyle işlenmesi, daha ağır ceza ile cezalandırılmayı gerektiren bir nitelikli unsur oluşturduğu belirtilmiştir.

Bilişim sistemlerinin kullanılması suretiyle işlenen hırsızlık suçuna örnek verecek olursak, genellikle lise çağındaki çocukların online olarak oynadıkları Metin2, Knight Online, Wolfteam vb. oyunlardaki sanal karakterlerinin ve bu karakterlere ait eşyaların çalınması bu suç kapsamında değerlendirilmektedir. Her ne kadar sanal bir karakter ve eşya da olsa, internet üzerinde bunlarında satışı yapıldığından bir değeri bulunmaktadır.

3.2.5.2 Nitelikli Dolandırıcılık

Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle dolandırıcılık suçu nitelikli dolandırıcılık suçunun tanımlandığı 158. maddenin 1. fıkrasının f bendinde yer almaktadır. Madde metninde dolandırıcılık suçunun bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi halinde, iki yıldan yedi yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılacağı hükmüne yer verilmiştir. Ancak 03.04.2013 tarihinde yapılan değişiklikte, hapis cezasının alt sınırı üç yıldan, adli para cezasının miktarı suçtan elde edilen menfaatin iki katından az olamayacağı şeklinde düzenleme yapılmıştır.

Madde gerekçesinde, dolandırıcılık suçunun, bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesinin, bu suçun nitelikli unsuru olarak kabul edildiği ve bilişim sistemlerinin ya da birer güven kurumu olan banka veya kredi kurumlarının araç olarak kullanılmasının, dolandırıcılık suçunun işlenmesi açısından önemli bir kolaylık sağladığı belirtilmiştir.

3.2.6 Genel Ahlaka Karşı Suçlar

3.2.6.1 Müstehcenlik

Müstehcenlik suçu 226. maddede açıklanmış ve madde metninde, müstehcenlik ile birlikte çocukların bu tür zararlı yayınlara karşı korunmasına yönelik hükümler yer almaktadır. Maddenin 2. fıkrasında müstehcen görüntü, yazı veya sözleri basın ve yayın yolu ile yayınlayan veya yayınlanmasına aracılık eden kişinin altı aydan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılacağı hükmüne yer verilerek müstehcen görüntü, yazı veya sözlerin basın ve yayın yolu ile yayınlanması veya yayınlanmasına aracılık edilmesi, ayrı bir suç olarak tanımlanmıştır.

Müstehcen görüntülerin üretilmesinde çocukların kullanılması veya hayvan ve ölmüş insan bedeninin konu olması durumu, ilgili maddenin 3. ve 4. fıkrasında düzenlenmiş ve basın yayın organı ile yayınlanması veya yayınlanmasına aracılık edilmesi durumunda altı yıldan on yıla kadar hapis veya beş bin güne kadar adli para cezası ile cezalandırılması ön görülmektedir (Aytekin vd. 2014).

Müstehcenlik maddesinin 3. fıkrasında düzenlenen çocuk pornografisi, genel anlamda cinsiyet ayrımı olmaksızın 15 yaş altındaki kız ve erkek çocukların cinsel istismarını içeren film, video ve resim gibi görüntülerden oluşan, uluslar arası olarak da yasaklanmış olan zararlı pornografi türüdür. Bu tür görüntülerin çekilmesi, üretilmesi, indirilmesi, dağıtılması ve paylaşılması suç olup, Türkiye açısından ise, yaş sınırı 18'dir (Benzer 2014).

3.2.6.2 Fuhuş

Fuhuş suçu 227. maddede tanımlanmış ve maddenin 2. fıkrasında bir kimseyi fuhşa teşvik eden, bunun yolunu kolaylaştıran ya da fuhuş için aracılık eden veya yer temin eden kişinin, iki yıldan dört yıla kadar hapis ve üçbin güne kadar adli para cezası ile cezalandırılacağı hükmüne yer verilmiştir.

Madde gerekçesinde, bir kimseyi fuhşa teşvik etmek, bunun yolunu kolaylaştırmak ya da fuhuş için aracılık etmek veya yer temin etmenin ayrı bir suç oluşturduğu, fuhşa sürüklenen kişinin kazancından yararlanılarak kısmen veya tamamen geçimin sağlanmasının, fuhşa teşvik sayılacağı belirtilmiştir.

Bilindiği üzere internette yayın yapan çok sayıda müstehcen içerikli web sitesi olduğu kadar, fuhuş amacıyla kurulmuş web siteleri de oldukça fazladır. Bunun en önemli sebebi ise, fuhuş suçunu oluşturan unsurlardan teşvik, yolunu kolaylaştırmak, aracılık ve yer temin etmek gibi etkenlerin internet ortamı üzerinden daha kolay sağlanmasıdır. Sosyal medyanın gün geçtikçe kullanılma oranının artması sebebiyle de, fuhuş artık her ortamda çok kolay işlenebilen bir suç haline gelmiştir. Kaldı ki sosyal paylaşım siteleri üzerinde sahte bilgiler ile açılan hesaplar fuhuş için oldukça kolaylık sağlamaktadır.

3.2.6.3 Kumar

Fuhuş suçu 228. maddede tanımlanmış ve maddenin metninde kumar oynanması için yer ve imkan sağlayan kişinin, bir yıla kadar hapis ve adli para cezası ile cezalandırılacağı hükmüne yer verilmiştir.

Madde gerekçesinde, suçun başkalarının kumar oynaması için yer veya başka surette imkan sağlamakla oluştuğu, bir oyunun kumar sayılması için, oyunun kazanç kastı ile icra edilmesi ve kar ve zararın talihe bağlı olması koşullarının arandığı ve kazanç kastı

olmaksızın, dostlar arasında eğlenmek üzere oyun oynanmasına imkan sağlanmasının bu suçu oluşturmadığı belirtilmiştir.

İnternet ortamı fuhuş suçunun işlenmesinde kolaylık sağladığı gibi, aynı kolaylık kumar suçu için de geçerlidir. Kumar Türkiye'de suç olarak tanımlandığından dolayı internet üzerinden yayın yapan kumar siteleri genellikle yurtdışından yayın yapmaktadır.

3.2.7 Diğer Suçlar

TCK'nın geneli incelendiğinde yukarıda açıklanan suç tanımlamalarının dışında aşağıda açıklanan suç türleri doğrudan bilişim sistemleri kullanılmak suretiyle kullanılması suretiyle işlenmese bile internet, bilgisayar, bilişim sistemi vb. araçlarla ilintili olarak işlenebilmektedir. Dolayısıyla, geleneksel ya da klasik suç olarak tabir edilen suçların çok büyük bir kısmında, bilişim sistemleri doğrudan olmasa da dolaylı bir şekilde kullanılmasının mümkün olduğu görülmektedir. Bir sonraki bölümde anlatılacak olan adli bilişim teknolojilerinin, neredeyse tüm suç türlerinde suçlara ilişkin delil elde edilebilmesi için kullanılmasını gerektirecek bir zorunluluk haline gelecektir.

Bilişim sistemlerinin dolaylı bir şekilde kullanıldığı suç türlerinin bazıları aşağıda gösterilmiştir.

- Devlet Sırlarına Karşı Suçlar ve Casusluk bölümünde yer alan maddeler
- Ticari Sır, Bankacılık Sırrı veya Müşteri Sırrı Niteliğindeki Bilgi veya Belgelerin Açıklanması
- İntihara Yönlendirme
- İftira
- Güveni Kötüye Kullanma
- Uyuşturucu veya Uyarıcı Madde İmal ve Ticareti
- Sağlık İçin Tehlikeli Madde Temini
- Organ veya Doku Ticareti
- Parada Sahtecilik

- Resmi Belgede Sahtecilik
- Mühürde Sahtecilik
- Özel Belgede Sahtecilik
- İhaleye Fesat Karıştırma

3.3 Diğer Kanunlarda Siber Suçlar

Bilişim sistemleri kullanılarak işlenen suçların TCK dışında hangi kanunlarda bulunup bulunmadığı incelendiğinde, EİK, FSEK ve BKK'da yer alan bazı maddelerde yer aldığı görülmüş ve aşağıda kanun maddelerinden bahsedilmiştir.

3.3.1 Elektronik İmza Kanununda Siber Suçlar

Bilgisayar ve internetin sosyal ve ekonomik yaşama girmesi ile birlikte, elektronik imzanın çeşitli alanlarda kullanılır olması sonucu çıkartılan EİK'da, elektronik imzanın hukuka aykırı kullanılması ceza yaptırımlarına bağlanmıştır. Bu suç türlerinin bilişim sistemleri olmaksızın işlenmesinin mümkün olmayacağından dolayı, siber suç olarak tanımlanması doğru olacaktır.

3.3.1.1 İmza Oluşturma Verilerinin İzinsiz Kullanımı

İmza oluşturma verilerinin izinsiz kullanımı 16. maddede suç olarak tanımlanmış ve ceza yaptırımına bağlanmıştır. Madde metninde, elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanların bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adli para cezasıyla cezalandırılacağı hükmüne yer verilmiştir.

3.3.1.2 Elektronik Sertifikalarda Sahtekarlık

Elektronik sertifikalarda sahtekarlık 17. maddede suç olarak tanımlanmış ve ceza yaptırımına bağlanmıştır. Madde metninde, tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler ile bu elektronik sertifikaları bilerek kullananlar, iki yıldan beş yıla kadar hapis ve yüz günden az olmamak üzere adli para cezasıyla cezalandırılacağı hükmüne yer verilmiştir.

3.3.2 Fikir ve Sanat Eserleri Kanununda Siber Suçlar

3.3.2.1 Manevi, Mali veya Bağlantılı Haklara Tecavüz

Manevi, mali veya bağlantılı haklara tecavüz başlıklı 71. madde metninde bir eseri, icrayı, fonogramı veya yapımı hak sahibi kişilerin yazılı izni olmaksızın işleyen, temsil eden, çoğaltan, değiştiren, dağıtan, her türlü işaret, ses veya görüntü nakline yarayan araçlarla umuma ileten, yayımlayan ya da hukuka aykırı olarak işlenen veya çoğaltılan eserleri satışa arz eden, satan, kiralamak veya ödünç vermek suretiyle ya da sair şekilde yayan, ticari amaçla satın alan, ithal veya ihraç eden, kişisel kullanım amacı dışında elinde bulunduran ya da depolayan kişinin hakkında bir yıldan beş yıla kadar hapis veya adli para cezası ile cezalandırılacağı hükmüne yer verilmiştir.

3.3.2.2 Koruyucu Programları Etkisiz Kılmaya Yönelik Hazırlık Hareketleri

Koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri başlıklı 72. madde metninde, bir bilgisayar programının hukuka aykırı olarak çoğaltılmasının önüne geçmek amacıyla oluşturulmuş ilave programları etkisiz kılmaya yönelik program veya teknik donanımları üreten, satışa arz eden, satan veya kişisel kullanım amacı dışında elinde bulunduran kişinin altı aydan iki yıla kadar hapis cezasıyla cezalandırılacağı hükmüne yer verilmiştir.

3.3.3 Banka Kartları ve Kredi Kartları Kanunu Kapsamında Siber Suçlar

3.3.3.1 Bilgilerin Saklanması

Bilgilerin saklanması başlıklı 23. madde metninde, "Üye işyerleri, kartın kullanımı sonucunda kart ve kart hamili ile ilgili edindikleri bilgileri, kanunla yetkili kılınan kişi, kurum ve kuruluşlar hariç olmak üzere kart hamilinin yazılı rızasını almadan başkasına açıklayamaz, saklayamaz ve kopyalayamaz. Üye işyerleri, kart bilgilerini üye işyeri anlaşması yaptığı kuruluş dışındaki şahıs veya kuruluşlarla paylaşamaz, satamaz, satın alamaz ve takas edemez. Üye işyeri anlaşması yapan kuruluşlar, bu fıkranın uygulanmasını gözetmekle yükümlüdür. Kart çıkaran kuruluşlar, edindikleri kişisel bilgileri gizli tutmak, kendi hizmetlerinin pazarlanması dışında başka amaçlarla kullanmamak ve kanunla yetkili kılınan kişi, kurum ve kuruluşlar dışında kalanların bu bilgilere ulaşmasını engellemek amacıyla gereken önlemleri almakla yükümlüdür." hükmüne yer verilmiştir.

3.3.3.2 Sırların Saklanması

Sırların saklanması başlıklı 31. madde metninde, "Kurul üyeleri ile Kurum personeli, görevleri sırasında öğrendikleri bu Kanun kapsamındaki kuruluşlara, kart hamillerine ve kefillere ait sırları kanunen açıkça yetkili olanlardan başkasına açıklayamaz ve kendi yararlarına kullanamazlar." hükmüne yer verilmiştir.

3.3.3.3 Bilgi Güvenliği Yükümlülüğüne Aykırı Davranılması

Bilgi güvenliği yükümlülüğüne aykırı davranılması başlıklı 39. madde metninde, "Bu Kanunun 8 inci maddesinin beşinci fıkrası ve 23 üncü maddesi hükümlerine kasten aykırı hareket eden kuruluşlar, üye işyerleri ve üye işyeri anlaşması yapan kuruluşların işlerini fiilen yöneten görevlileri ve işlemi yapan kişiler, bir yıldan üç yıla kadar hapis ve bin güne kadar adli para cezası ile cezalandırılırlar. Kartların kullanılması için zorunlu

olup gizli kalması gereken kod numarası, kart numarası, şifre ya da kimliği belirleyici başka bir yöntemin dikkatsizlik veya tedbirsizlik veya meslekte yetersizlik veya emir ve kurallara aykırılık nedeniyle açığa çıkmasına neden olan kart çıkaran kuruluşlar, üye işyerleri ve üye işyeri anlaşması yapan kuruluşların işlerini fiilen yöneten görevli ve ilgili mensupları bin güne kadar adli para cezası ile cezalandırılırlar. Bu Kanunun 31 inci maddesine aykırı davrananlar hakkında bir yıldan üç yıla kadar hapis ve bin güne kadar adli para cezası uygulanır.” hükmüne yer verilmiştir.

4. ADLİ BİLİŞİM İNCELEMELERİ

Teknolojinin ve bilgisayar sistemlerinin çok hızlı bir gelişme göstermesi, artık birçok suç türünün bilgisayar ve teknoloji sistemleri kullanılarak daha kolay işlenmesi, yakalanma riskinin azalması ve kendilerini daha kolay gizleyebilmeleri suç işleyen şüphelilerin kullandıkları yöntemlerde değişikliğe gitmelerine neden olmuştur.

Günlük hayatta yapılan tüm işlerde bilgisayarların ve elektronik cihazların kullanılması, sadece siber suç soruşturmalarında değil, kanunlarla belirlenen birçok suç türü soruşturmasında ve araştırmasında adli bilişim tekniklerinden her geçen gün daha fazla faydalanıldığı görülmektedir (Henkoğlu 2014).

"Dokurer (2005)'e göre, adli bilişim çalışmaları, olay yerinden alınan elektronik bir delilin mahkemede sunulmasına kadar geçen süre içerisinde yapılan laboratuar çalışmalarını kapsamaktadır (Çakır ve Kılıç 2013)."

Siber suçların araştırılması esnasında en çok dijital delillere ihtiyaç duyulmakta ve aynı zamanda olay yerine gidilmeden de internet kullanılarak birçok delil elde edilebildiğinden, siber suç soruşturmalarında elde edilen deliller sadece olay yeri ile sınırlı değildir (Uzunay ve Bıçakçı 2005). Adli bilişim teknikleri kullanılmadan delil elde etme işlemi yapılamayan neredeyse hiçbir siber suç türü yoktur. Adli bilişim teknikleri kullanılmayan bir siber suç soruşturma dosyası düşünülemez. Her ne kadar IP numarası tespiti yapılmış ve alınan şüpheli ifadelerinde de olay aydınlatılmış olsa dahi, böyle bir soruşturma her zaman için eksik kalmış bir soruşturmadır.

Adli bilişim teknolojileri kapsamında, bilgisayarların herhangi bir suça iştiraki genel olarak aşağıdaki üç şekilde karşımıza çıkmaktadır (Henkoğlu 2014). Bunlar;

- Bilişim Suçunun Hedefi Olarak: Bilgisayarın erişebilirliği, gizliliği ve bütünlüğüne zarar verilmesi.

- Bilişim Suçunu Gerçekleştirmek İçin Araç Olarak: Yasadışı maddelerin/ürünlerin satışı, çocuk pornografisi, internet dolandırıcılığı ve fikri mülkiyet haklarının ihlal edilmesi.
- Bilişim Suçunun Gerçekleştirilmesinde Faydalanılarak: Bilişim işlenmesinde farkında olmadan pay sahibi olan (Botnet ve DDOS gibi saldırı uygulamaları içerisinde) bilgisayarın oluşumuna katkıda bulunduğu suçlardır.

4.1 Adli Bilişim Nedir?

Suça karışan her suçlunun işlediği suçla ilgili arkasında iz, delil ve emare bırakmaması mümkün değildir. Suç ve suçluların ortaya çıkartılabilmesi ve bunların ceza muhakemesinde delil olarak kullanılabilmesi için belli kurallara uygun davranılması gerekmektir (Dülger 2013). Adli bilişim, kendi içerisinde belli kuralları olan dijital delil elde etme yöntemlerinin bütünü olan bir bilim dalıdır.

Türkçeye "Computer Forensic (Bilgisayar Adli Bilimi)" tabirinden geçen adli bilişim, Vikipedia Özgür Ansiklopide "elektromanyetik ve elektrooptik ortamlarda muhafaza edilen veya bu ortamlarca iletilen ses, görüntü, veri, bilgi veya bunların birleşiminden oluşan her türlü bilişim nesnesinin, mahkemede sayısal delil niteliği taşıyacak şekilde tanımlanması, elde edilmesi, saklanması, incelenmesi ve mahkemeye sunulması çalışmaları bütünüdür." şeklinde tanımlanmıştır (İnt.Kyn. 21).

Henkoğlu (2014) adli bilişimi, "bilişim sistemleri ve üzerinde bulunan depolama ünitelerinin, herhangi bir suçu işlemede veya yasaklanmış bir faaliyette kullanılıp kullanılmadığını tespit etmek amacıyla yapılan çalışmaların tümüdür." şeklinde tanımlamıştır.

Öztürk (2007)'e göre ise adli bilişim, tüm bilişim donanım, yazılım ve yöntemlerinin hukuki kurallar çerçevesinde bütünleşik olarak kullanılabilmesiyle anlam bulan bir disiplin olarak tanımlanmıştır.

Bir başka kaynakta ise, adli bilişimin suçun aydınlatılabilmesi için bilimsel yöntemler kullanılarak, dijital medyalar üzerinde bulunan, suçla ilgili dijital delillerin bozulmadan ve zarar görmeden anlaşılabilir bir şekilde adli makamlara sunulmaya hazır hale getirilmesini sağlayan ve bilimsel teknik prensiplerin uygulandığı bir delil inceleme süreci olarak tanımlandığı görülmüştür (İnt.Kyn.22).

Başka bir ifade ile bilgisayar üzerindeki verilerden, suç soruşturmasını aydınlatacak ve ihtiyaç duyulan verilerin çıkartılarak, bunların delil olarak kullanılması olarak ifade edilen adli bilişim; sadece veri kurtarma, silinmiş verileri bulma, kaybedilen evrakları geri getirme demek değil, işlenen bir suçun delillendirmesidir. Siber suçlar ya da bilişim yoluyla işlenen suçların soruşturulmasında, şüpheliden elde edilecek her türlü dijital verinin incelenmesiyle suçun işlendiği ispatlanabileceği gibi, klasik suçlardan olan cinayet, gasp, hırsızlık vb. suçların şüphelilerinden elde edilecek malzemelerin incelenmesi ile de, işlenen suçla ilgili delil niteliğinde dijital verilere ulaşmak mümkün olacaktır. Dolayısıyla dijital delil incelenmesiyle, siber suçlar ya da bilişim yoluyla işlenen suçların yanı sıra, klasik suçların veya suçluların tespiti ya da tespit edilenlerin dijital delilerle desteklenmesi de imkan dahilindedir.

4.2 Dijital Delil

Adli bilişim ile alakalı bir çalışma esnasında, bilişim sistemleri (bilgisayarlar, akıllı cep telefonları, tablet bilgisayarlar, USB bellekler, dijital fotoğraf makineleri vb.) ve bu kapsamdaki depolama aygıtları üzerinden elde edilen adli delillere dijital delil denmektedir (Henkoğlu 2014).

Dijital deliller, yapı itibariyle bozulmaya ve kolay bir şekilde değiştirilmeye müsait oldukları için, hukuki yönden kabul edilebilirlikleri konusunda bazı sıkıntılar ile karşılaşılmaktadır. Bu delillerin mahkeme esnasında gerçek delil özelliği gösterebilmeleri için, delillerin ilk alındığı andan itibaren değişmediğinin, hangi tarihte, nereden ve kimlerden alındığının doğrulanması büyük önem arz etmektedir (Uzunay ve

Bıçakçı 2005).

Genel olarak, daha çok siber suçlar olmak üzere işlenen tüm suçlarda, elektronik veya manyetik bir ortam üzerinden iletilen veya bu ortamlara kaydedilen delil niteliği taşıyan veri ve bilgilere dijital delil demek mümkündür. Dijital delillerin en çok rastlanıldığı alanlar ise, veri dosyaları, kurtarılmış silinmiş dosyalar, kayıp alanlardan kurtarılmış veriler, dijital fotoğraf ve video görüntüleri, yazılımlar, e-postalar, chat (sohbet) kayıtları, ziyaret edilen web sayfaları, internet geçmişi, temporary/temp dosyaları (Geçici dosya kayıtları), log kayıtları (günlük yapılan işlemleri gösteren kayıtlar) ve abone kayıtları vb. şeklindedir.

Henkoğlu (2014)'a göre adli bilişim sürecinin her aşamasında yapılan işlemlerin, delilin güvenilirliğine, gerçekliğine, eksiksizliğine, inanılabilirliğine ve tekrarlanabilirliğine şüphe düşürmeyecek yöntemlerin kullanılarak yapılması gerekmektedir.

4.3 Adli Bilişimin Mevzuattaki Yeri

Türkiye'de adli bilişimin uygulaması ile ilgili mevzuat çalışmasında bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma hükümleri ile dijital delil incelemesi konusu CMK'nın 134 üncü maddesinde ve Adli ve Önleme Aramaları Yönetmeliğinin 17. Maddesinde düzenlenmiştir. Ancak bu çalışmada sadece CMK'da bulunan düzenleme incelenecektir.

4.3.1 5271 Sayılı Ceza Muhakemesi Kanununda Adli Bilişim

CMK'nın 134 üncü maddesi 1. fıkrasında; "Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkanının 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

haline getirilmesine hakim tarafından karar verileceği" düzenlenmiştir.

Maddenin 2. fıkrasında; "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 elkonulabileceği, şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazların gecikme olmaksızın iade edileceği" düzenlenmiştir.

Maddenin 3. fıkrasında; "Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesinin yapılacağı" düzenlenmiştir.

Maddenin 4. fıkrasında; "Üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verileceği ve bu hususun tutanağa geçirilerek imza altına alınacağı" düzenlenmiştir.

Maddenin 5. ve son fıkrasında; "Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyasının alınabileceği, kopyası alınan verilerin kâğıda yazdırılarak, bu hususun tutanağa kaydedileceği ve ilgililer tarafından imza altına alınacağı" düzenlenmiştir.

Suç dolayısıyla yapılan bir soruşturmada, madde kapsamında gerçekleştirilen işlemlerde 2. fıkraya istinaden bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması nedeniyle el koyma işlemi gerçekleştirilmiş ise, 3. fıkra hükmüne göre el konulan dijital materyallerin içerisinde bulunan bütün verilerin yedeklemesi yapıldıktan sonra, 4. fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınması gerekmektedir. Ayrıca, yedekleme işlemlerinin tamamlanmasının ardından yine 2. fıkra hükmü gereğince el konulan cihazlar, gecikme olmaksızın şüpheli şahsa geri iade edilir.

Madde kapsamında el koyma işlemi gerçekleştirilen soruşturmalarda, yargılamanın soruşturma ve kovuşturma aşamasında hukuki ihtilafa düşülmesi halinde tekrar inceleme işleminin gerçekleştirilebilmesi için adli emanete teslim edilmesi ve 4. fıkra hükmü gereğince şüpheliye verilmesi gereken yedekleme cihazlarının temini ile ilgili ne madde metninde ne de herhangi bir yönetmelikte herhangi bir düzenleme bulunmamaktadır. Ayrıca, alınan kopyaların/imajların saklanıp saklanmayacağı, saklanacaksa ne kadar süre ve ne şekilde saklanacağı konusunda ise belirsizlik mevcuttur.

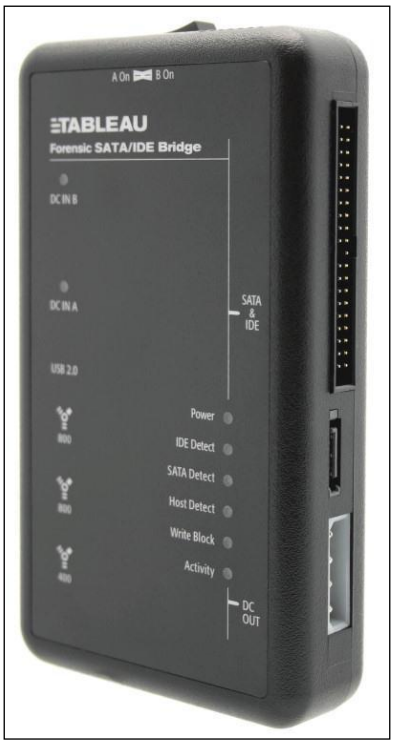
4.4 Adli Bilişimde Kullanılan Donanım ve Yazılımlar

Adli bilişim teknolojilerinde kullanılan materyallere kısaca bakacak olursak, donanım ve yazılım olarak 2'ye ayırmak gerekecektir. Bu ikisinden herhangi birinin olmaması adli bilişim sürecinin işleyişini olumsuz etkileyecek hatta sürecin işlemini engelleyecektir.

4.4.1 Donanım

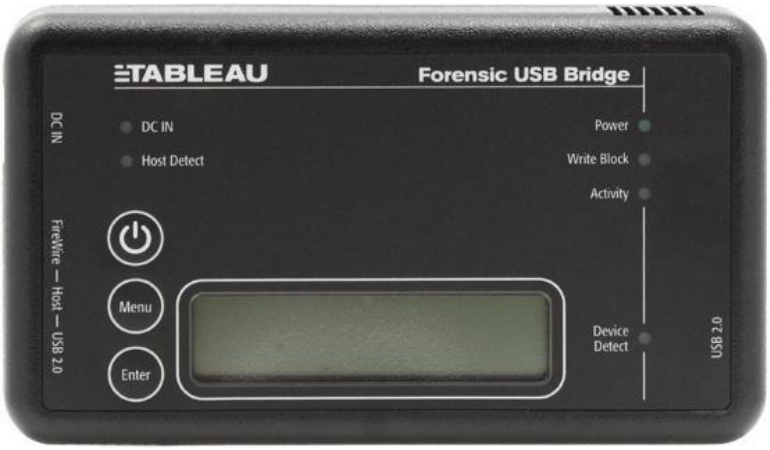
Adli bilişimde kullanılan donanımları yazma koruma ve imaj alma cihazları olmak üzere ikiye ayırabiliriz. Yazma koruma cihazları ile imaj alabilmek için imaj alma yazılımı gerekirken, imaj alma cihazları ile harici herhangi bir yazılıma ihtiyaç duyulmadan cihaz içeriğinde bulunan yazılım vasıtası ile imaj alınabilmektedir.

Resim 4.1'de Tableau firmasına ait SATA/IDE köprüsü (Write Block) gösterilmiştir. Bu cihazların imaj alma işlemlerinde kullanılabilmesi için, herhangi bir imaj alma yazılımı ile birlikte bir de bilgisayara ihtiyaç duyulmaktadır. Veri akışına delilden bilgisayara doğru tek yönlü sağlamakta ve delil bütünlüğünü korumak için kullanılmaktadır. WiebeTech isimli firma tarafından üretilen modeller de piyasada bulunmaktadır.



Resim 4.1 Tableau Firmasına Ait SATA/IDE Köprüsü.

Write blocklar aparatları ile birlikte kullanıldığında, bilgisayara herhangi bir sürücü yüklemesi yapılmasına gerek olmaksızın IDE, SATA, SCSI, MSC MS Pro, SMC, xD, ve SD MMC aygıtlar için tüm sürücü desteği otomatik olarak sağlanmaktadır. Resim 4.2'de Tableau firmasına ait USB köprüsü gösterilmiştir.



Resim 4.2 Tableau Firmasına Ait USB Köprüsü.

Adli bilişim standartlarına uygun olarak adli makamlara sunulmak üzere delilin adli kopyasının alınmasında kullanılan temel donanım araçlarından bir tanesi de, doğrudan cihaz üzerinden imaj alma işlemi gerçekleştirebilen Tableau firmasına ait TD1 cihazıdır. TD1 cihazı ile, iki tür kopyalama işlemi gerçekleştirilmektedir. Birincisi Disk-to-Disk'dir, yani kaynak disk (delil) içerisindeki tüm verilerin olduğu gibi başka bir diske tüm sektörleri ile kopyalanması anlamına gelir. İkincisi ise, Disk-to-File seçeneğidir. Kaynak disk içerisinde bulunan tüm veriler hedef diske uluslar arası adli bilişim inceleme programlarının dosya uzantısı ile istenilen boyutlarda imaj olarak aktarılmasıdır. Disk-to-File seçeneğinde hedef diskin boyutuna göre birden fazla kaynak diskin imajı hedef disk içerisine aktarılabilmektedir. TD1'in yerini aynı firma tarafından piyasa sürülen TD2 ve TD2u cihazları almaya başlamıştır. Bu iki cihazın da ortak özellikleri daha hızlı imaj alma ve bir adet kaynak diskten iki adet imaj disk oluşturmaktır. Resim 4.3'de Tableau firmasına ait TD1 model Forensic Duplicator gösterilmiştir.

Resim 4.3 Tableau Firmasına Ait TD1 Model Forensic Duplicator.

Donanımsal imaj alma cihazları arasında Logicube firmasına ait Falcon, Intelligent Computer Solutions firmasına ait The Rapid Image 7020, Salvation Data Teknoloji

firmasına ait Data Copy King ve mh SERVICE GmbH firmasına ait BeeCube isimli cihazlarda bulunmakta ve adli bilişim sektöründe kullanılmaktadır (Bakan ve Saluk 2014).

4.4.2 Yazılım

4.4.2.1 İmaj Alma Yazılımları

İmaj alma yazılımlarından en sıklıkla kullanılanlarına sırasıyla bakacak olursak;

FTK imager, Amerika'da bulunan AccessData isimli firma tarafından üretilen ve internet sitesinde ücretsiz olarak kullanıma sunulan imaj alma ve ön izleme programıdır (Bakan ve Saluk 2014). En sık kullanılan ve imaj alma sonrasında kolaylıkla imaj kontrolü yapılabilen bir programdır.

EnCase Forensic İmager, Amerika'da bulunan Guidance Software isimli firma tarafından üretilen ve internet sitesinde ücretsiz olarak kullanıma sunulan imaj alma programıdır. Yazılım ile lokal makinede imaj alınabilmekte, ancak ağ üzerinden imaj alınamamaktadır (Bakan ve Saluk 2014).

X-Ways İmager, Almanya'da bulunan X-Ways firmasına ait ücretli imaj alma programıdır. Akıllı sıkıştırma yapma, boş disk bölümlerini imaja dahil etmeme, tersten imaj alabilme gibi özellikleri bulunmakta ve dongle ile çalışmaktadır (Bakan ve Saluk 2014).

Helix 3 Pro, Amerika'da kurulu e-fense firmasının ürettiği, boot olabilen veya canlı (açık) sistemlerde kullanılabilen imaj alma ile beraber incelemeye yönelik diğer yazılımları da barındıran CD'dir (Bakan ve Saluk 2014). Genellikle harddiski zor bir yerde bulunan dizüstü bilgisayarların ya da açık sistemlerin imaj almasında kullanılmaktadır.

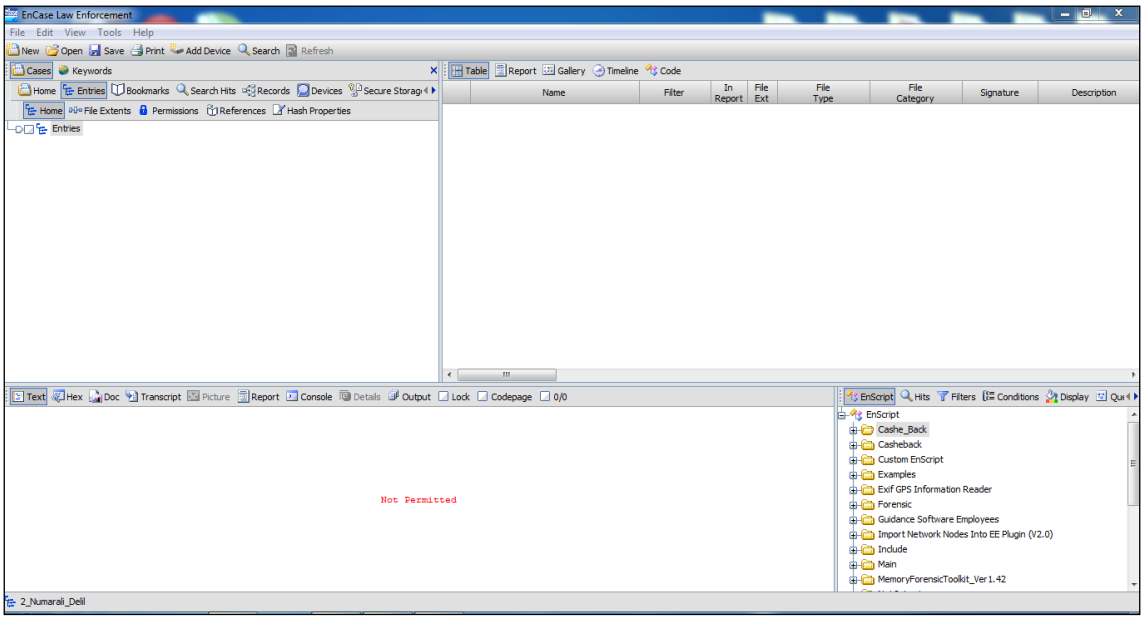
AIR (Automated Image and Restore) ve Guymager, Linux tabanlı çalışan, farklı formatlarda imaj almak için grafik ara yüzü şeklinde geliştirilmiş açık kaynak kodlu bir uygulamadır (Bakan ve Saluk 2014).

4.4.2.2 İnceleme Yazılımları

Adli bilişim alanında en çok bilinen inceleme programları olan EnCase Forensic, FTK (Forensic Toolkit) ve X-Ways Forensic gibi yazılımlar, inceleme konusu dijital delil üzerinde oldukça tutarlı ve tekrar edilebilir sonuçlar vermeleri, ticari yazılımlar arasında ön plana çıkmalarını sağlamıştır (Henkoğlu 2014).

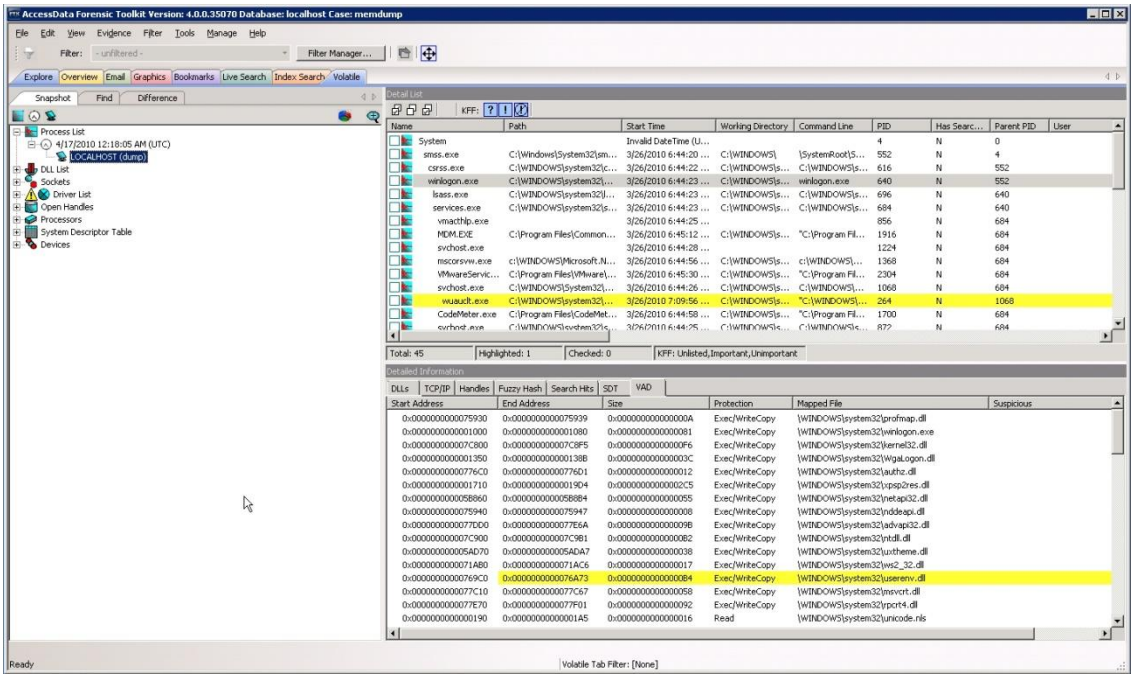
EnCase Forensic, Amerika'da bulunan Guidance Software isimli firma tarafından geliştirilen en popüler adli bilişim yazılımlarından biridir. Bire bir kopya (imaj) oluşturma, analiz aşamasından raporlama aşamasına kadar tüm aşamalarda kullanılabilen ve güvenilirliği en fazla olan yazılımlardan biridir. Encase neredeyse tüm dosya sistemlerini tanıyan, birçok imaj formatı ile uyumlu ve RAID sistemlerini destekleyen Windows işletim sistemi tabanlı bir yazılımdır (Henkoğlu 2014).

Encase aynı zamanda, kendine özgü imaj formatları olan (E01, Ex01 vb.), imaj içerisinde bulunan mevcut ve silinmiş tüm alanları inceleyebilen, anahtar kelimesi tarayabilen, veri kurtarma, e-posta ve sohbet kayıtları tespiti ve hash analizi yapabilen bir yazılımdır (Bakan ve Saluk 2014). Resim 4.4'de EnCase Forensic yazılımına ait ekran görüntüsü gösterilmiştir.



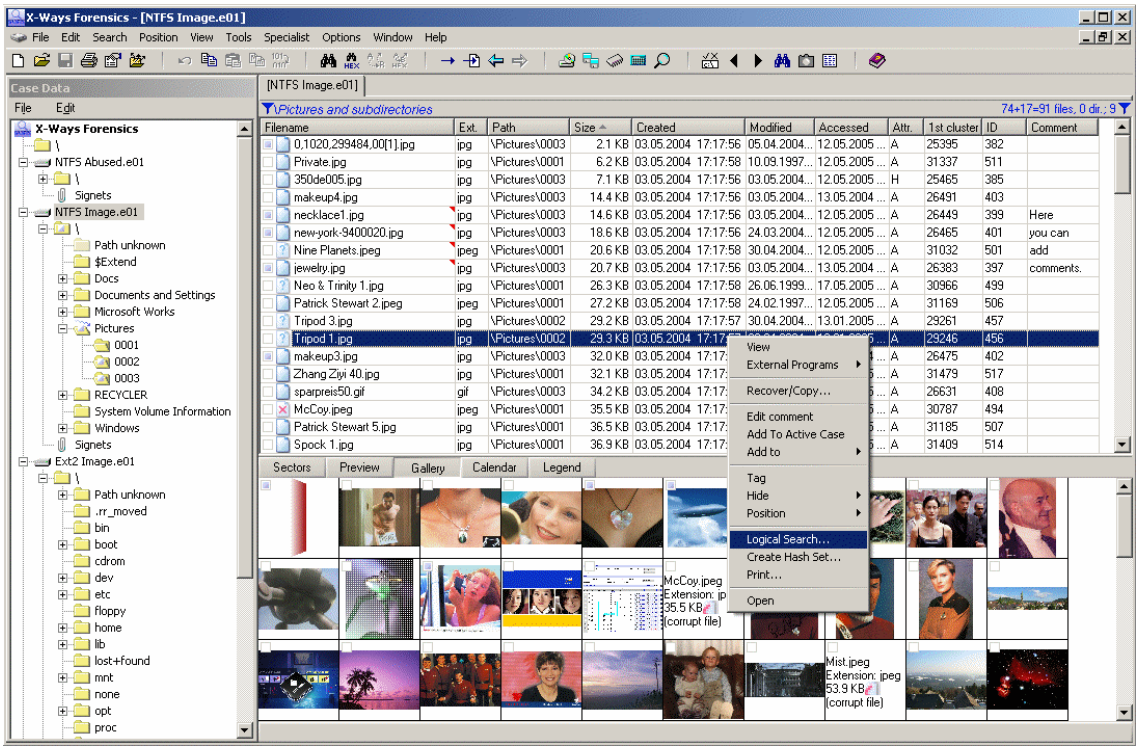
Resim 4.4 EnCase Forensic Kullanıcı Ara Yüzü Ekran Görüntüsü.

FTK, Amerika'da bulunan AccessData isimli firma tarafından geliştirilen adli bilişim alanındaki Windows tabanlı ikinci en popüler yazılımdır. Encase üzerinde bulunmayan bazı özelliklere sahip olduğundan ve kullanımının daha kolay olması nedeniyle adli bilişim uzmanları tarafından tercih edilmektedir. Encase Forensic'te olduğu gibi adli bilişimin tüm aşamalarında kullanılmakta ve maliyeti Encase'e oranla daha düşüktür (Henkoğlu 2014). Resim 4.5'de FTK yazılımına ait ekran görüntüsü gösterilmiştir.



Resim 4.5 FTK Kullanıcı Ara Yüzü Ekran Görüntüsü.

X-Ways Forensics, Almanya'da bulunan X-Ways firması tarafından geliştirilmiş Windows işletim sistemi tabanlı bir adli bilişim yazılımıdır. Program ara yüzü Encase ve FTK ile benzer özellikler taşımaktadır. Bu yazılımlar dışında desteklediği mobil cihazlar veya imajları incelenebilmektedir (Bakan ve Saluk 2014). Resim 4.6'de X-Ways Forensic yazılımına ait ekran görüntüsü gösterilmiştir.



Resim 4.6 X-Ways Forensic Kullanıcı Ara Yüzü Ekran Görüntüsü (İnt.Kyn.25).

4.5 Adli Bilişim Aşamaları

Şüpheli şahıslardan elde edilen bilgisayar harddisklerinin ve veri depolamaya yarayan her türlü bilgisayar çevre birimlerinin mümkün olan en kısa sürede adli kopyasının (imaj - birebir kopya) alınması, kopyalama işleminden sonra ise, asıl dijital materyaller üzerinde hiçbir işlem yapılmadan kopya üzerinde gerekli teknik incelemelerin yapılması gerekmektedir. Bu sebeple, adli bilişim incelemeleri uzun bir süreç olduğundan dolayı çeşitli aşamalara ayrılmıştır. Bu çalışmada adli bilişim aşamaları hazırlık aşaması, dijital delillere ilk müdahale aşaması, adli kopya (imaj) alma aşaması, inceleme aşaması ve raporlama aşaması olmak üzere 5'e ayrılmıştır.

Sevli ve Küçüksille (2013), adli bilişim aşamalarını 4'e ayırmış ve buna göre adli bilişim soruşturmaları doğrusal bir işlem süreci izlediğinden, bu sürecin temel adımlarını; tanımlama, çıkarım, analiz ve delilin sunumunun oluşturduğundan bahsedilmiştir.

Henkoğlu (2014) ise, adli bilişim aşamalarını 3 başlık altında toplamıştır. Bunlar;

- Delillerin tespit edilmesi, toplanması ve muhafazası,
- Delilleri açığa çıkartma, inceleme ve analiz yapılması,
- Delillerin raporlanması.

4.5.1 Hazırlık Aşaması

Hazırlık aşaması, çoğu adli bilişim çalışmalarında yer almamaktadır. Ancak adli bilişim aşamalarında yer almasının önemi büyüktür. Şöyle ki, soruşturma neticesinde tespiti yapılan şüpheli şahıs ile ilgili bilgilerin toplanması, teknik bilgi ve becerisinin tespitine çalışılması ve adli bilişim kapsamında ne seviyede olduğunun öğrenilmesi arama ve el koyma işlemlerinin uygulandığı esnada önem arz etmektedir. Aksi halde, şüpheli ile karşılaşıldığında hazırlamış olduğu bir düzenek ile açık vaziyette bulunan ve internete bağlantı sağladığı tüm cihazlar kapatılabilir ve uçucu olan dijital delillere bir daha ulaşılamayabilir.

Arama ve el koyma işlemine konu, yetkili mahkemeden alınan kararda, CMK 134. maddenin bulunup bulunmadığı mutlaka kontrol edilmelidir. Arama ve el koyma işlemi öncesinde şüpheli şahıs hakkında her ne kadar bilgi edilmiş olsa da, arama yapılacak ortamda neler bulunduğu tam olarak bilinemeyeceğinden, her şeye hazırlıklı olunarak gidilmeli ve ihtiyaç olabilecek tüm yazılım, donanım ve yedekleme ünitelerinden yeteri kadar miktar hazır bulundurulmalıdır.

4.5.2 Dijital Delillere İlk Müdahale Aşaması

Dijital delillere ilk müdahale genellikle olay yerinde bulunan kolluk kuvvetleri tarafından yapıldığından (Henkoğlu 2014), dijital delillere ilk müdahale herhangi bir kolluk kuvveti vasıtası ile değil, adli bilişim konusunda eğitim almış uzman personel tarafından yapılmalıdır. Aksi halde delil bütünlüğünün bozulması vazgeçilmez olacaktır.

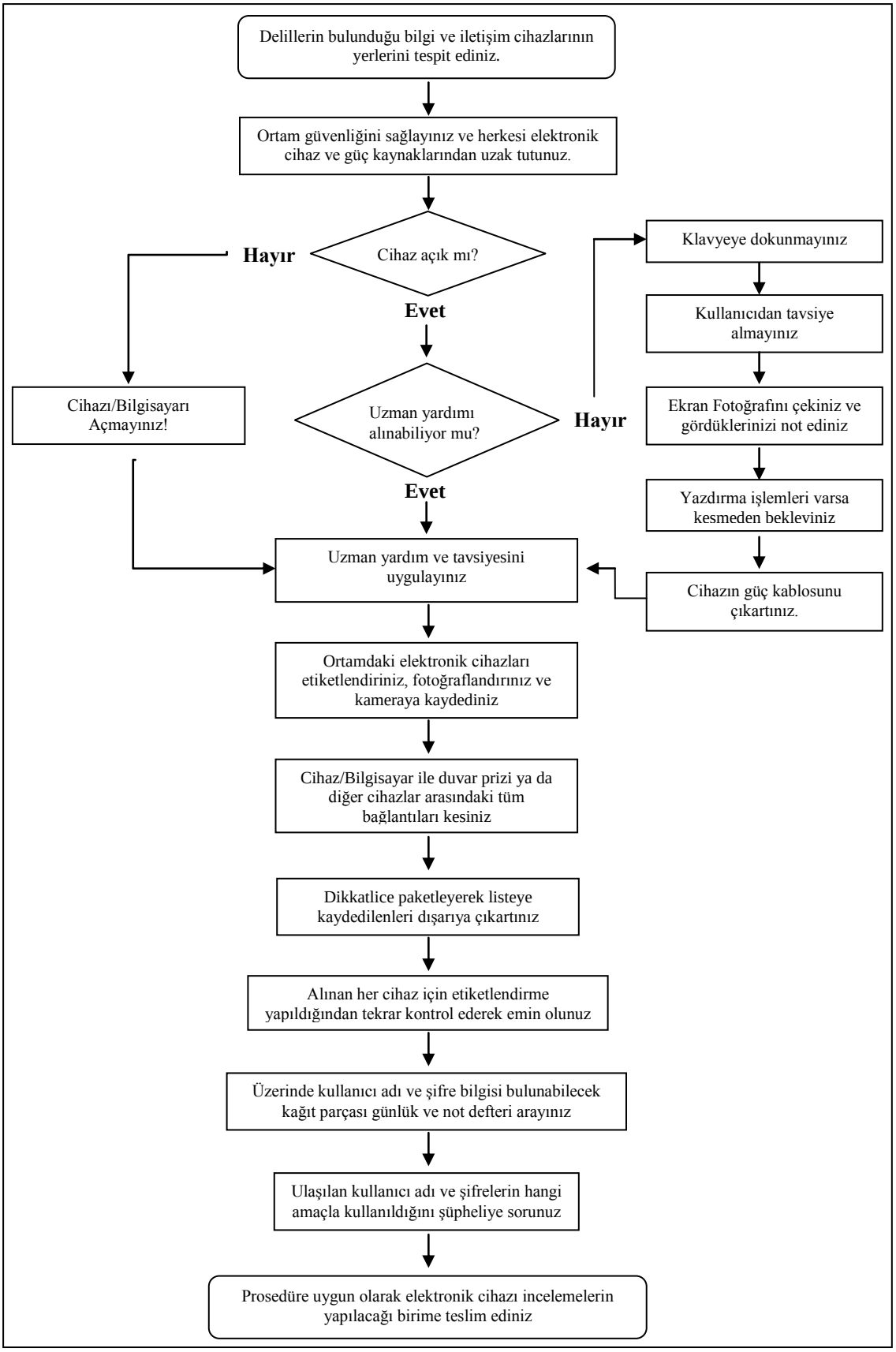
Bu aşamada en önemli amaç, adli makamlara sunulan elektronik delillerin kabul edilebilirliğini sağlamak ve her aşamada buna yönelik tedbirler almak olduğundan, elektronik delillerin en iyi şekilde elde edilmesine etki eden faktörler personel, delilin orijinalliği, kullanılan yöntemler, kullanılan donanım ve yazılımlar ve delil koruma ve gözetim zinciridir (Kiçeci 2014).

Dijital delillere müdahale aşamasında dikkat edilmesi gereken hususlar aşağıya çıkartılmıştır.

- Dijital delillere ilk müdahale, mutlaka adli bilişim alanında eğitim almış uzman personel tarafından yapılmalı, eğer uzman personel bulunmuyor ise, Şekil 4.1'de belirtilen hususlara dikkat edilmeli,
- Arama yapılacak bölgede delillerin bulunduğu yerler tespit edilmeli ve gerekli görülmesi halinde fotoğraflandırma işlemleri yapılmalı veya kamera kaydına alınmalı,
- İlk müdahale esnasında insan vücudunda oluşan statik elektriği engelleyecek bileklikler takmak suretiyle oluşabilecek risklere karşı önlem alınmalı,
- Bilgisayar açık konumda ise, ekranın fotoğrafı çekilerek bilgisayarda hali hazırda çalışan sistemlerin tespiti ile ilgili notlar alındıktan sonra elektrik bağlantısı kesilmeli ya da bataryası çıkartılmalı,
- Eğer hali hazırda çalışan sistem bilgilerinin alınması gerekli değil ise, açık bulunan bilgisayar elektrik fişinden çekilmek suretiyle kapanmalı ve kesinlikle tekrar fişi takılmamalı,
- Arama yapılan yerde bulunan şüpheli şahıs, delillerden arındırılmalı ve el konulacak dijital materyallere müdahale edebilecek kadar yaklaştırmamalı,
- Olay yerinde imaj alma işlemlerinin yapılması gerekiyor ise, kesintisiz güç kaynağının olup olmadığı araştırılmalı, kesintisiz güç kaynağı bulunmuyorsa arama tutanağında bu husus belirtilerek CMK 134. Maddesi gereğince el koyma hükümleri uygulanmalı,
- Olay yerinde imaj alma işlemi gerçekleştirilmiş ise, işlem bitiminde imaj almaya ne

zaman başladığı ve ne zaman son bulduğu ve tespit edilen hash değerleri mutlaka arama tutanağına yazılmalı,

- Dijital materyallere el koyma işlemi gerçekleştiriliyor ise, imaj alma işlemi gerçekleştirilmeksizin şüpheli şahıs ya da vekili talep etse dahi, kesinlikle hash değeri hesaplatma yöntemi ile tespit edilen hash değerleri şüpheli şahıs ya da vekiline verilmemeli,
- Olay yerinde birden fazla bilgisayar veya dijital materyal bulunuyor ise, suçta kullanıldığı muhtemel bilgisayarın tespiti adına tüm dijital materyallerin tek tek kime ait oldukları ve kim tarafından kullanıldığı gibi bilgiler sıcağı sıcağına öğrenilmeli,
- Eğer dijital materyallere el konulacak ise, el konulan dijital materyallerin fiziksel özellikleri, marka, model, seri numarası ve boyut bilgileri mutlaka belirtilmeli ve hepsi teker teker etiketlerle numaralandırıldıktan sonra, delil torbalarına konularak ağızları mühürlenip aramada bulunan şüpheliye ve hazır bulunana imzalatılmalı,
- Olay yerindeki işlemler sonlandırılıp tutanağa geçirildikten sonra arama yapılan bölgeden ayrılmadan, el konulan dijital materyallerin son kontrolü yapılmalı ve eksik olmadığından emin olunmalı,
- Arama işlemi neticesinde, el konulan dijital materyaller sıvı maddelerden ve manyetik ortamlardan uzak ısı ve nem kontrolü bulunan bir ortamda muhafaza edilmeli,
- El konulan deliller, saydam statik/anti-statik veya köpük korumalı/kabarcıklı delil torbası içerisinde bir taşıma çantası vasıtasıyla taşınmalıdır.



Şekil 4.1 Olay Yeri İncelemesi Faaliyet Akış Diyagramı (Henkoğlu 2014).

4.5.3 Adli Kopya (İmaj) Alma Aşaması

İmaj alma, genellikle laboratuar ortamında yapılması uygun görülen bir işlem olup, çeşitli donanım ve yazılımlar kullanılmak suretiyle yazma koruma engellemesi önlemi alındıktan sonra, dijital materyalin içerisinde bulunan verilerin fiziksel (silinmiş, silinmemiş vb.) olarak birebir (bit-to-bit) kopyasının alınması işlemidir. İnceleme işlemleri, delil bütünlüğünün korunması açısından imaj üzerinde gerçekleştirildiğinden, bu aşamanın kusursuz olması gerekmektedir.

İmaj alma aşaması, delil bütünlüğü açısından dijital materyallere ilk müdahale aşamasından sonra en önemli aşamadır. Delil ile yakın temas halinde bulunulan bu aşamada, bilinmesi gereken bazı kavramlar vardır. Adli bilişimin temel yapı taşları denebilecek bu kavramlar hash algoritması ve write block (yazma koruma engellemesi)'dur.

4.5.3.1 Hash Algoritması

Dünyada daha çok adli bilişim alanında delil bütünlüğünün korunup korunmadığı amacıyla kullanılan hash algoritması, bilgisayar medyasında bulunan tüm 0 ve 1'lerin birbirleri ile belli bir algoritma ile çarpılmasıyla elde edilmektedir (Kılıç 2014).

İmaj alma işlemi neticesinde, kullanılan yazılım tarafından otomatik olarak oluşturulan metin belgesi içerisinde 2 farklı hash ibaresi yer almaktadır. Bunlardan, acquisition hash dijital materyalin incelemeye başlanmadan önceki dijital delil inceleme cihazında alınmış doğrulama algoritması iken, verify hash ise inceleme sonunda dijital materyalin delil bütünlüğünün bozulmadığını gösteren doğrulama algoritmasıdır. Delil bütünlüğünün bozulmadığını söyleyebilmek için acquisition hash ile verify hash değerleri birbirinin aynısı olması gerekmektedir. Aksi takdirde, hakkında soruşturma yapılan sanık ya da vekili delilin üzerinde değişiklik yapıldığı iddiasında bulunulabilecektir. Ceza yargılama hukukunda yazılı olmayan "şüpheden sanık

yararlanır” ilkesi gereği, gerçekte suçu işlediği yönünde deliller elde edilse dahi, sanığa ceza verilememesi dahi söz konusudur.

Bilgisayar medyası üzerinde yapılan en küçük bir değişiklik ile aynı olması mümkün olmayan hash değeri, MD5 için 32 karakter uzunluğunda 0-9 ve a-f karakterlerinden oluşan bir değer iken, SHA1 için aynı karakterlerden oluşan 40 karakter uzunluğunda bir değerdir (Kılıç 2014). Bir çalışma kapsamında alınan imaja ait örnek MD5 ve SHA1 hash değerleri aşağıdaki gibidir.

- **MD5** : e8359ebbe97f3bae584c76971059c35b
- **SHA-1** : 5dbd53e4e7b0f6b8dd19d084af57722da83018e9

4.5.3.2 Write Block (Yazma Koruma Engellemesi)

Yazma koruma için kullanılan write blocklar, delil bütünlüğünü koruyarak imaj alabilmek veya inceleme yapabilmek için geliştirilmiş yazılım ya da donanımlardır. Veri depolama birimi bu write blocklar kullanılarak bilgisayara bağlandığında, orijinal medya üzerinde yazma işlemi gerçekleştirmeden sadece okuma işlemi yapacaktır (Bakan ve Saluk 2014). Adli bilişimde imaj alma işlemleri esnasında mutlaka write block kullanılmalıdır. Write block kullanılmadığı takdirde, imaj alma esnasında kullanılan bilgisayarda virüs, trojan vb. zararlı yazılımın olması halinde, kullanıcının haberi dahi olmadan delile veri yazılmış ve hash değeri de otomatik olarak değişmiş olacaktır.

Her ne kadar yazılımsal write blockların varlığından ve adli bilişim alanında kullanılabilirliğinden bahsedilse de, imaj alma aşamasında donanımsal write block kullanarak daha risksiz bir sonuca ulaşılmaktadır.

4.5.4 İnceleme Aşaması

İnceleme aşamasında delil niteliği taşıyan veriler, imaj içerisinden bütünlüğü

sağlanacak şekilde çıkartılır. İncelemeci, bilgisayar ortamında bulunan somut olmayan verilerin uçuculuğun farkında olmalı ve çıkarım sürecinde bu problemi azaltacak araç ve gereçleri kullanmalıdır (Sevli ve Küçüksille 2013).

İnceleme aşaması, en çok teknik bilgi gerektiren ve en uzun sürecek safhadır. Uzman personel inceleyeceği materyalde ne araması gerektiğini bilmeli ve ona uygun yöntemler uygulamalıdır. Her inceleme talep edilen olay için ayrı bir yöntem geliştirmelidir. Örneğin, cinayet olayı ile ilgili el konulan dijital materyallerde yapılacak inceleme ile bilişim sistemine girme suçu kapsamında yapılacak inceleme işlemi farklılık gösterecektir. Bu sebeple incelenen materyale ait tüm detaylar soruşturma biriminden adli bilişim uzmanı tarafından istenmelidir.

4.5.5 Raporlama Aşaması

İnceleme esnasında tespit edilmesi gereken ilk husus, incelenecek bilgisayar depolama ortamlarına ait genel bilgilerin çıkarılması ve raporlanmasıdır. İnceleme raporunda bulunması gereken genel bilgiler toplam kapasite, partition (disk bölümü) sayısı, dosya sistemi, işletim sistemi türü ve sürümü, işletim sisteminin kurulum tarihi, bilgisayarda kayıtlı kullanıcı bilgileri ve bilgisayar son kapanış tarihi bilgileridir (Çakır ve Kılıç 2013).

"Bilgisayar medyasında bulunan veriler adli bilişim sürecinde çeşitli yöntemlerle ortaya çıkartılırken, raporlama esnasında bu verilerden doğrudan suç ile ilgili olanlar raporlanır ve delil haline getirilmiş olur" (Kılıç 2014).

İnceleme Raporunda akıcı ve herkes tarafından anlaşılır bir dil kullanılmalı, teknik ifadelerin açıklamaları mutlaka raporun altında belirtilmelidir. Hazırlanan inceleme raporu sanığı mahkumiyete ya da özgürlüğe götüreceğinden dikkatli ve duyarlı davranılmalıdır.

Burucu ve Kuşoğlu (2014)'na göre hazırlanan inceleme raporu açık ve anlaşılır olması,

etkin ve doyurucu olmasının yanında bilimselliğe de uygun olması gerekmektedir.

Adli bilişimin son aşaması olan raporlama aşamasında elde edilen sonuçlar, geçerli bir delil teşkil edecek şekilde hazır hale getirilir ve mahkemeye sunulur. (Sevli ve Küçüksille 2013)

5. MATERYAL VE METOT

Bu bölümde, Banka ve/veya Kredi Kartlarının Kötüye Kullanılması suçu ile ilgili bir senaryo hazırlanmış ve bu senaryo kapsamında, aşağıda ayrıntıları belirtilen 1, 2 ve 3 numaralı dijital materyaller üzerinde CMK 134. maddesi kapsamında uygulanan işlemler anlatılmıştır. Bu sayede öncelikle siber suçlar biriminde çalışan kolluk kuvvetleri olmak üzere, adli birimlerde çalışan tüm kolluk kuvvetlerinin karşılaştıkları soruşturmalarda adli bilişim aşama ve yöntemlerini nasıl uygulayacakları konusunda bilgi sahibi olmaları amaçlanmıştır.

1 ve 2 numaralı delil içerisine suça konu bilgi, belge, resim vb. dokümanlar kopyalanmış, kopyalanan verilerin bazıları ise gizlenmiş ya da silinmiştir. 3 numaralı delil olarak tanımlanan bilgisayar vasıtasıyla ise, www.ofix.com isimli web sitene 95.9.133.146 IP numarası ile bağlantı sağlanarak yasinbasar60@gmail.com isimli mail adresi ile kayıt yapılmış ve aktif olarak kullanılan gerçek bir kredi kartı ile alışveriş işlemi gerçekleştirilmiştir. Alışveriş işleminde senaryo içerisinde 2 numaralı delil olarak tanımlanan Sandisk marka 16 GB kapasiteli bir USB bellek siparişi yapılmıştır.

Bu kapsamda, senaryo gereği yürütülen siber suç soruşturması neticesinde, bir bankaya ait kredi kartından müştekinin bilgisi ve rızası dışında internet üzerinden gerçekleştirilen bir işleme ait IP numarasının tespit edildiği ve EK-1'de örnek olarak gösterilen adli makamlardan alınması gereken arama ve el koyma izinlerinin alındığı varsayılarak, IP numarası tespiti yapılan şüpheli şahsın suçu gerçekleştirdiği adreste arama işlemi yapılmış ve yapılan aramada, 3 adet suç unsuru olduğu değerlendirilen dijital materyale CMK'nın 134. maddesi gereği yedek alma ve inceleme işlemlerinin yapılabilmesi amacıyla el koyma işlemi gerçekleştirilmiştir.

Arama ve el koyma işlemi neticesinde, dijital materyallerin nerede, ne şekilde bulunduğu ve kim tarafından kullanıldığının ayrıntılı bir tespiti yapılarak, numaralandırma işlemi gerçekleştirilmek suretiyle el konulan dijital materyallerin

marka, model, seri numarası ve boyut bilgilerinin de yer aldığı ve arama esnasında bulunan görevliler, hazır bulunanlar, varsa ikamette bulunanlar ve şüphelinin de imzasının bulunduğu EK –2'de örnek olarak gösterilen "Arama ve El Koyma Tutanağı" mahallinde hazırlanarak taraflarca imza altına alınmıştır.

Senaryo gereği el konulan dijital materyallerden kısaca bahsetmek gerekirse,

- 1 Numaralı Delil; üzerinde el yazısı ile "DATA" ibresi yazılı bulunan DVD'yi,
- 2 Numaralı Delil; senaryo gereği sipariş edilen 16 GB kapasiteli bir USB belleği,
- 3 Numaralı Delil; arama esnasında kapalı vaziyette bulunan bir taşınabilir bilgisayar içerisinden sökülen 320 GB kapasiteli bilgisayar harddiski, ifade etmekte olup, el konulan materyallerin resimleri sırasıyla aşağıda gösterilmiştir.

Resim 5.1 1 Numaralı Delil.

Resim 5.2 2 Numaralı Delil.

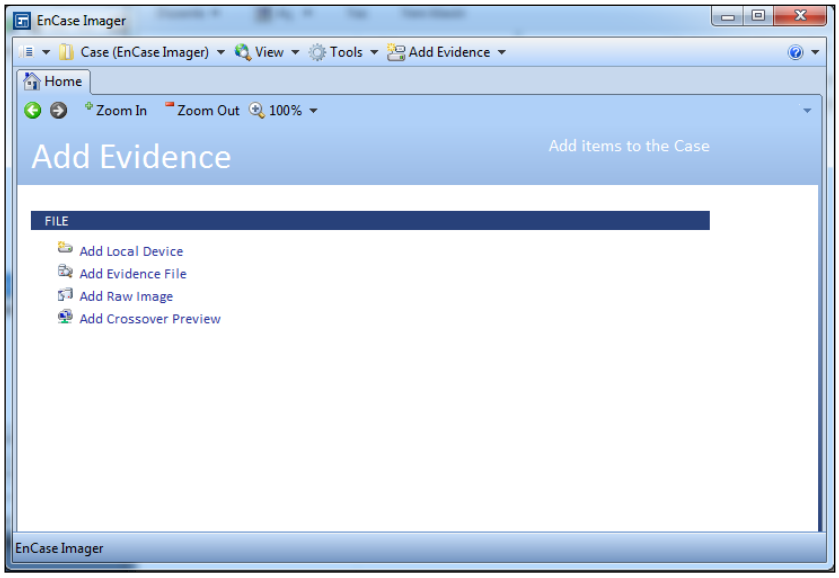
Resim 5.3 3 Numaralı Delil.

Adli bilişim alanında yapılan tüm inceleme ve analiz işlemleri, orijinalinde herhangi bir değişiklik meydana gelmemesi ve delil bütünlüğünün bozulmaması için delillerin birebir kopyaları üzerinde yapılması (Şirikçi ve Cantürk 2012) gerektiğinden; el konulan 3 adet dijital materyalin asılları üzerinden inceleme işlemi gerçekleştirilmeksizin imaj alma işlemleri yapılmıştır.

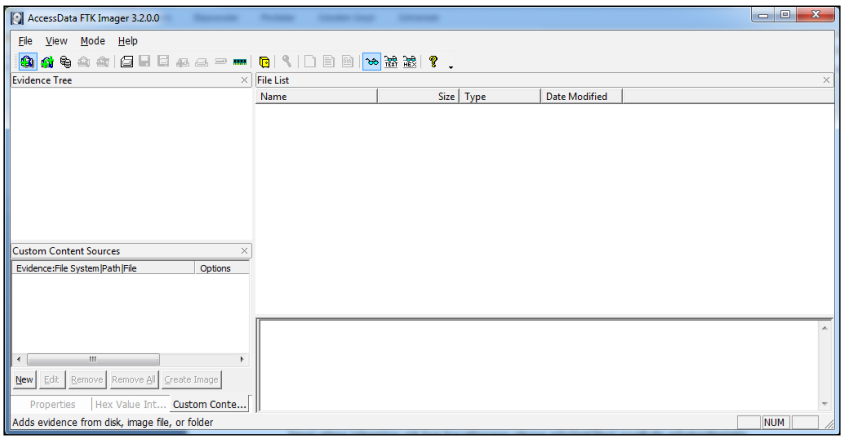
Uluslararası adli bilişim standartları gereği imaj alma işlemi esnasında, (İnt.Kyn. 23)'den

temin edilen yazılımsal Write Block (Yazma Koruma Engellemesi) ile, el konulan delillerin imaj alınacak olan bilgisayara bağlandığı andan itibaren, içerisinde bulunan verilerde herhangi bir değişikliğe ve yazma işlemine maruz kalması engellenmiştir. Aksi takdirde imaj alma işlemi gerçekleştirilecek olan bilgisayarda virüs, trojen vb. casus yazılım bulunuyor ise, aynı yazılımların delillere bulaşma riski çok yüksek olacak ve delil bütünlüğü bozulmuş olacaktır.

Yazma koruma engellemesi alındıktan sonra, delillerin imaj alma işlemleri internet kullanıcılarına ücretsiz olarak sunulan AccessData firmasına ait FTK İmager (Ver. 3.2.0) ve Guidance Software firmasına ait EnCase İmager (Ver. 7.06) isimli adli bilişim programları vasıtasıyla alınmıştır. Programların ara yüzlerine ait ekran görüntüsü aşağıda gösterilmiştir.

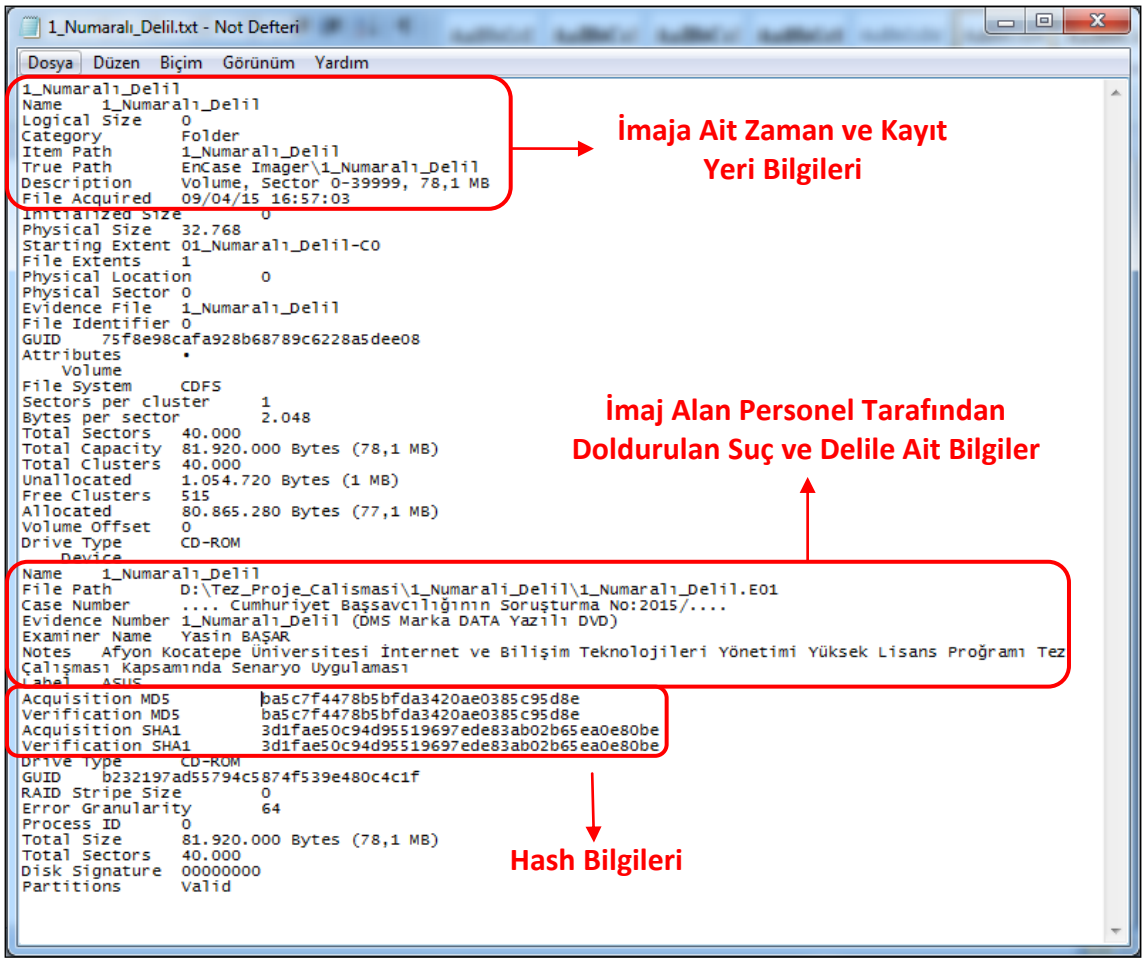


Resim 5.4 EnCase İmager Programının Ara Yüzü.

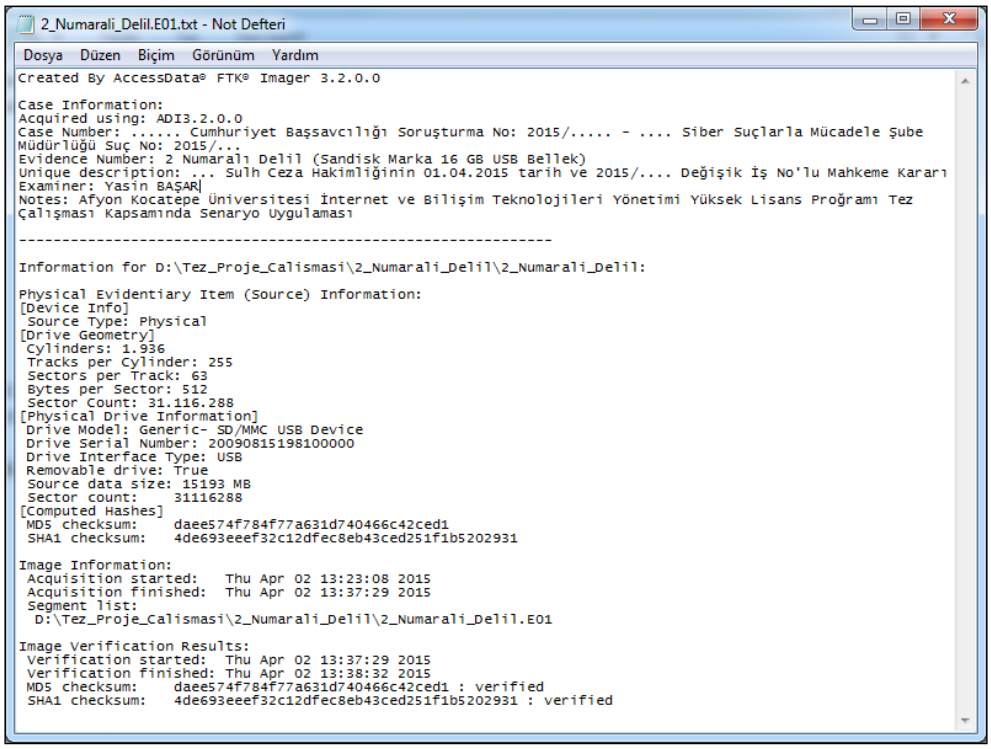


Resim 5.5 FTK İmager Programının Ara Yüzü.

İmaj alma tamamlandıktan sonra, imaja ait bilgilerin yer aldığı dosya “.txt” formatında imaj dosyalarının kopyalandığı klasör içerisine kaydolur ve inceleme işlemi esnasında, inceleme işlemini gerçekleştirecek olan uzman personele imajın ne zaman başlayıp ne zaman bittiği, imaj alınan cihazın özellikleri, hash değerleri vb. şekilde özet bilgi verir. 3 adet delilin imaj alma işlemine ait log kayıtlarının ekran görüntüleri aşağıda gösterilmiştir.



Resim 5.6 1 Numaralı Delile Ait Log Dosyası.

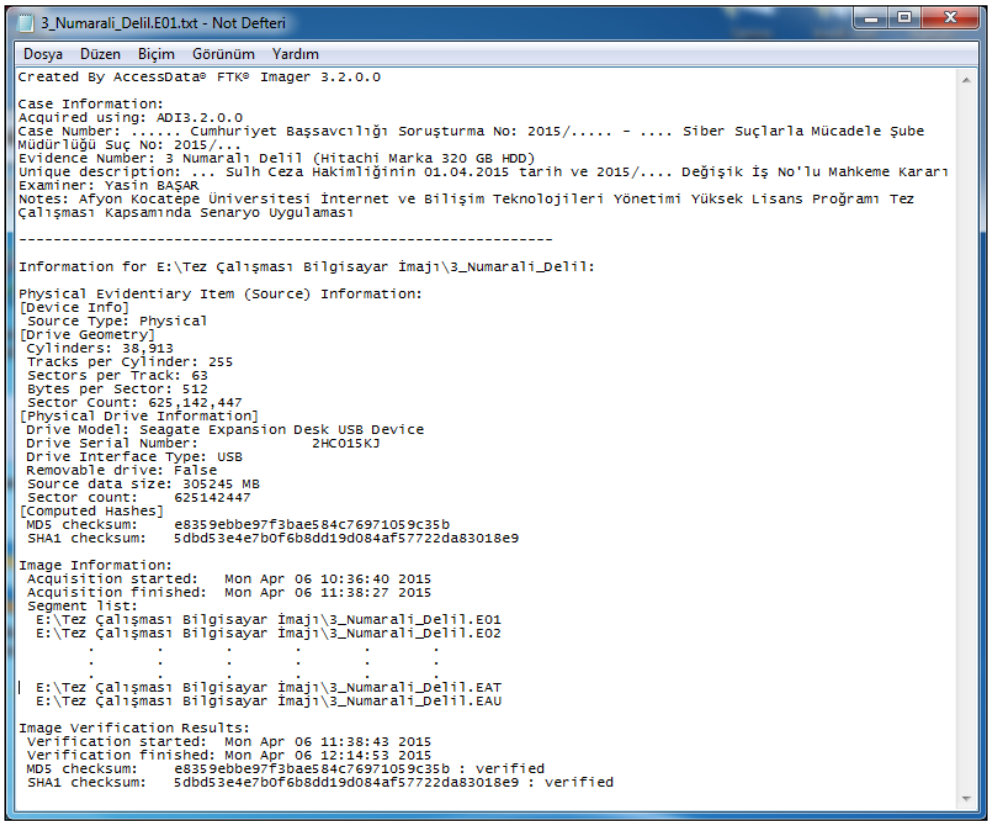


2_Numarali_Delil.E01.txt - Not Defteri

Dosya Düzen Biçim Görünüm Yardım

```
Created By AccessData® FTK® Imager 3.2.0.0

Case Information:
Acquired using: ADI3.2.0.0
Case Number: ..... Cumhuriyet Başsavcılığı Soruşturma No: 2015/..... - .... Siber Suçlarla Mücadele Şube
Müdürlüğü Suç No: 2015/...
Evidence Number: 2 Numaralı Delil (Sandisk Marka 16 GB USB Bellek)
Unique description: ... Sulh Ceza Hakimliğinin 01.04.2015 tarih ve 2015/.... Değişik İş No'lu Mahkeme Kararı
Examiner: Yasin BAŞAR
Notes: Afyon Kocatepe Üniversitesi İnternet ve Bilişim Teknolojileri Yönetimi Yüksek Lisans Proğramı Tez
Çalışması Kapsamında Senaryo Uygulaması

------------------------------------------------------------

Information for D:\Tez_Proje_Calismasi\2_Numarali_Delil\2_Numarali_Delil:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1.936
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 31.116.288
[Physical Drive Information]
 Drive Model: Generic- SD/MMC USB Device
 Drive Serial Number: 20090815198100000
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 15193 MB
 Sector count:    31116288
[Computed Hashes]
 MD5 checksum:    daee574f784f77a631d740466c42ced1
 SHA1 checksum:   4de693eeef32c12dfec8eb43ced251f1b5202931

Image Information:
 Acquisition started:   Thu Apr 02 13:23:08 2015
 Acquisition finished:  Thu Apr 02 13:37:29 2015
 Segment list:
  D:\Tez_Proje_Calismasi\2_Numarali_Delil\2_Numarali_Delil.E01

Image Verification Results:
 Verification started:  Thu Apr 02 13:37:29 2015
 Verification finished: Thu Apr 02 13:38:32 2015
 MD5 checksum:    daee574f784f77a631d740466c42ced1 : verified
 SHA1 checksum:   4de693eeef32c12dfec8eb43ced251f1b5202931 : verified
```

Resim 5.7 2 Numaralı Delile Ait Log Dosyası.



3_Numarali_Delil.E01.txt - Not Defteri

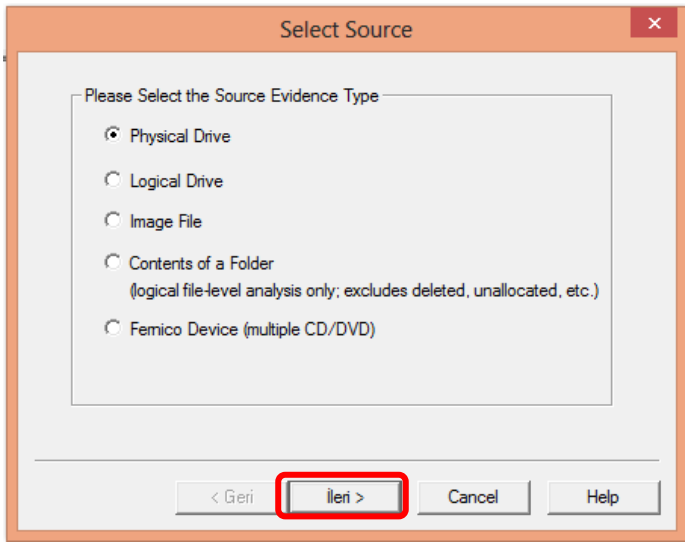
Dosya Düzen Biçim Görünüm Yardım

```
Created By AccessData® FTK® Imager 3.2.0.0

Case Information:
Acquired using: ADI3.2.0.0
Case Number: ..... Cumhuriyet Başsavcılığı Soruşturma No: 2015/..... - .... Siber Suçlarla Mücadele Şube
Müdürlüğü Suç No: 2015/...
Evidence Number: 3 Numaralı Delil (Hitachi Marka 320 GB HDD)
Unique description: ... Sulh Ceza Hakimliğinin 01.04.2015 tarih ve 2015/.... Değişik İş No'lu Mahkeme Kararı
Examiner: Yasin BAŞAR
Notes: Afyon Kocatepe Üniversitesi İnternet ve Bilişim Teknolojileri Yönetimi Yüksek Lisans Proğramı Tez
Çalışması Kapsamında Senaryo Uygulaması

------------------------------------------------------------

Information for E:\Tez Çalışması Bilgisayar İmajı\3_Numarali_Delil:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 38,913
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 625,142,447
[Physical Drive Information]
 Drive Model: Seagate Expansion Desk USB Device
 Drive Serial Number:           2HC015KJ
 Drive Interface Type: USB
 Removable drive: False
 Source data size: 305245 MB
 Sector count:    625142447
[Computed Hashes]
 MD5 checksum:    e8359ebbe97f3bae584c76971059c35b
 SHA1 checksum:   5dbd53e4e7b0f6b8dd19d084af57722da83018e9

Image Information:
 Acquisition started:   Mon Apr 06 10:36:40 2015
 Acquisition finished:  Mon Apr 06 11:38:27 2015
 Segment list:
  E:\Tez Çalışması Bilgisayar İmajı\3_Numarali_Delil.E01
  E:\Tez Çalışması Bilgisayar İmajı\3_Numarali_Delil.E02
       .       .       .       .       .       .
       .       .       .       .       .       .
       .       .       .       .       .       .
  E:\Tez Çalışması Bilgisayar İmajı\3_Numarali_Delil.EAT
  E:\Tez Çalışması Bilgisayar İmajı\3_Numarali_Delil.EAU

Image Verification Results:
 Verification started:  Mon Apr 06 11:38:43 2015
 Verification finished: Mon Apr 06 12:14:53 2015
 MD5 checksum:    e8359ebbe97f3bae584c76971059c35b : verified
 SHA1 checksum:   5dbd53e4e7b0f6b8dd19d084af57722da83018e9 : verified
```

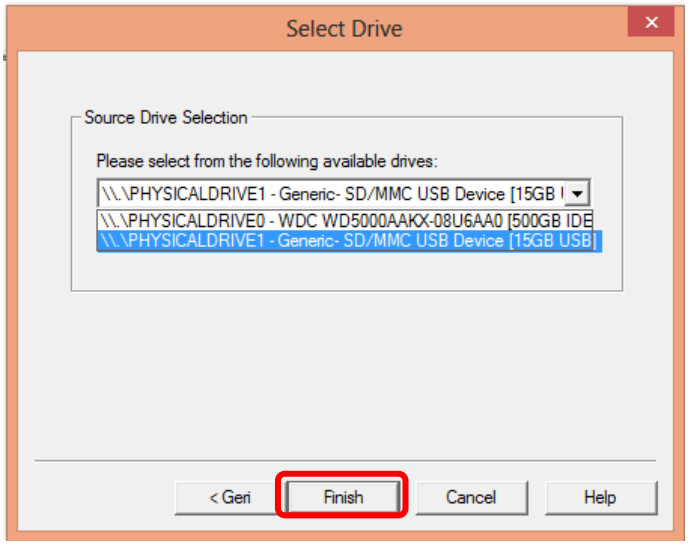
Resim 5.8 3 Numaralı Delile Ait Log Dosyası.

Yukarıda gösterilen delillere ait log dosyalarından anlaşılacağı üzere, imaj alma işleminin sıkıntısız tamamlandığı ve MD5 - SHA1 formatındaki hash değerlerinin değişmediği ve doğrulama işleminin tamamlandığı, yani delil bütünlüğünün bozulmadığı görülmektedir. İmaj alma işleminde herhangi bir aksaklıkla karşılaşılmamasından sonra, alınan 3 adet imaj dosyasının düzgün çalışıp çalışmadığının kontrolünü yapmak amacıyla, imajlar sırasıyla FTK İmager programı vasıtası ile açılmış ve imajların çalıştığı görülmesi üzerine EK – 3'te gösterilen "Adli Kopya (İmaj) Alma Tutanağı" tanzim edilmiştir.

Çalışma esnasında, 2 numaralı delilin imajı FTK İmager programı ile alınmış ve imaj alma işleminden elde edilen ekran görüntüleri örnek olarak sırasıyla aşağıda gösterilmiştir.

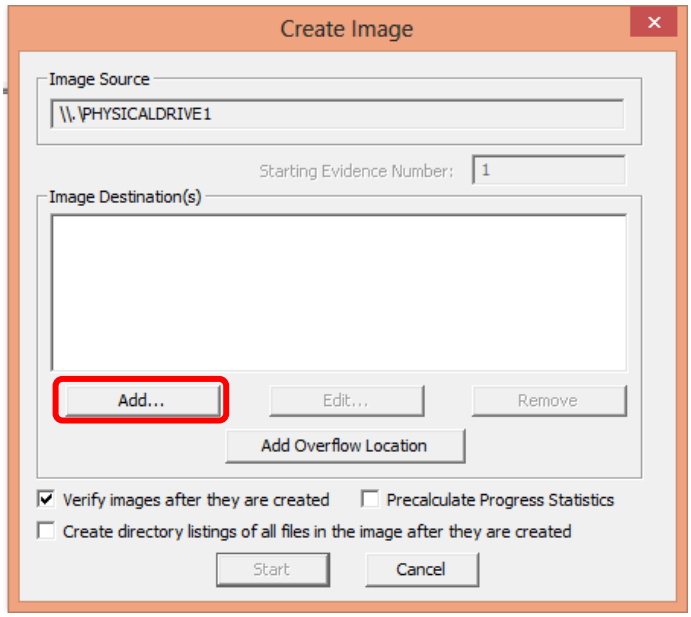


Resim 5.9 Kaynak Seçme (Select Source).



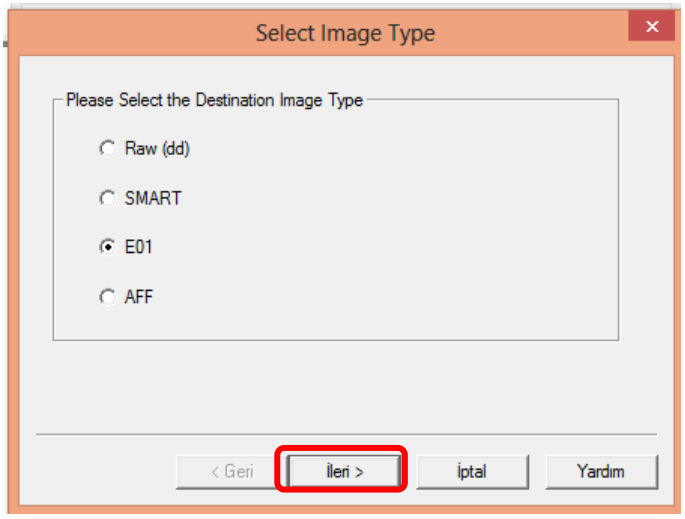
Resim 5.10 Sürücü Seçme (Select Drive).

FTK İmager programı açıldıktan sonra "Create Disk İmage" seçeneği tıklanır ve Resim 5.9'da bulunan ekran ile karşılaşılır. İmaj, bit-to-bit yani bire bir olarak alınması gerektiğinden "Physical Drive" seçeneği işaretlenerek fiziksel sürücülerin seçileceği Resim 5.10'daki ekranın gelmesi sağlanır. Bilgisayarda takılı bulunan fiziksel sürücülerden imajı alınacak olan sürücü seçilerek "Finish"e tıklanır.

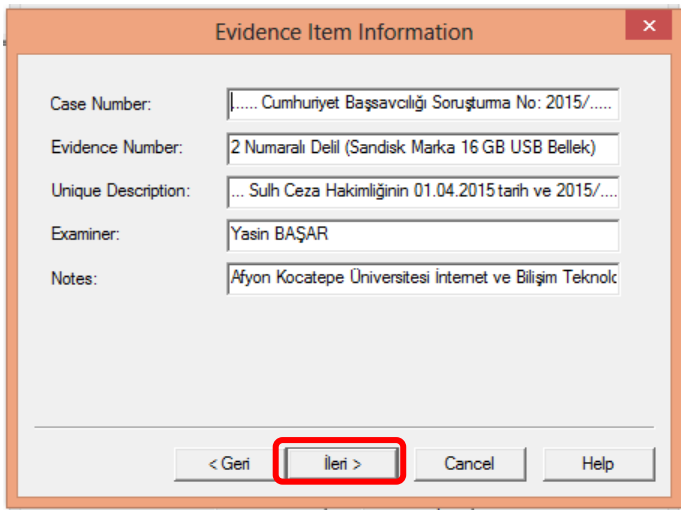


Resim 5.11 İmaj Oluşturma (Create Image).

İmaj kaynağı olan sürücü seçildikten sonra, Resim 5.11'de gösterilen ekran görüntüsündeki "Add…" seçeneği tıklanarak imaj ile ilgili bilgilerin seçileceği ekranlar karşımıza çıkar.

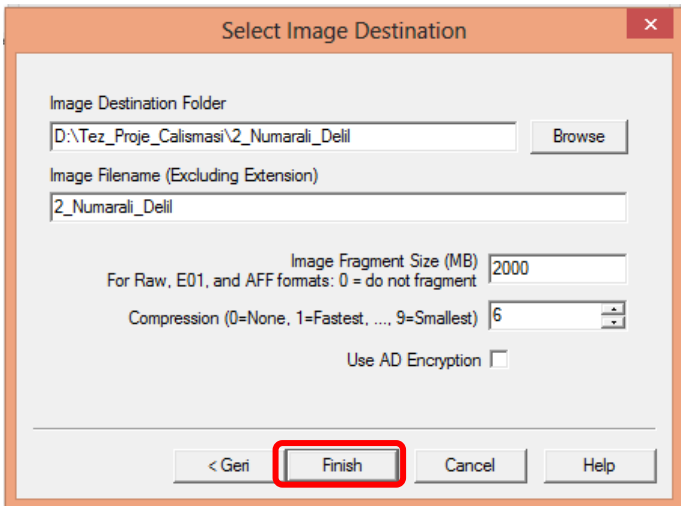


Resim 5.12 İmaj Tipi Seçme (Select Image Type).

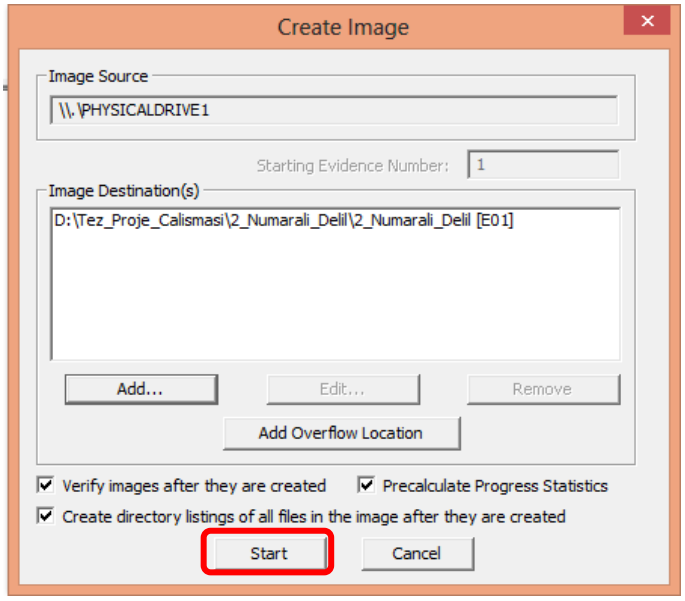


Resim 5.13 Delil Bilgisi (Evidence Item Information).

Resim 5.12'de gösterilen 4 adet imajın tipinden en sık kullanılan "E01" seçeneği işaretlenerek "İleri"ye tıklanır. Resim 5.13'de gösterilen bir sonraki seçenekte imaja konu olan suç ile ilgili ayrıntılı ve incelemeyi yapacak olan uzman personel için gerekli bilgiler doldurularak "İleri"ye tıklanır.

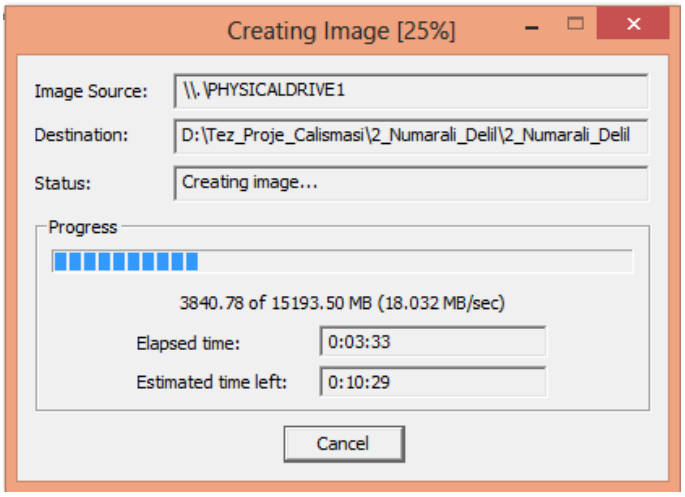


Resim 5.14 Hedef İmajı Seçme (Select Image Destination).

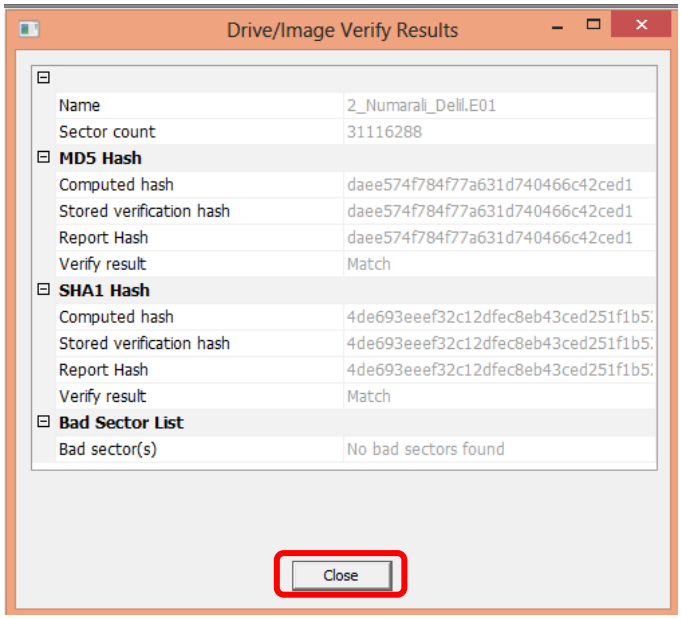


Resim 5.15 İmaj Oluşturma (Create Image).

Resim 5.14'de gösterilen bölümde imajın kopyalanacağı hedef klasör, imajın dosya ismi, imaj boyutu ve sıkıştırma oranı ayarlandıktan sonra "Finish"e tıklanarak imaj oluşturma işlemleri tamamlanır. Resim 5.15'de gösterilen "Verify images after they ara created", "Precalculate Progress Statistics" ve "Create directory listings of all files in the image after they are created" seçenekleri seçildikten sonra "Start"a tıklanarak imaj alma işlemi başlatılır.



Resim 5.16 İmaj Oluşturuluyor (Creating Image).

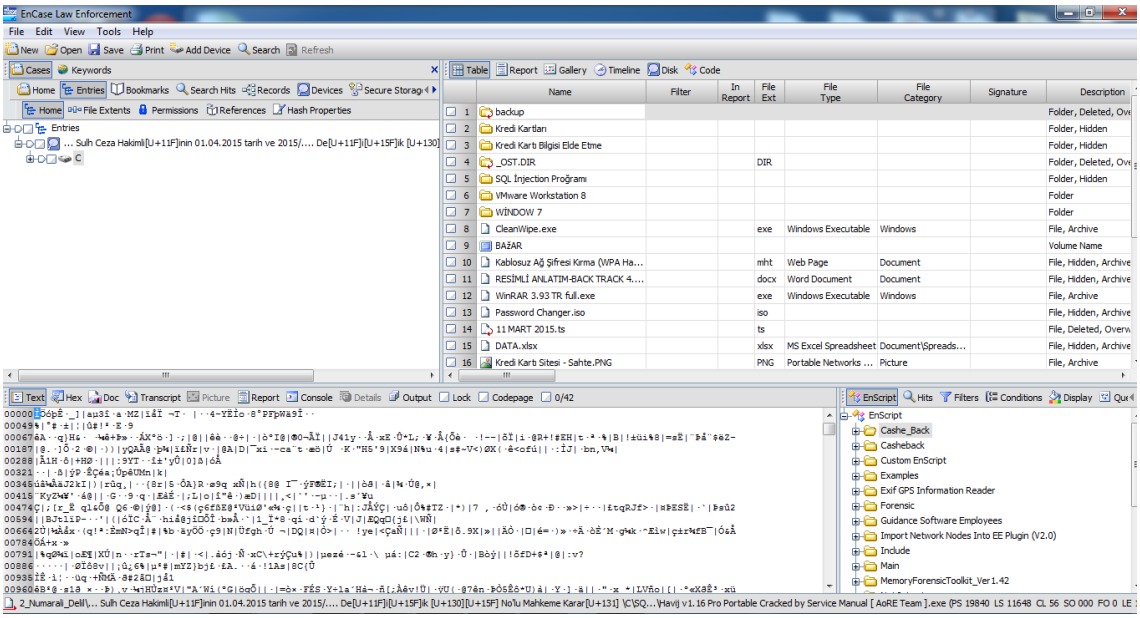


Resim 5.17 Sürücü/İmaj Doğrulama Sonuçları (Drive/Image Verify Results).

Resim 5.16'da imaj alma esnasındaki kullanıcıya gösterilen bilgi ekranı gösterilmiş ve Resim 5.17'de ise, imajın tamamlanmasının ardından MD5 ve SHA1 hash değerleri ile imajın doğrulandığını gösterir ekran görüntüsü ile karşılaşıldıktan sonra, "Close"a tıklanarak imaj alma işlemi sonuçlandırılır.

Alınan imaj dosyaları EnCase Forensic (Ver. 6.19) yazılımı ile incelenmek üzere açılarak

tekrar Verifing (Doğrulama) yapması sağlanmış, 1 ve 2 numaralı imaj dosyaları yalnız veri depolamaya yarayan materyaller olduğundan dolayı, doğrulama sonrasında içerisinde kayıtlı bulunan dosya ve klasörler (gizlenmiş – silinmiş dosya ve klasörler ile birlikte) Export (Dışarı Çıkarma) edilmiştir. Her iki materyale ait imaj içerisinde silinmiş dosyaların kurtarılması işlemi gerçekleştirilmiş ve gizli klasörlerin tespiti yapılarak, suç unsuru olduğu değerlendirilen bilgi, belge, resim ve programların özelliklerini belirtir ayrıntılar ile birlikte inceleme raporuna eklenmiştir. EnCase Forensic yazılımının senaryo kapsamındaki incelemeye ait kullanıcı ara yüz ekran görüntüsü Resim 5.18'de gösterilmiştir.



Resim 5.18 EnCase Forensic Yazılımının İnceleme Esnasındaki Ara Yüzü.

3 numaralı imaj dosyası, laptop tabir edilen taşınabilir bilgisayardan sökülen içerisinde işletim sistemi kurulu bir harddiske ait olduğundan dolayı, inceleme esnasında farklı işlemler uygulanmıştır. Uygulanan işlemlerden bahsedecek olursak, imaj doğrulama yaptıktan sonra bilgisayarda kurulu bulunan işletim sistemi bilgilerinin tespit edilerek en son ne zaman yüklendiği, bilgisayarın en son ne zaman kapatıldığı vb. bilgiler tespit edilmiştir. Daha sonra silinmiş dosyaların tespiti amacıyla Recovery (Kurtarma) işlemi gerçekleştirilerek silinmiş veriler üzerinden delil elde edilmeye çalışılmıştır. İmaj

içerisinde kayıtlı olan tüm bilgi, belge, dosya ve klasörlerin kontrolü yapılmış ve suç unsuru olduğu değerlendirilen dosya ve klasörlerin özellikleri tespit edilerek Export edilmiştir.

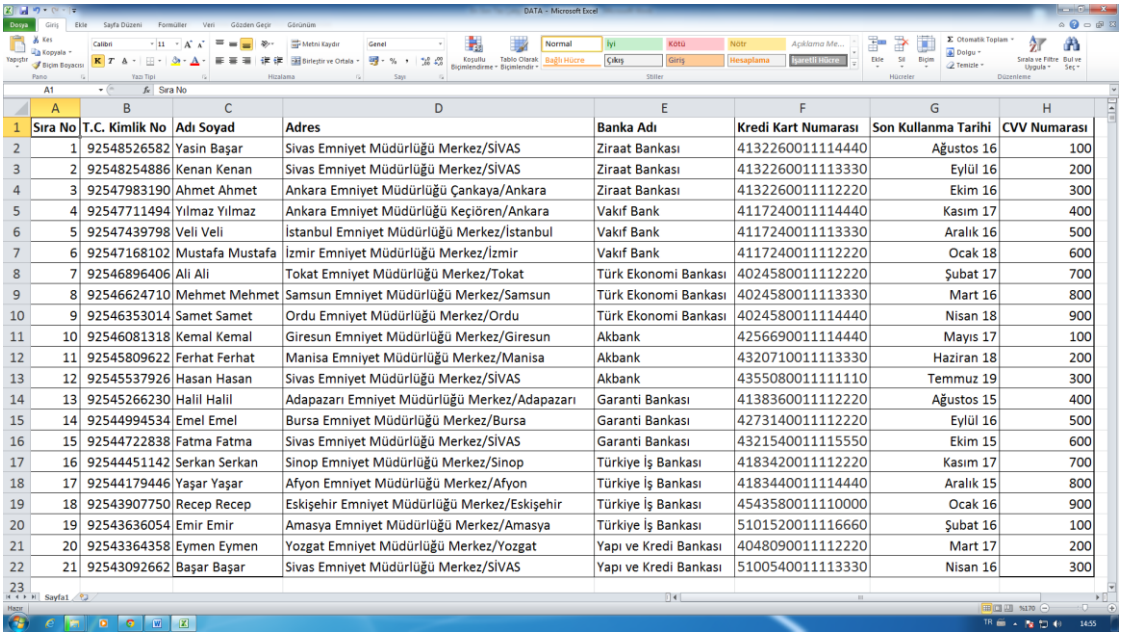
Bilgisayarda kullanılmış olan tüm IP numarası bilgilerinin tespiti yapılmış ve senaryo gereği alışveriş esnasında kullanılan ve soruşturma kapsamında tespiti yapılan IP numarası ve mail adresinin bu bilgisayar tarafından kullanılıp kullanılmadığı tespit edilmeye çalışılmıştır. (İnt.Kyn. 24)'ten temin edilen Türkiye'de faaliyet gösteren bankaların kullanmakta oldukları kredi ve bankamatik kart numaralarının ilk altı hanesi (BIN Listesi), EnCase Forensic yazılımı üzerinden "qrep" hazırlama yöntemiyle keyword (anahtar kelime) taraması yapılarak çıkan sonuçlar değerlendirilmiş ve senaryoda kullanılan kredi kartı bilgisi ile ilgili olanlar suç unsuru olarak Export edilmiştir.

Senaryo kapsamında el konulan 1, 2 ve 3 numaralı delillerin incelemesi neticesinde, suça konu elde edilen delillerin bir kısmı EK – 4'te gösterilen "İnceleme Raporu"nda ve tamamı ise, Delil DVD'sinde belirtilerek çalışma sonuçlandırılmıştır.

6. BULGULAR

Senaryo gereği yapılan 1 numaralı delilin incelemesinde, üzerinde işletim sistemi barındırmayan depolama amaçlı kullanılan dijital materyal olduğundan dolayı, materyalin içerisinde kayıtlı bulunan gizli ve kayıtlı bulunan dosya ve klasörlerin incelemesi yapıldıktan sonra suç unsuru olduğu değerlendirilen bilgi ve belgelerin inceleme işlemi yapılmış ve elde edilen deliller EK-4'de bulunan inceleme raporuna eklenmiştir.

1 numaralı delilin incelemesi kapsamında, delil içerisinde kayıtlı bulunan ve suç unsuru olduğu değerlendirilen dosya ve klasörlerin, delil içerisinde gizlenmiş bir şekilde kayıtlı olduğu görülmüş ve yüklenme tarihi, son erişim tarihi, hash bilgileri vb. ayrıntıları tespit edilerek inceleme raporuna delil olarak eklenmiştir. 1 numaralı delilden elde edilen deliller incelendiğinde, web sitesi hackleme yöntemlerinde kullanılan "Havij", IP numarası değiştirme işleminde kullanılan "ProxySwitcher" ve hackleme sonrasında bilgisayarın kayıt defterine düşen bilgilerin temizlemesinde kullanılan "Registrar Lite" isimli programların kayıtlı olduğu ve içerisinde çok sayıda kredi kartı ile açık kimlik bilgisinin kayıtlı olduğu anlaşılan "DATA.xlsx" isimli Microsoft Excel dosyası tespit edilmiş ve örnek olarak ekran görüntüsü aşağıda gösterilmiştir. Ayrıca delil içerisinde hackleme ile ilgili doküman ve kredi kartı bilgileri ile ilgili resimler tespit edilmiştir.



Sıra No	T.C. Kimlik No	Adı Soyad	Adres	Banka Adı	Kredi Kart Numarası	Son Kullanma Tarihi	CVV Numarası
1	92548526582	Yasin Başar	Sivas Emniyet Müdürlüğü Merkez/SİVAS	Ziraat Bankası	4132260011114440	Ağustos 16	100
2	92548254886	Kenan Kenan	Sivas Emniyet Müdürlüğü Merkez/SİVAS	Ziraat Bankası	4132260011113330	Eylül 16	200
3	92547983190	Ahmet Ahmet	Ankara Emniyet Müdürlüğü Çankaya/Ankara	Ziraat Bankası	4132260011112220	Ekim 16	300
4	92547711494	Yılmaz Yılmaz	Ankara Emniyet Müdürlüğü Keçiören/Ankara	Vakıf Bank	4117240011114440	Kasım 17	400
5	92547439798	Veli Veli	İstanbul Emniyet Müdürlüğü Merkez/İstanbul	Vakıf Bank	4117240011113330	Aralık 16	500
6	92547168102	Mustafa Mustafa	İzmir Emniyet Müdürlüğü Merkez/Izmir	Vakıf Bank	4117240011112220	Ocak 18	600
7	92546896406	Ali Ali	Tokat Emniyet Müdürlüğü Merkez/Tokat	Türk Ekonomi Bankası	4024580011112220	Şubat 17	700
8	92546624710	Mehmet Mehmet	Samsun Emniyet Müdürlüğü Merkez/Samsun	Türk Ekonomi Bankası	4024580011113330	Mart 16	800
9	92546353014	Samet Samet	Ordu Emniyet Müdürlüğü Merkez/Ordu	Türk Ekonomi Bankası	4024580011114440	Nisan 18	900
10	92546081318	Kemal Kemal	Giresun Emniyet Müdürlüğü Merkez/Giresun	Akbank	4256690011114440	Mayıs 17	100
11	92545809622	Ferhat Ferhat	Manisa Emniyet Müdürlüğü Merkez/Manisa	Akbank	4320710011113330	Haziran 18	200
12	92545537926	Hasan Hasan	Sivas Emniyet Müdürlüğü Merkez/SİVAS	Akbank	4355080011111110	Temmuz 19	300
13	92545266230	Halil Halil	Adapazarı Emniyet Müdürlüğü Merkez/Adapazarı	Garanti Bankası	4138360011112220	Ağustos 15	400
14	92544994534	Emel Emel	Bursa Emniyet Müdürlüğü Merkez/Bursa	Garanti Bankası	4273140011112220	Eylül 16	500
15	92544722838	Fatma Fatma	Sivas Emniyet Müdürlüğü Merkez/SİVAS	Garanti Bankası	4321540011115550	Ekim 15	600
16	92544451142	Serkan Serkan	Sinop Emniyet Müdürlüğü Merkez/Sinop	Türkiye İş Bankası	4183420011112220	Kasım 17	700
17	92544179446	Yaşar Yaşar	Afyon Emniyet Müdürlüğü Merkez/Afyon	Türkiye İş Bankası	4183440011114440	Aralık 15	800
18	92543907750	Recep Recep	Eskişehir Emniyet Müdürlüğü Merkez/Eskişehir	Türkiye İş Bankası	4543580011110000	Ocak 16	900
19	92543636054	Emir Emir	Amasya Emniyet Müdürlüğü Merkez/Amasya	Türkiye İş Bankası	5101520011116660	Şubat 16	100
20	92543364358	Eymen Eymen	Yozgat Emniyet Müdürlüğü Merkez/Yozgat	Yapı ve Kredi Bankası	4048090011112220	Mart 17	200
21	92543092662	Başar Başar	Sivas Emniyet Müdürlüğü Merkez/SİVAS	Yapı ve Kredi Bankası	5100540011113330	Nisan 16	300

Resim 6.1 DATA.xlsx İsimli Microsoft Excel Dosyası İçeriği.

2 numaralı delilin incelemesinde, 1 numaralı delilde olduğu gibi üzerinde işletim sistemi barındırmayan depolama amaçlı kullanılan dijital materyal olduğundan dolayı, aynı işlemler bu delile de uygulanmış ve soruşturma kapsamında suç unsuru olduğu değerlendirilen bilgi ve belgelerin tespiti yapılarak inceleme raporuna eklenmiştir.

2 numaralı delilin incelemesi kapsamında, delil içerisinde kayıtlı bulunan ve suç unsuru olduğu değerlendirilen dosya ve klasörlerin, 1 numaralı delil içerisinde kayıtlı olan ve suç unsuru olarak tespiti yapılan dosya, klasör ve programların aynısının kayıtlı olduğu ve bunlar dışında ise, harddisk temizlemede kullanılan “CleanWipe”, web sitesi hacklemede kullanılan “Hakops SQL İnj. Scaner” ve sanal makine kurmada kullanılan “VMware Workstation 8” isimli programların yanı sıra, 4 adet farklı bankalara ait kredi kartlarının ön ve arka yüzlerinin bulunduğu resimler ve hackleme işlemlerinde kullanılan “Back Track” programının anlatıldığı belgenin kayıtlı olduğu görülmüştür. Ayrıca inceleme konusu kapsamında olmayan, Fikir ve Sanat Eserleri Kanununa göre suç unsuru olduğu değerlendirilen dosyalara rastlanılmış ve ayrıntılar inceleme raporunda belirtilmiştir. Kredi kartı ön ve arka yüzlerinin bulunduğu resimlerden bir tanesi örnek olarak aşağıda gösterilmiştir.

Resim 6.2 Kredi Kartı Ön ve Arka Yüzü.

3 numaralı delilin incelemesinde ise, 1 ve 2 numaralı delilden farklı olarak üzerinde işletim sistemi kurulu olan bir bilgisayar harddiski olduğundan dolayı, diğer delillerden birkaç farklı yöntem uygulanmıştır. Uygulanan yöntemlere sırası ile bakacak olursak;

- Sistem özelliklerinin tespiti,
- Bilgisayarda yüklü olan yazılımların tespiti,
- Silinmiş dosyaların kurtarılması,
- Ziyaret edilen web sitelerinin taranması,
- Kullanılan mail adreslerinin tespiti,
- Kullanılan IP numaralarının tespiti,
- Keyword taraması,
- Kayıtlı resim, belge ve dokümanların kontrolü vb.

Yukarıda bahsi geçen yöntemlerin kullanılması neticesinde, suç unsuru olduğu değerlendirilen dosya, klasör ve programların tespiti yapılarak inceleme raporunda ayrıntıları belirtilmiştir.

3 numaralı delilin incelemesi esnasında, imaj dosyalarından E36 ve E37 uzantılı olan dosyalar arızalanmış ve inceleme işlemi tamamlanamamıştır. Yapılan çalışmalar neticesinde imaj dosyalarının açılması sağlanamadığından dolayı, el konulan 3 numaralı delilin imajı tekrar alınmış ve hash bilgisi kontrol edildiğinde ise, hash bilgisinin değişmediği tespit edilmiştir.

3 numaralı delilin incelemesi kapsamında suçta kullanılan mail adresi, IP numarası ve sipariş işlemine ait bilgi ve belgeler tespit edilmiştir. Ancak sipariş işleminde kullanılan kredi kartı numarasına ait herhangi bir bilgi ve belgeye rastlanılmamıştır.

1, 2 ve 3 numaralı delillerin incelemesi neticesinde tespit edilen hususlar ayrıntılı bir şekilde hazırlanan ve EK-4'de bulunan inceleme raporuna eklenmiştir.

7. TARTIŞMA VE SONUÇ

Çalışma kapsamında yapılan inceleme neticesinde, tespiti yapılan bilgilerin soruşturmanın akıbeti açısından çok önemli bilgiler olduğu bilindiğinden, tespit edilen bilgiler ışığında şüphelinin suçu işlediği yönünde kesin delil elde etme imkanı sağlanmıştır. Adli bilişim teknikleri kullanılmasaydı, şüpheli şahıs yalnız IP numarası tespiti ile cezalandırılması hukuki olmayacağından dolayı, suçu işleyen cezasız kalacak ve adalet tecelli edemeyecekti. Kaldı ki, adli bilişim incelemelerinin sadece siber suç soruşturmalarında değil klasik suç türlerinde de kullanılmasının soruşturmaya yarar sağlayacağı değerlendirilmiştir.

Adli bilişim tekniklerinin, klasik suçlar olarak tanımlanan mağdur ve şüphelinin aynı ortamda bulunduğu suç türleri ile mücadele eden tüm kolluk kuvvetlerinin yürütmekte oldukları soruşturmalarda kullanılması, soruşturmanın seyrini değiştirecek sonuçların elde edilmesini sağlayacaktır. Örneğin; cinayet suçu soruşturması yürüten kolluk kuvvetlerinin, maktul ya da suça karıştığı değerlendirilen kişilerin kullanmakta oldukları bilgisayar ve bilgisayar kütüklerinde yapacakları inceleme işlemi neticesinde, katilin yakalanmasını sağlayacak çok önemli deliller elde edebileceklerdir. Bu sebeple, adli bilişim tekniklerinin kullanılmasının ne kadar önemli olduğu, suç soruşturması alanında çalışan tüm kolluk kuvvetleri tarafından bilinmesi gerektiği değerlendirilmiştir.

Adli bilişim incelemeleri, son zamanlarda çok popüler bir hale gelen yeni delil elde etme yöntemlerinden olmakla birlikte, delilin somut olmaması inandırıcılığı ve güvenilirliği açısından tereddütler oluşturmaktadır. Bu tereddütlerin ortadan kaldırılması ve suç işleyen kişilerin yaptıklarının yanına kar kalmaması için, dijital ortamda elde edilen delil zincirinin adli makamlara ayrıntılı ve anlaşılır bir biçimde izah edilmesi gerekmektedir. Aksi halde, adli makamlar tarafından anlaşılırlığı olmayan delilden sanık faydalanacaktır.

Adli bilişimin tüm süreçlerinde yapılan işlemler muhakkak yazınsal ya da görsel bir

şekilde kayıt altına alınmalı ve işlemler sırası ile eksiksiz bir biçimde tamamlanarak adli makamlara sunulan delilin herkes tarafından anlaşılır bir dille izah edilmesi sağlanmalıdır. Adli bilişim incelemelerinde elde edilen deliller somut olmadığından, herkes tarafından anlaşılabilmesi beklenmemeli, ancak teknik bir anlatım yerine herkes tarafından anlaşılacak bir dil kullanılmalıdır.

İnceleme işlemleri esnasında takip edilen aşamalarda, uluslar arası adli bilişim standartlarına uygun bir şekilde hareket edilmesi, delilin güvenilirliğini ve anlaşılabilirliğini artıracaktır. İnceleme yapan personel kendisini bu alanda meydana gelen tüm gelişmelere açık tutmalı ve devamlı eğitimlerle desteklenmelidir. Her geçen gün daha ileriye giden teknolojiye ayak uydurmayan bir personel, zamanla körelecek ve yaptığı incelemeler eksik kalacaktır.

Adli bilişim incelemelerinde dikkat edilmesi gereken bir hususta, imaj alma işlemi gerçekleştirilmeden önce, şüpheli şahıs ya da vekili talep etse dahi hash değeri hesaplatma yöntemi ile tespit edilen hash değerleri verilmemeli, aksi takdirde delili taşıma ya da imaj alma esnasında oluşacak en ufak bir darbe ya da sektör hatası nedeniyle hash değeri değişecek ve delil hükmünü kaybetmesine yol açacaktır. Böyle bir taleple karşılaşıldığında, yerinde imaj alma imkanı varsa, imaj alma işlemi tamamlandıktan sonra elde edilen hash değerinin tutanağa bağlanmak suretiyle verilmesi, yerinde imaj alma imkanı bulunmayan bir ortamda ise, el koyma işlemi sonrasında laboratuar ortamında gerçekleştirilecek imaj alma işlemine şüpheli ya da vekili dahil edilerek imaj alma işlemine refakati sağlanmalıdır.

Gerek adli bilişimin olmazsa olmaz olarak kullanıldığı siber suç soruşturmalarında, gerekse klasik suç soruşturmalarında, dijital delilin uçuculuğu göz önünde bulundurularak en kısa zamanda gerekli adli izinlerin alınarak müdahale edilmesi gerekmektedir. Aksi halde, şüpheli kullanmakta olduğu dijital materyalleri ya da bu materyaller üzerinde bulunan bilgi ve belgeleri çok kısa bir süre içerisinde geri getirilemez şekilde silebilecek ve soruşturma kapsamında dijital delil elde etme imkanı

ortadan kalkacaktır.

Senaryo kapsamında yapılan çalışma esnasında, imaj dosyalarında meydana gelen arızadan dolayı imaj üzerinde inceleme işlemine devam edilemediğinden, el konulan harddiskin imajı tekrar alınması ihtiyacı ortaya çıkması üzerine, çalışma kapsamında 3 numaralı delilin tekrar imaj alma işlemi gerçekleştirilmiştir. Böyle bir durumla karşılaşılması halinde, ya şüpheli şahsa teslim edilen imaj üzerinde inceleme işlemine devam edilmesi gerekecek ya da yeniden imaj almak gerekecektir. Hali hazırda devam etmekte olan uygulamada, CMK 134. maddesinin 2. Fıkrasına istinaden, el konulan materyalin gerekli kopyasının alınması halinde, el konulan cihazlar gecikme olmaksızın şüpheli şahsa iade edilmektedir. Bu çalışmada anlaşılmıştır ki, inceleme işlemi tamamlanıncaya kadar el konulan materyallerin tekrar imaj alma ihtiyacı ortaya çıkabileceğinden, en azından inceleme işlemi tamamlanıncaya kadar asıl delilin şüpheli şahsa iade edilmemesi gerekmektedir.

İnceleme aşamasında ise, her soruşturmada olduğu gibi gizlilik en üst seviyede sağlanmalı, inceleme yapan uzman personel dışında delilin inceleme işlemi hiçbir personel tarafından ulaşılması engellenmelidir. Her ne kadar bir suç soruşturması kapsamında anayasanın belirtmiş olduğu izinler çerçevesinde şüphelinin özel hayatına müdahale edilse de, suç ile alakası olmayan ve şüphelinin özel hayatına ilişkin bilgi ve belgeler kullanmakta oldukları dijital materyallerde depolanmaktadır. İnceleme yapan uzman personel profesyonelliği elinden bırakmadan, öncelikle suç konusu ile ilgili incelemesini yapmalı, tesadüfen elde edilen delil olması halinde ise, gecikmeksizin soruşturmayı yürüten Cumhuriyet Savcısına bilgi vermeli ve verilen talimata göre hareket etmesi gerekmektedir. Aksi takdirde, inceleme esnasında elde edilen bilgilerin yetkisiz kişilerin eline geçmesi, dönüşü mümkün olmayan sonuçlarla karşılaşılmasına sebep olabilecektir.

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.

Bu çalışmada web sitesinin yazılım dilinden kaynaklandığı değerlendirilen sebeplerden dolayı, “qrep” ve “keyword” taraması neticesinde alışveriş işleminde kullanılan kredi kartı bilgisi ile ilgili herhangi bir sonuca ulaşılamamıştır. Kredi kart bilgisinin kullanılıp kullanılmadığı yönündeki kesin bilginin, işlem sonrasında RAM (Random Access Memory – Rastgele Erişimli Hafıza) imajının alınması neticesinde elde edilebileceği değerlendirilmektedir. RAM hafızası geçici olduğundan dolayı web sitesi kayıtlarında bulunmayan kayıtlar, RAM üzerinde olan bilgilerden elde edilebilecektir. Ancak RAM hafızası kalıcı olmadığından ve bilgisayar kapatıldıktan kısa bir süre sonra kaybolacağından bu yöntemle delil elde etme imkanı da oldukça zor olmaktadır. Bu sebeple adli bilişim yöntemleri uygulanacak suç türü iyi analiz edilmeli ve her suç türüne göre delile müdahale edilmelidir. Banka ve/veya Kredi Kartlarının Kötüye Kullanılması suçunda olay yerinde canlı imaj ve aynı zamanda RAM imajını almak hayati önem taşımaktadır.

8. KAYNAKLAR

Aydın, E.D. (1992). Bilişim Sistemlerinde, Güvenlik, Güvenilirlik, Mahremiyet ve Bilişim Suçları. *Marmara İletişim Dergisi*, **1:**109-137.

Aytekin, A., Kılıç, M.S. ve Çakır H. (2014). Karşılaştırmalı Hukuk Açısından Siber Suçlar. Edit: Çakır H. ve Kılıç M.S., Güncel Tehdit: Siber Suçlar, Seçkin Yayıncılık, Ankara, 181-202.

Bakan, M. ve Saluk, A. (2014). Adli Bilişimde Kullanılan Ekipmanlar. Edit: Çakır H. ve Kılıç M.S., Adli Bilişim ve Elektronik Deliller, Seçkin Yayıncılık, Ankara, 199-267.

Benzer, R. (2014). Siber Suçlar ve Teorik Yaklaşımlar. Edit: Çakır H. ve Kılıç M.S., Güncel Tehdit: Siber Suçlar, Seçkin Yayıncılık, Ankara, 21-39.

Bilek, B.T. (2012). Bilişim Suçları ve Üniversite Lisans Öğrencilerinin Bilişim Suçlarına Yönelik Görüşleri. Yüksek Lisans Tezi. Gazi Üniversitesi, Bilişim Enstitüsü, Ankara.

Bilgi Teknolojileri ve İletişim Kurumu (2014). Üç Aylık Pazar Verileri Raporu, 2014 Yılı 3. Çeyrek (Temmuz-Ağustos-Eylül). Türkiye Elektronik Haberleşme Sektörü, Ankara.

Burkay, S. (2008). Teorik Çerçevede Suç. *ETHOS: Felsefe ve Toplumsal Bilimlerde Diyaloglar,* Sayı:2/4

Burlu, K. (2012). Bilişimin Karanlık Yüzü. Nirvana Yayınları, 3. Baskı, Ankara.

Burucu, E. ve Kuşoğlu, İ. (2014). Rapor Hazırlama. Edit: Çakır H. ve Kılıç M.S., Adli Bilişim ve Elektronik Deliller, Seçkin Yayıncılık, Ankara, 491-507.

Canbek, G. (2005). Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme. Yüksek Lisans Tezi. Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

Çakır, H. ve Doğan T. (2014). İnternet Üzerinden Dolandırıcılık. Edit: Çakır H. ve Kılıç M.S., Güncel Tehdit: Siber Suçlar, Seçkin Yayıncılık, Ankara, 97-134.

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

Çubukçu, A. (2014). İnternet Düzenlemeleri. Edit: Çakır H. ve Kılıç M.S., Güncel Tehdit: Siber Suçlar, Seçkin Yayıncılık, Ankara, 65-89.

Çubukçu, A. ve Bayzan, Ş. (2013). Türkiye'de Dijital Vatandaşlık Algısı ve Bu Algıyı İnternetin Bilinçli, Güvenli ve Etkin Kullanımı ile Artırma Yöntemleri. *Middle Eastern & African Journal of Educational Research*, **5:** 148-174.

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

Hekim, H. ve Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları. *Polis Akademisi Uluslararası Güvenlik ve Terörizm Dergisi*, **4 (2):** 135-158.

Henkoğlu, T. (2014). Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi. Pusula Yayıncılık, 2. Baskı, İstanbul.

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

Kılıç, M.S. (2014). Elektronik Deliller ve Yapısal Özellikleri. Edit: Çakır H. ve Kılıç M.S., Adli Bilişim ve Elektronik Deliller, Seçkin Yayıncılık, Ankara, 139-155.

Kiçeci, H. (2014). Bilgisayar Medyalarına İlk Müdahale. Edit: Çakır H. ve Kılıç M.S., Adli Bilişim ve Elektronik Deliller, Seçkin Yayıncılık, Ankara, 161-191.

Öztürk, M.İ. (2007). Bilişim Cihazlarındaki Sayısal Delillerin Tespiti ve Değerlendirilmesinde İş Akış Modelleri. Yüksek Lisans Tezi. Ankara Üniversitesi, Sağlık Bilimleri Enstitüsü, Ankara.

Say, K. (2006). Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanmasi ve Laboratuvarda İncelenmesi. Yüksek Lisans Tezi. Ankara Üniversitesi, Sağlık Bilimleri Enstitüsü, Ankara.

Seferoğlu, S.S. (2006). Öğretim Teknolojileri ve Materyal Tasarımı. Pegem A Yayıncılık, 3. Baskı, Ankara.

Sevli, O. ve Küçüksille U. (2013). Bulut Ortamında Adli Bilişim. 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı, 268-273.

Şirikçi, A.S. ve Cantürk, N. (2012). Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının Önemi. *Bilişim Teknolojileri Dergisi*, **5 (3):** 29-34.

Taşkın, Ş.C. (2008). Bilişim Suçları. Beta Yayıncılık, 1. Baskı, İstanbul.

Topaloğlu, N. (2014). Bilgisayar Mimarisi. Edit: Çakır H. ve Kılıç M.S., Adli Bilişim ve Elektronik Deliller, Seçkin Yayıncılık, Ankara, 25-91.

Uzunay, Y. ve Bıçakçı, K. (2005). A3D3M: Açık Anahtar Altyapısı Destekli Dijital Delilleri Doğrulama Modeli. ABG2005: National Network and Information Security Symposium, İstanbul, Haziran 2005.

İnternet Kaynakları

1. http://tr.wikipedia.org/wiki/Bilgisayar, 22/01/2015
2. http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.54c0c7b4b5c542.75370318, 22/01/2015
3. http://www.bilgisayarnedir.com/bilgisayarnedir.html, 22/01/2015
4. http://www.netmarketshare.com/downloads/guest635576092290800000.pdf, 23/01/2015
5. http://web.iku.edu.tr/~tkaynas/bgpp.pdf, 26/05/2015
6. http://tr.wikipedia.org/wiki/Bilgisayar_a%C4%9F%C4%B1, 23/01/2015
7. http://www.mtuncel.com/bilgisayaraglari.htm, 24/01/2015
8. http://tr.wikipedia.org/wiki/%C4%B0nternet#cite_noteWebster1, 24/01/2015
9. http://www.ipnumaram.com/ipadresi.html, 28/01/2015
10. http://tr.wikipedia.org/wiki/Alan_ad%C4%B1_(%C4%B0nternet), 29/01/2015
11. http://archive.icann.org/en/tlds/, 28/01/2015
12. http://tr.wikipedia.org/wiki/Bar%C4%B1nd%C4%B1rma_hizmeti, 29/01/2015
13. http://yetkilendirme.btk.gov.tr/Yetkilendirme/, 18/02/2015
14. https://tr.wikipedia.org/wiki/%C4%B0%C3%A7erik_sa%C4%9Flay%C4%B1c%C4%B1, 29/05/2015
15. http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5423b0921f2d07.14356840, 25/09/2014
16. http://tr.wikipedia.org/wiki/Su%C3%A7, 19/09/2014
17. http://www.dildernegi.org.tr/TR,274/turkcesozlukarabul.html, 22/01/2015
18. https://sibersuclar.iem.gov.tr/siber_suclari.html, 25/09/2014
19. http://tr.wikipedia.org/wiki/K%C3%B6t%C3%BC_ama%C3%A7l%C4%B1_yaz%C4%B1l%C4%B1m, 20/02/2015
20. http://tr.wikipedia.org/wiki/Yemleme, 20/02/2015
21. http://www.ekizer.net/adli-bilisim-computer-forensics/, 16/09/2014
22. http://tr.wikipedia.org/wiki/Adli_bili%C5%9Fim, 29/09/2014

23. http://www.howtogeek.com/howto/windowsvista/registryhacktodisablewritingtousbdrives/, 09/02/2015

24. https://gist.github.com/berkayunal/1595676, 11/10/2014

25. http://www.x-ways.net/pics/xwf_screen_eng.png, 03/06/2015

26. http://www.btk.gov.tr/bilgi_teknolojileri/internet_alan_adlari/index.php, 05/06/2015

ÖZGEÇMİŞ

Adı Soyadı	: Yasin BAŞAR
Doğum Yeri ve Tarihi	: Erbaa – 06.05.1987
Yabancı Dili	: İngilizce
İletişim (Telefon/e-posta)	: 0505 824 57 88 – yasin.basar@egm.gov.tr

Eğitim Durumu (Kurum ve Yıl)

Lise	: İlhami Ertem Lisesi / EDİRNE (2001-2004)
Ön Lisans	: 19 Mayıs Polis Meslek Yüksekokulu / SAMSUN (2005-2007)
Lisans	: Anadolu Üniversitesi İktisat Fakültesi İktisat Bölümü / ESKİŞEHİR (2007-2010)
Yüksek Lisans	: Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü İnternet ve Bilişim Teknolojileri Anabilim Dalı / AFYONKARAHİSAR (2013-2015)

Çalıştığı Kurum/Kurumlar ve Yıl :Konya Emniyet Müdürlüğü – KOM Şube Müdürlüğü (2007 - 2009)

Sivas Emniyet Müdürlüğü – KOM Şube Müdürlüğü ve Siber Suçlarla Mücadele Şube Müdürlüğü (2009 - 2015)

Ordu Emniyet Müdürlüğü – Gölköy İlçe Emniyet Müdürlüğü (2015 - ……..)

EKLER

EK – 1 Örnek Mahkeme Kararı

T.C.

SULH CEZA MAHKEMESİ

DEĞİŞİK İŞ KARAR

DEĞİŞİK İŞ NO : 2014/ D.İş

HAKİM :
KATİP :

C.Başsavcılığının 11/04/2014 tarih ve 2014/ sayılı yazıları ile aşağıda belirtilen adreste arama yapılması halinde suç delillerinin elde edileceği hususunda somut şüphe bulunduğundan (müşteki tarafından dosyaya sunulan fotoğraflar), suç delillerinin elde edilmesi amacıyla şüphelinin ikametinde bulunabilecek dijital materyallerde (Bilgisayar, Cep Telefonu harddisk, flashbellek, hafıza kartı vb.) söz konusu suçun işlendiğini gösterir emareler bulunabileceği değerlendirildiğinden, belirtilen ikamet adresinde **14/04/2014** tarihinde gündüzleyin bir defaya mahsus olmak üzere arama yapılması ve aramada bulunabilecek dijital materyallere yönelik CMK 116, 127, 134. Maddesi gereğince bilgisayar, bilgisayar programları, bilgisayar kütükleri, flash bellek, hafıza kartı, cep telefonu üzerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine; 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 konulmasına dair karar verilmesi CMK'nun 134.maddesi gereğince kamu adına talep edilmekle dosya incelendi.

GEREĞİ DÜŞÜNÜLDÜ:

TALEBİN KABULÜNE,

1- Şüpheli , ve oğlu, 30/03/1990 doğumlu, T.C kimlik nolu, Mahallesi, caddesi, apt. Sitesi no:9 İç Kapı no:1 adresi ve şüphelinin üzerinde bir defaya mahsus olmak üzere **14/04/2014** tarihinde **gündüzleyin ARAMA YAPILMASINA,** bilgisayar, bilgisayar programları, bilgisayar kütükleri, flash bellek, hafıza kartı, cep telefonu üzerinde arama yapılmasına, bilgisayar kayıtlarından kopya **ÇIKARILMASINA,**

2-Bu kayıtların çözülerek metin haline getirilmesine, 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 CMK'nun 134. maddesine göre **EL KONULMASINA,**

3- Kararın gereği için C.Başsavcılığına tevdiine,

Dair,evrak üzerinde yapılan inceleme sonucu karar verildi.11/04/2014

Katip Hakim

EK – 2 Örnek Ev Arama, Yakalama ve Elkoyma Tutanağı

EV ARAMA, YAKALAMA VE ELKOYMA TUTANAĞI

Sivas Cumhuriyet Başsavcılığının 11.04.2015 tarih ve **Soruşturma No:** 2015/…… sayılı **TCK 245 (Banka ve/veya Kredi Kartlarının Kötüye Kullanılması)** suçu soruşturması ile ilgili olarak, Sivas Sulh Ceza Mahkemesinin 11.04.2015 tarih ve 2015/…… Değişik İş numaralı mahkeme kararına istinaden, kararda belirtilen Sivas - Merkez - …… Mahallesi nüfusuna kayıtlı …… ve …… oğlu/kızı 01/01/1990 doğumlu şüpheli …… **(T.C. Kimlik No:……)** isimli şahsın **…… Mah.** …….. **Cad.** ……..**Apt. No:1 İç Kapı No:1 Merkez/SİVAS** sayılı ikametine 14.04.2015 günü saat 10:45 sıralarında yeteri kadar kuvvet ile gelinmiş, kapı usulüne uygun olarak çalınmış, kapıyı açan ve açık kimlik bilgilerini sonradan öğrendiğimiz şüpheli …… isimli şahsa Polis Kimlik Kartlarımız gösterilmiş, mahkeme kararı yüzüne karşı okunmuş ve okutulduktan sonra şüpheli …… isimli şahıs aynı gün saat 10:50 sıralarında yasal hakları yüzüne karşı yüksek sesle okunup anladığını beyan ettikten sonra biz görevlilerce yakalaması yapılmış ve güvenlik amaçlı kaba üst aramasında herhangi bir suç ve suç unsuruna rastlanılmamıştır.

İkamette hazurun olarak bulundurulan …… Mahalle Muhtarı …… **(T.C. Kimlik No: ……..)** isimli şahıs ile ikamette bulunan …… (annesi) isimli şahıs huzurunda 3 (üç) oda, 1 (bir) salon, mutfak, banyo, tuvalet ve müştemilatından ibaret ikamette aynı gün saat 10:55 sıralarında arama işlemine başlanılmıştır.

İkamette yapılan aramada, internet olup olmadığı kontrol edildiğinde, internet hattının olduğu ve kablolu modem ile internete giriş yapıldığı görülmüş, ancak internet hattının paylaşılmadığı tespit edilmiştir. İkametin oturma odası olarak kullanılan odanın girişine göre solda bulunan masanın çekmecesinde üzerinde el yazısı ile yazılmış **"Data"** ibaresi yazılı bulunan **1 ile numaralandırılmış DMS Copy** marka **DR5FA1-00636** seri numaralı **DVD**'ye, aynı çekmecede bulunan **2 ile numaralandırılmış** Sandisk marka **Dual USB Drive 16 GB** model **BL141100028** seri numaralı **16 GB** kapasiteli USB belleğe ve masa üzerinde kapalı vaziyette bulunan **HP** marka **Pavilion DV6** model seri numarası tespit edilemeyen siyah renkli laptop tabir edilen bilgisayar içerisinden sökülen **3 ile numaralandırılmış Hitachi** marka **HTS725032A9A364** model **100414PCKC04VPHZU8MJ** seri numaralı **320 GB** kapasiteli harddiske, arama yapılan ikamette kesintisiz güç kaynağı olmadığından ve harddisk içerisinde şifrelenmiş dosya/klasör olduğu değerlendirildiğinden mahkeme kararına istinaden gerekli yedek alma ve çözümleme işlemleri yapılabilmesi amacıyla, işlemler tamamlanıncaya kadar biz görevlilerce el konulmuştur.

Yapılan arama neticesinde başkaca suç ve unsuruna rastlanılmamış olup, hazurun …… Mahalle Muhtarı …… huzurunda ikamette bulunan şüpheli ……..'a ikamette yapılan aramadan dolayı herhangi bir zarar ve ziyanın olup olmadığı sorulmuş, **"HAYIR - YOKTUR"** demeleri üzerine arama işlemine aynı gün saat 11:10 sıralarında son verilmiş olup,

İş bu Ev Arama, Yakalama ve Elkoyma Tutanağı tarafımızdan mahallinde tanzim edilerek doğruluğu taraflarca okunup anlaşıldıktan sonra altı birlikte imza altına alınmıştır. 14.04.2015 saat 12:00

……	……	……	……
Polis Memuru	Polis Memuru	Polis Memuru	Polis Memuru
……	……	……	……
Polis Memuru	Polis Memuru (Bayan)	Mahalle Muhtarı Hazurun	İkamette Bulunan
			……
			Şüpheli - Yakalanan

EK – 3 Adli Kopya (İmaj) Alma Tutanağı (1. Sayfa)

SİVAS VALİLİĞİ
İl Emniyet Müdürlüğü
Siber Suçlarla Mücadele Şube Müdürlüğü
Adli Bilişim Büro Amirliği

ADLİ KOPYA (İMAJ) ALMA TUTANAĞI

İncelemeyi Talep Eden Birim:	Siber Suçlarla Mücadele Şube Müdürlüğü / Suç Araştırma ve Soruşturma Büro Amirliği
Talep Tarihi:	09/04/2015
Soruşturma Makamı ve Numarası:	Sivas Cumhuriyet Başsavcılığı – Soruşturma No: 2015/…….
İnceleme Karar Makamı:	Sivas Sulh Ceza Hakimliği
Karar Tarih ve No:	08/04/2015 – Değişik İş No: 2015/…….
İnceleme Konusu:	Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu
Materyalin Ele Geçirildiği Şahsın Açık Kimliği:	Şüpheli …… (T.C. Kimlik No:……): ……..-Merkez-Cumhuriyet Mah. nüfusuna kayıtlı …….. – …….. oğlu Sivas – 01/01/1990 doğumlu.

İMAJI ALINAN MATERYALLER

S.No	Marka	Model	Seri No	Açıklama
1	DMS Copy	-	DR5FA1-00636	Şüpheli …… isimli şahsın ikamet adresinde yapılan arama neticesinde el konulan, üzerinde el yazısı ile yazılmış **"DATA"** ibaresi bulunan DVD.

Adli Kopya (İmaj) Alma Tutanağının 1. Sayfasıdır.

EK – 3 Adli Kopya (İmaj) Alma Tutanağı (2. Sayfa)

2	Sandisk	Dual USB Drive 16 GB	BL141100028	Aynı ikamet adresinde yapılan arama neticesinde el konulan, **Sandisk** marka siyah renkli, **USB 2.0** ve **Micro USB** girişleri bulunan 16 GB kapasiteli USB Bellek.

Materyalin Markası

Materyalin Model, Boyut ve Seri Numarası

3	Hitachi	HTS725032A9A364	100414PCKC04VPHZU8MJ	Aynı ikamet adresinde yapılan arama neticesinde el konulan, **HP** marka **Pavilion DV6** model seri numarası tespit edilemeyen siyah renkli laptop tabir edilen taşınabilir bilgisayar içerisinden sökülen **Hitachi** marka **320 GB** kapasiteli Harddisk.

Materyalin Söküldüğü Laptop Tabir Edilen Taşınabilir Bilgisayarın Markası

Materyale Ait Marka, Model, Seri Numarası vb. Teknik Bilgiler

Adli Kopya (İmaj) Alma Tutanağının 2. Sayfasıdır.

EK – 3 Adli Kopya (İmaj) Alma Tutanağı (3. Sayfa)

İMAJ ALMA SÜRECİ :

Yukarıda yazılı özellikleri yazılı bulunan **3 (üç) adet** dijital materyalin imaj alma işlemi esnasında Uluslararası Adli Bilişim Standartlarına uygun şekilde yazılım tabanlı **Write Block (Yazma Koruma)** kullanılarak delil bütünlüğü korunmak suretiyle imaj alma işlemleri tamamlanmış, delil bütünlüğünün korunduğunu gösterir **Hash değerleri (MD5** ve **SHA1)** ayrı ayrı tespit edilerek aşağıda gösterilmiştir.

İmaj alma işlemi esnasında ücretsiz olarak kullanıma sunulan **FTK Imager (Versiyon 3.2.0.0)** ve **EnCase Forensic Imager (Versiyon 7.06)** programlarından faydalanılmıştır.

1 NO'LU MATERYALE AİT İMAJ ALMA İŞLEMİ :

DMS Copy marka ve **DR5FA1-00636** seri numaralı, üzerinde el yazısı ile yazılmış **"DATA"** ibaresi bulunan DVD'nin imaj alma işlemi **EnCase Forensic Imager 7.06** programı ile gerçekleştirilmiş olup, işleme ait teknik özellikler aşağıya çıkartılmıştır.

Image Information :

Acquisition :

File Acquired: 09/04/15 16:57:03

MD5: ba5c7f4478b5bfda3420ae0385c95d8e

SHA1: 3d1fae50c94d95519697ede83ab02b65ea0e80be

Verification :

MD5: ba5c7f4478b5bfda3420ae0385c95d8e : **verified**

SHA1: 3d1fae50c94d95519697ede83ab02b65ea0e80be : **verified**

2 NO'LU MATERYALE AİT İMAJ ALMA İŞLEMİ :

Sandisk marka **Dual USB Drive 16 GB** model **BL141100028** seri numaralı **16 GB** kapasiteli USB belleğin imaj alma işlemi **Created By AccessData® FTK® Imager 3.2.0.0** programı ile gerçekleştirilmiş olup, işleme ait teknik özellikler aşağıya çıkartılmıştır.

Image Information :

Acquisition started: Thu Apr 02 13:23:08 2015

Acquisition finished: Thu Apr 02 13:37:29 2015

Computed Hashes :

MD5 checksum: daee574f784f77a631d740466c42ced1

SHA1 checksum: 4de693eeef32c12dfec8eb43ced251f1b5202931

EK – 3 Adli Kopya (İmaj) Alma Tutanağı (4. Sayfa)

Image Verification Results :

Verification started: Thu Apr 02 13:37:29 2015

Verification finished: Thu Apr 02 13:38:32 2015

MD5 checksum: daee574f784f77a631d740466c42ced1 : **verified**

SHA1 checksum: 4de693eeef32c12dfec8eb43ced251f1b5202931 : **verified**

3 NO'LU MATERYALE AİT İMAJ ALMA İŞLEMİ :

HP marka **Pavilion DV6** model seri numarası tespit edilemeyen siyah renkli laptop tabir edilen taşınabilir bilgisayar içerisinden sökülen **Hitachi** marka **HTS725032A9A364** model **100414PCKC04VPHZU8MJ** seri numaralı **320 GB** kapasiteli harddiskin imaj alma işlemi **Created By AccessData® FTK® Imager 3.2.0.0** programı ile gerçekleştirilmiş olup, işleme ait teknik özellikler aşağıya çıkartılmıştır.

Image Information :

Acquisition started: Mon Apr 06 10:36:40 2015

Acquisition finished: Mon Apr 06 11:38:27 2015

Computed Hashes :

MD5 checksum: e8359ebbe97f3bae584c76971059c35b

SHA1 checksum: 5dbd53e4e7b0f6b8dd19d084af57722da83018e9

Image Verification Results :

Verification started: Mon Apr 06 11:38:43 2015

Verification finished: Mon Apr 06 12:14:53 2015

MD5 checksum: e8359ebbe97f3bae584c76971059c35b : **verified**

SHA1 checksum: 5dbd53e4e7b0f6b8dd19d084af57722da83018e9 : **verified**

İş bu Adli Kopya (İmaj) Alma Tutanağı tarafımdan tanzim edilerek altı imza altına alınmıştır. 10.04.2015 saat 15:00

Yasin BAŞAR
Polis Memuru
Adli Bilişim Uzmanı

****

Teknik Detaylar : Tutanak içerisinde geçen teknik terimlerin açıklaması aşağıda belirtilmiştir.

Write Block: Yazma engelleme anlamına gelmektedir. İmajı alınacak materyalin yazma engellemesi sağlanarak imaj alınır. Donanımsal ya da yazılımsal olarak sağlanabilmektedir. Yukarıda belirtilen imaj alma işlemi esnasında yazılımsal yazma engellemesi kullanılmıştır. Yazma engellemesi dijital materyalin el konulduktan sonra içerisine herhangi bir veri yazılmasını ve delil bütünlüğünün sağlanması için kullanılmaktadır. Uluslararası Adli Bilişim Standartlarına göre Write Block kullanımı zorunlu tutulmaktadır.

MD5 ve SHA1 Hash Değerleri: Veri bütünlüğünü test etmek için kullanılan bir dosya şifreleme biçimidir. Bir dosyaya MD5 ve SHA1 testi yapılarak dosya doğruluğu ve bütünlüğü kontrol edilebilir. Delil bütünlüğünün bozulup bozulmadığı yönünde bilgi verir. Hash değerleri doğrulama neticesinde bir birini tutmuyor ise, veri üzerinde oynama ya da değişikliğin söz konusu olduğu değerlendirilir.

EK – 4 İnceleme Raporu (1. Sayfa)

SİVAS VALİLİĞİ
İl Emniyet Müdürlüğü
Siber Suçlarla Mücadele Şube Müdürlüğü
Adli Bilişim Büro Amirliği

İNCELEME RAPORU

İncelemeyi Talep Eden Birim:	Siber Suçlarla Mücadele Şube Müdürlüğü / Suç Araştırma ve Soruşturma Büro Amirliği
Talep Tarihi:	09/04/2015
Soruşturma Makamı ve Numarası:	Sivas Cumhuriyet Başsavcılığı – Soruşturma No: 2015/…….
İnceleme Karar Makamı:	Sivas Sulh Ceza Hakimliği
Karar Tarih ve No:	08/04/2015 – Değişik İş No: 2015/…….
İnceleme Konusu:	Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu
Materyalin Ele Geçirildiği Şahsın Adı Soyadı - T.C Kimlik No:	Şüpheli …… (T.C. Kimlik No:……): ……..-Merkez-Cumhuriyet Mah. nüfusuna kayıtlı …….. – …….. oğlu Sivas – 01/01/1990 doğumlu.

İNCELENEN MATERYALLER

S.No	Marka	Model	Seri / IMEI / ICCID No	Açıklama
1	DMS Copy	-	DR5FA1-00636	Şüpheli …… isimli şahsın ikamet adresinde yapılan arama neticesinde el konulan, üzerinde el yazısı ile yazılmış "DATA" ibaresi bulunan DVD.
2	Sandisk	Dual USB Drive 16 GB	BL141100028	Aynı ikamet adresinde yapılan arama neticesinde el konulan, Sandisk marka siyah renkli, USB 2.0 ve Micro USB girişleri bulunan 16 GB kapasiteli USB Bellek.
3	Hitachi	HTS725032A9A364	100414PCKC04VPH ZU8MJ	Aynı ikamet adresinde yapılan arama neticesinde el konulan, HP marka Pavilion DV6 model seri numarası tespit edilemeyen siyah renkli laptop tabir edilen taşınabilir bilgisayar içerisinden sökülen Hitachi marka 320 GB kapasiteli Harddisk.

EK – 4 İnceleme Raporu (2. Sayfa)

İNCELEME SÜRECİ

Dijital materyallerin incelenmesi aşamasında, uluslararası adli bilişim standartlara uygun olarak yazma koruması (Yazılımsal Write Blocker) kullanmak suretiyle veri bütünlüğünün korunması sağlandıktan sonra, birebir kopyaları (imaj) alınan dijital materyaller içerisindeki silinmiş veriler de dahil olmak üzere inceleme işlemi gerçekleştirilmiştir. İnceleme işleminde **Encase Forensic (Ver. 6.19)** programı kullanılmıştır.

İncelemeye konu materyallerden çıkan, **Banka ve/veya Kredi Kartlarının Kötüye Kullanılması** suçu soruşturması kapsamında delil olarak değerlendirilen verilerin tümü rapor ekinde gönderilen DVD içerisine kopyalandığından, inceleme raporu değerlendirilirken sadece raporda belirtilen hususlar değil, DVD içerisine çıkartılan orijinal dosyalar da göz önünde bulundurulmalıdır.

1 NOLU MATERYALE AİT İNCELEME SONUCU

MATERYALE AİT SİSTEM BİLGİLERİ	
Name	1_Numaralı_Delil
Description	Volume, Sector 0-39999, 78,1MB
File Acquired	04/09/15 04:57:03
Physical Size	32.768
Evidence File	1_Numaralı_Delil
VOLUME	
File System	UDF
Sectors per cluster	1
Bytes per sector	2.048
Total Sectors	40.000
Total Capacity	81.920.000 Bytes (78,1MB)
Total Clusters	40.000
Unallocated	1.245.184 Bytes (1,2MB)
Free Clusters	608
Allocated	80.674.816 Bytes (76,9MB)
Drive Type	CD-ROM
DEVİCE	
Actual Date	04/09/15 04:57:03
Target Date	04/09/15 04:57:07
File Path	F:\Tez_Proje_Calismasi\1_Numarali_Delil\1_Numaralı_Delil.E01
Case Number	.... Cumhuriyet Başsavcılığının Soruşturma No:2015/....
Evidence Number	1_Numaralı_Delil (DMS Marka DATA Yazılı DVD)
Examiner Name	Yasin BAŞAR
Notes	Afyon Kocatepe Üniversitesi İnternet ve Bilişim Teknolojileri Yönetimi Yüksek

EK – 4 İnceleme Raporu (3. Sayfa)

	Lisans Programı Tez Çalışması Kapsamında Senaryo Uygulaması
Drive Type	CD-ROM
File Integrity	Unverified
Acquisition MD5	ba5c7f4478b5bfda3420ae0385c95d8e
Verification MD5	ba5c7f4478b5bfda3420ae0385c95d8e
Acquisition SHA1	3d1fae50c94d95519697ede83ab02b65ea0e80be
Verification SHA1	3d1fae50c94d95519697ede83ab02b65ea0e80be
GUID	b232197ad55794c5874f539e480c4c1f
EnCase Version	7.06
System Version	Windows 8
Error Granularity	64
Index File	F:\Tez_Proje_Calismasi\Delil_DVD'si\1_Numarali_Delil\Index\1_Numaralı_Delil-b232197ad55794c5874f539e480c4c1f.Index
Compression	Best
Total Size	81.920.000 Bytes (78,1MB)
Total Sectors	40.000
Disk Signature	00000000
Partitions	Valid

DMS Copy marka **DR5FA1-00636** seri numaralı DVD'nin alınan imajı üzerinde yapılan inceleme neticesinde; depolama aygıtı olarak kullanılan DVD içerisinde kayıtlı bulunan ve soruşturma kapsamında suç unsuru olduğu değerlendirilen bilgi ve belgeler özellikleri ile birlikte aşağıya çıkartılmıştır.

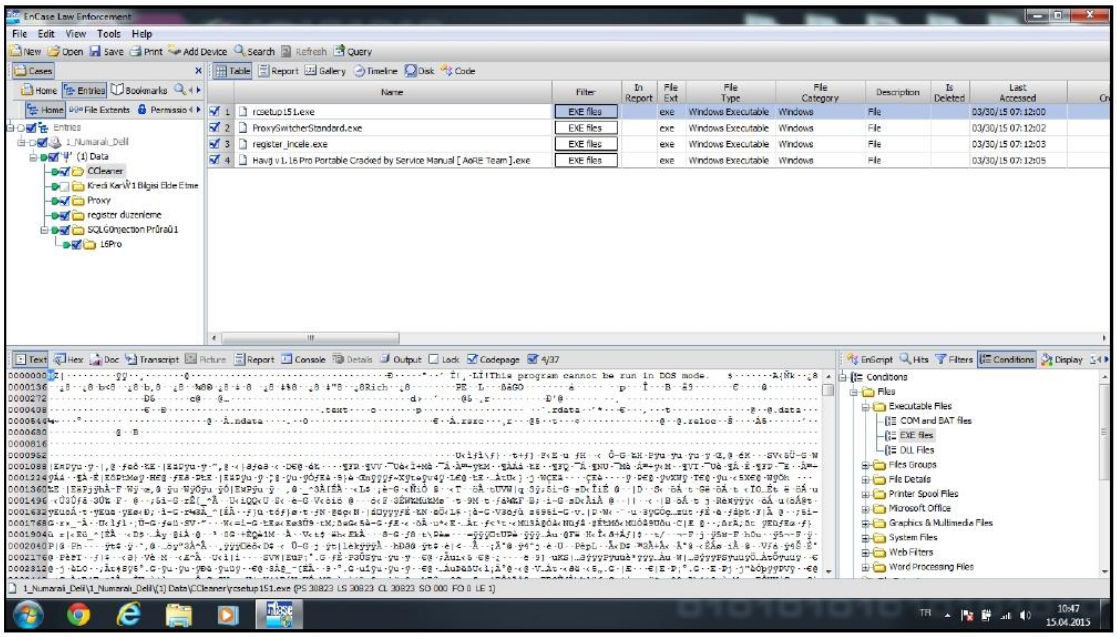
❖ Delil içeriğinde kayıtlı bulunan ve soruşturma kapsamımda suç unsuru olduğu değerlendirilen toplam 5 (beş) adet programın IP numarası değiştirme, sistem hackleme ve hackleme işlemi neticesinde oluşacak olan sistem kayıtlarını temizlemeye yarayan programlar olduğu görülmüş ve bu programlardan 4 (dört) tanesinin gizlenmiş olduğu anlaşılmıştır. Ayrıca inceleme esnasında elde edilen programlara ait ekran çıktısı ve bazı programların oluşturma ve erişim tarihleri ile hash değerlerine ait bilgiler örnek olarak aşağıda gösterilmiştir.

Name	:	ProxySwitcherStandard.exe
Description	:	File, Hidden, Read Only
Last Accessed	:	03/30/15 10:12:02
File Created	:	02/12/15 03:27:16
Last Written	:	02/12/15 03:27:16
Entry Modified	:	03/30/15 10:12:45
Hash Value	:	592004a7c15967e4531e75b1f22bd5b1
Full Path	:	1_Numarali_Delil\Single Files\NoName\Proxy\ProxySwitcherStandard.exe

Name	:	Havij v1.16 Pro Portable Cracked by Service Manual [AoRE Team].exe
Description	:	File, Hidden, Read Only
Last Accessed	:	03/30/15 10:12:05
File Created	:	09/22/12 09:18:18

Last Written	:	09/22/12 09:18:18
Entry Modified	:	03/30/15 10:12:45
Hash Value	:	984e28e70d1000272a2ab61e34d12d6e
Full Path	:	1_Numarali_Delil\Single Files\NoName\SQL İnjection Proğramı\16Pro\Havij v1.16 Pro Portable Cracked by Service Manual [AoRE Team].exe

Name	:	register_incele.exe
Last Accessed	:	03/30/15 07:12:03
Entry Modified	:	04/09/10 11:18:28
Hash Value	:	8d6f3d01853e6a4087f48ed65a00db5b
Full Path	:	1_Numarali_Delil\1_Numaralı_Delil\(1)Data\register düzenleme\register_incele.exe



Programlara Ait Encase Forensic Yazılımından Alınan Ekran Çıktısı

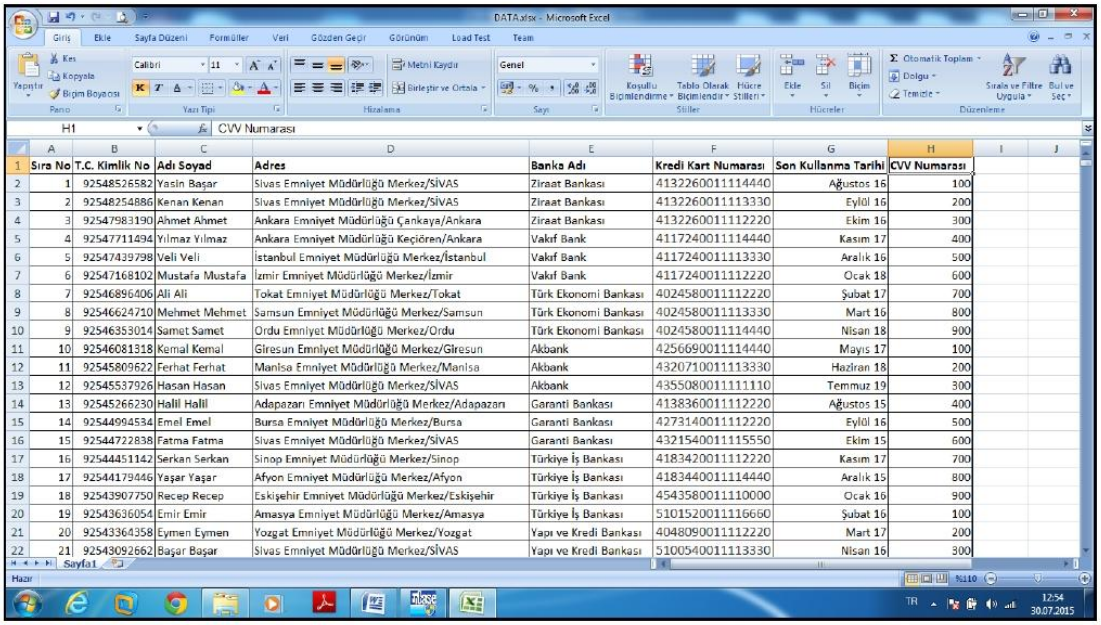
❖ Delil içeriğinde kayıtlı bulunan ve soruşturma kapsamımda suç unsuru olduğu değerlendirilen toplam 6 (altı) adet dokümanın kredi kartı bilgileri ve kredi kartı bilgileri elde etme ile ilgili dokümanlar olduğu görülmüş ve bu dokümanlardan 3 (üç) tanesinin gizlenmiş olduğu anlaşılmıştır. "DATA.xlsx" isimli doküman içeriğinde çok sayıda şahsa ait kimlik, adres ve kredi kartı bilgilerinin kayıtlı olduğu tespit edilmiş ve ekran görüntüsü ilgili dokümanın altında gösterilmiştir. Tespiti yapılan bazı dokümanların oluşturma ve erişim tarihleri ile hash değerlerine ait bilgiler örnek olarak aşağıda gösterilmiştir.

Name	:	Credit Card Generator with CVV v2.pdf
Description	:	File, Hidden, Read Only
Last Accessed	:	03/30/15 10:12:00
File Created	:	02/12/15 02:55:34
Last Written	:	02/12/15 02:55:34
Entry Modified	:	03/30/15 10:12:45
Hash Value	:	160878db47e8201bea22fd05a37a9de0

EK – 4 İnceleme Raporu (5. Sayfa)

Full Path	:	1_Numarali_Delil\Single Files\NoName\Kredi Kartı Bilgisi Elde Etme\Credit Card Generator with CVV v2.pdf

Name	:	DATA.xlsx
Description	:	File, Hidden, Read Only
Last Accessed	:	03/30/15 10:12:05
File Created	:	03/30/15 10:10:14
Last Written	:	03/30/15 10:10:14
Entry Modified	:	03/30/15 10:12:45
Hash Value	:	9c92ac5156dba28f94d7f0d0c094c049
Full Path	:	1_Numarali_Delil\Single Files\NoName\DATA.xlsx



Sıra No	T.C. Kimlik No	Adı Soyad	Adres	Banka Adı	Kredi Kart Numarası	Son Kullanma Tarihi	CVV Numarası
1	92548526582	Yasin Başar	Sivas Emniyet Müdürlüğü Merkez/SİVAS	Ziraat Bankası	4132260011114440	Ağustos 16	100
2	92548254886	Kenan Kenan	Sivas Emniyet Müdürlüğü Merkez/SİVAS	Ziraat Bankası	4132260011113330	Eylül 16	200
3	92547983190	Ahmet Ahmet	Ankara Emniyet Müdürlüğü Çankaya/Ankara	Ziraat Bankası	4132260011112220	Ekim 16	300
4	92547711494	Yılmaz Yılmaz	Ankara Emniyet Müdürlüğü Keçiören/Ankara	Vakıf Bank	4117240011114440	Kasım 17	400
5	92547439798	Veli Veli	İstanbul Emniyet Müdürlüğü Merkez/İstanbul	Vakıf Bank	4117240011113330	Aralık 16	500
6	92547168102	Mustafa Mustafa	İzmir Emniyet Müdürlüğü Merkez/İzmir	Vakıf Bank	4117240011112220	Ocak 18	600
7	92546896406	Ali Ali	Tokat Emniyet Müdürlüğü Merkez/Tokat	Türk Ekonomi Bankası	4024580011112220	Şubat 17	700
8	92546624710	Mehmet Mehmet	Samsun Emniyet Müdürlüğü Merkez/Samsun	Türk Ekonomi Bankası	4024580011113330	Mart 16	800
9	92546353014	Samet Samet	Ordu Emniyet Müdürlüğü Merkez/Ordu	Türk Ekonomi Bankası	4024580011114440	Nisan 18	900
10	92546081318	Kemal Kemal	Giresun Emniyet Müdürlüğü Merkez/Giresun	Akbank	4256690011114440	Mayıs 17	100
11	92545809622	Ferhat Ferhat	Manisa Emniyet Müdürlüğü Merkez/Manisa	Akbank	4320710011113330	Haziran 18	200
12	92545537926	Hasan Hasan	Sivas Emniyet Müdürlüğü Merkez/SİVAS	Akbank	4355080011111110	Temmuz 19	300
13	92545266230	Halil Halil	Adapazarı Emniyet Müdürlüğü Merkez/Adapazarı	Garanti Bankası	4138360011112220	Ağustos 15	400
14	92544994534	Emel Emel	Bursa Emniyet Müdürlüğü Merkez/Bursa	Garanti Bankası	4273140011112220	Eylül 16	500
15	92544722838	Fatma Fatma	Sivas Emniyet Müdürlüğü Merkez/SİVAS	Garanti Bankası	4321540011115550	Ekim 15	600
16	92544451142	Serkan Serkan	Sinop Emniyet Müdürlüğü Merkez/Sinop	Türkiye İş Bankası	4183420011112220	Kasım 17	700
17	92544179446	Yaşar Yaşar	Afyon Emniyet Müdürlüğü Merkez/Afyon	Türkiye İş Bankası	4183440011114440	Aralık 15	800
18	92543907750	Recep Recep	Eskişehir Emniyet Müdürlüğü Merkez/Eskişehir	Türkiye İş Bankası	4543580011110000	Ocak 16	900
19	92543636054	Emir Emir	Amasya Emniyet Müdürlüğü Merkez/Amasya	Türkiye İş Bankası	5101520011116660	Şubat 16	100
20	92543364358	Eymen Eymen	Yozgat Emniyet Müdürlüğü Merkez/Yozgat	Yapı ve Kredi Bankası	4048090011112220	Mart 17	200
21	92543092662	Başar Başar	Sivas Emniyet Müdürlüğü Merkez/SİVAS	Yapı ve Kredi Bankası	5100540011113330	Nisan 16	300

"DATA.xlsx" İsimli Doküman İçeriğine Ait Ekran Çıktısı

Name	:	Kredi KarŴ1 BIN Listesi.pdf
Last Accessed	:	03/30/15 07:11:54
Entry Modified	:	10/11/14 06:14:40
Hash Value	:	fd7aa8cc4b5737ca09605081cbb8a5e8
Full Path	:	1_Numarali_Delil\1_Numaralı_Delil\(1) Data\Kredi KarŴ1 BIN Listesi.pdf

Name	:	Kredi KarŴ1 Hack Pro 2015 Sürümü _ Direct Download (Yeni).pdf
Last Accessed	:	03/30/15 07:11:54
Entry Modified	:	02/12/15 12:09:14
Hash Value	:	4241804a7ea05b07fa13ac57e6a28bb1
Full Path	:	1_Numarali_Delil\1_Numaralı_Delil\(1) Data\Kredi KarŴ1 Hack Pro 2015 Sürümü _ Direct Download (Yeni).pdf

❖ Delil içeriğinde kayıtlı bulunan ve soruşturma kapsamımda suç unsuru olduğu değerlendirilen toplam 3 (üç) adet resmin kredi kartı bilgileri ve kredi kartı bilgileri elde etme ile ilgili resimler olduğu görülmüş ve bu resimlerden 2 (iki) tanesinin gizlenmiş olduğu anlaşılmıştır.

EK – 4 İnceleme Raporu (6. Sayfa)

Tespiti yapılan bazı dokümanların oluşturma ve erişim tarihleri ile hash değerlerine ait bilgiler örnek olarak aşağıda gösterilmiştir.

Name	:	paypal3b.gif
Description	:	File, Hidden, Read Only
Last Accessed	:	03/30/15 10:11:55
File Created	:	02/12/15 02:51:24
Last Written	:	02/12/15 02:51:24
Entry Modified	:	03/30/15 10:12:45
Hash Value	:	dbab0d21155bf16462ce71fed2d9bbe7
Full Path	:	1_Numarali_Delil\Single Files\NoName\paypal3b.gif

Name	:	Kredi KarŴ1 Sitesi - Sahte.PNG
Last Accessed	:	03/30/15 07:11:54
Entry Modified	:	02/12/15 12:03:44
Hash Value	:	4faf8d22edaa15de3436bd3d676d6dde
Full Path	:	1_Numarali_Delil\1_Numaralı_Delil\(1) Data\Kredi KarŴ1 Sitesi - Sahte.PNG

Yukarıda tespiti yapılan ve soruşturma kapsamında delil olarak değerlendirilen bilgi ve belgeler rapor ekindeki **Delil DVD**'si içerisinde bulunan **"1_Numarali_Delil"** isimli klasöre kopyalanmıştır.

EK – 4 İnceleme Raporu (7. Sayfa)

2 NOLU MATERYALE AİT İNCELEME SONUCU

MATERYALE AİT SİSTEM BİLGİLERİ	
Name	2 Numaral[U+131] Delil
File Ext	Sivas Sulh Ceza Hakimli[U+11F]inin 01.04.2015 tarih ve 2015/.... De[U+11F]i[U+15F]ik [U+130][U+15F] No'lu Mahkeme Karar[U+131]
Description	Physical Disk, 31.116.288 Sectors 14,8GB
Physical Size	512
Evidence File	2 Numaral[U+131] Delil
DEVİCE	
Actual Date	04/02/15 10:23:08
Target Date	04/02/15 10:23:08
File Path	F:\Tez_Proje_Calismasi\2_Numarali_Delil\2_Numarali_Delil.E01
Case Number	Sivas Cumhuriyet Ba[U+15F]savc[U+131]l[U+131][U+11F][U+131] Soru[U+15F]turma No: 2015/..... - .... Siber Suçlarla Mücadele [U+15E]ube Müdürlü[U+11F]ü Suç No: 2015/...
Evidence Number	2 Numaral[U+131] Delil (Sandisk Marka 16 GB USB Bellek)
Examiner Name	Yasin BAŞAR
Notes	Afyon Kocatepe Üniversitesi [U+130]nternet ve Bili[U+15F]im Teknolojileri Yönetimi Yüksek Lisans Pro[U+11F]ram[U+131] Tez Çal[U+131][U+15F]mas[U+131] Kapsam[U+131]nda Senaryo Uygulamas[U+131]
Drive Type	Fixed
File Integrity	Unverified
Acquisition MD5	daee574f784f77a631d740466c42ced1
Verification MD5	daee574f784f77a631d740466c42ced1
Acquisition SHA1	4de693eeef32c12dfec8eb43ced251f1b5202931
Verification SHA1	4de693eeef32c12dfec8eb43ced251f1b5202931
EnCase Version	ADI3.2.0.0
System Version	Win 201x
Is Physical	•
Index File	F:\Tez_Proje_Calismasi\Delil_DVD'si\2_Numarali_Delil\Index\... Sulh Ceza Hakimli[U+11F]inin 01.04.2015 tarih ve 2015/.... De[U+11F]i[U+15F]ik [U+130][U+15F] No'lu Mahkeme Karar[U+131] .Index
Compression	None
Total Size	15.931.539.456 Bytes (14,8GB)
Total Sectors	31.116.288
Disk Signature	00000000
Partitions	Valid
PARTITIONS	
ID	0c
Type	FAT32X
Start Sector	8.192
Total Sectors	31.108.096

Size	14.8 GB

Sandisk marka **Dual USB Drive 16 GB** model **BL141100028** seri numaralı siyah renkli **16 GB** kapasiteli USB belleğin alınan imajı üzerinde yapılan inceleme neticesinde; depolama aygıtı olarak kullanılan USB belleğin içerisinde kayıtlı bulunan ve soruşturma kapsamında suç unsuru olduğu değerlendirilen bilgi ve belgeler özellikleri ile birlikte aşağıya çıkartılmıştır.

❖ Delil içeriğinde kayıtlı bulunan ve soruşturma kapsamımda suç unsuru olduğu değerlendirilen toplam 6 (altı) adet programın sistem hackleme, sanal makine kurma ve hackleme işlemi neticesinde oluşacak olan sistem kayıtlarını temizlemeye yarayan programlar olduğu görülmüş, bu programlardan **"Havij v1.16 Pro"** ve **"Password Changer.iso"** isimli programların gizlenmiş olarak kaydedildiği ve **"HAKOPS SQL İnj Scanner.rar"** isimli programın ise, 1 numaralı delil üzerinde yapılan inceleme neticesinde soruşturma kapsamında delil olarak değerlendirilen programlardan birisi olduğu (hash değerleri de aynı) anlaşılmıştır. Ayrıca inceleme esnasında elde edilen programlardan 1 numaralı delilden farklı olarak tespit edilen 5 (beş) adet programdan bazılarının oluşturma ve erişim tarihleri ile hash değerlerine ait bilgiler örnek olarak aşağıda gösterilmiştir.

Name	:	Password Changer.iso
Description	:	File, Hidden, Archive
Last Accessed	:	03/30/15
File Created	:	02/17/15 10:43:50
Last Written	:	02/18/10 12:20:00
Hash Value	:	8acecfa8a169219a8f2923045ddf92fb
Full Path	:	2_Numarali_Delil\C\Password Changer.iso
Short Name	:	PASSWO~1.ISO

Name	:	CleanWipe.exe
File Type	:	Windows Executable
File Category	:	Windows
Description	:	File, Archive
Last Accessed	:	03/30/15
File Created	:	02/17/15 10:24:44
Last Written	:	07/14/08 03:56:24
Hash Value	:	4cda8b9dcc98eef4bb90d271d0191e7c
Full Path	:	2_Numarali_Delil\C\CleanWipe.exe
Short Name	:	CLEANW~1.EXE

❖ Delil içeriğinde kayıtlı bulunan ve soruşturma kapsamımda suç unsuru olduğu değerlendirilen toplam 8 (sekiz) adet dokümandan **"IMPORTANT FILE {must read}.txt"**, **"DATA.xlsx"**, **"Kredi Kartı Hack Pro 2015 Sürümü _ Direct Download (Yeni).pdf"** ve **"Kredi Kartı BIN Listesi.pdf"** isimli dokümanlar, 1 numaralı delil üzerinde yapılan inceleme neticesinde soruşturma kapsamında delil olarak değerlendirilen dokümanlar ile aynı olduğu (hash değerleri de

aynı) anlaşılmıştır. Ayrıca inceleme esnasında elde edilen dokümanlardan 1 numaralı delilden farklı olarak tespit edilen 4 (dört) adet dokümandan **"RESİMLİ ANLATIM-BACK TRACK 4.docx"** ve **"Kablosuz Ağ Şifresi Kırma (WPA Hacking).mht"** isimli dokümanların gizlenmiş olduğu tespit edilmiş ve bazı dokümanların oluşturma ve erişim tarihleri ile hash değerlerine ait bilgiler örnek olarak aşağıda gösterilmiştir. Tespiti yapılan dokümanların sanal makine kurma ve sistem hackleme ile ilgili bilgiler içerdiği anlaşılmıştır.

Name	:	VMware Workstation 8.docx
File Type	:	Word Document
File Category	:	Document
Description	:	File, Archive
Last Accessed	:	03/25/15
File Created	:	02/17/15 10:43:36
Last Written	:	10/04/11 01:52:32
Hash Value	:	badc7fdf22f448d3eac478f08b45c0e3
Full Path	:	2_Numarali_Delil\C\VMware Workstation 8\VMware Workstation 8.docx

Name	:	RESİMLİ ANLATIM-BACK TRACK 4.docx
File Type	:	Word Document
File Category	:	Document
Description	:	File, Hidden, Archive
Last Accessed	:	03/30/15
File Created	:	02/17/15 10:33:10
Last Written	:	03/27/11 09:22:42
Hash Value	:	873242e5d023f5434879aa0423410487
Full Path	:	2_Numarali_Delil\C\RESİMLİ ANLATIM-BACK TRACK 4.docx

Name	:	Kablosuz Ağ Şifresi Kırma (WPA Hacking).mht
File Type	:	Web Page
File Category	:	Document
Description	:	File, Hidden, Archive
Last Accessed	:	03/30/15
File Created	:	02/17/15 10:25:32
Last Written	:	02/27/13 04:16:14
Hash Value	:	4172b7a601ab2f023bb2069be066ba40
Full Path	:	2_Numarali_Delil\C\Kablosuz Ağ Şifresi Kırma (WPA Hacking).mht

❖ Delil içeriğinde kayıtlı bulunan ve soruşturma kapsamımda suç unsuru olduğu değerlendirilen toplam 5 (beş) adet resimden **"Kredi Kartı Sitesi - Sahte.PNG"** isimli resmin, 1 numaralı delil üzerinde yapılan inceleme neticesinde soruşturma kapsamında delil olarak değerlendirilen resim ile aynı olduğu (hash değerleri de aynı) anlaşılmıştır. Diğer 4 (dört) adet resmin ise, kredi kartlarına ait resimler olduğu görülmüş ve bu resimlerin tamamının gizlenmiş olduğu anlaşılmıştır. Tespiti yapılan bazı resimlerin oluşturma ve erişim tarihleri ile hash değerlerine ait bilgiler örnek olarak aşağıda gösterilmiştir.

Name	:	Maximum.jpg
File Type	:	JPEG

EK – 4 İnceleme Raporu (10. Sayfa)

File Category	:	Picture
Description	:	File, Hidden, Archive
Last Accessed	:	03/30/15
File Created	:	03/30/15 11:45:31
Last Written	:	03/30/15 11:45:32
Hash Value	:	9c8019c5367415c9940b268625815797
Full Path	:	2_Numarali_Delil\C\Kredi Kartları\Maximum.jpg
Short Name	:	MAXIMUM.JPG

Name	:	Teb.jpg
File Type	:	JPEG
File Category	:	Picture
Description	:	File, Hidden, Archive
Last Accessed	:	03/30/15
File Created	:	03/30/15 05:30:27
Last Written	:	03/30/15 05:33:08
Hash Value	:	6783ebd134df5aaf1a62791c4b1b052b
Full Path	:	2_Numarali_Delil\C\Kredi Kartları\Teb.jpg
Short Name	:	TEB.JPG

Yukarıda tespiti yapılan ve soruşturma kapsamında delil olarak değerlendirilen bilgi ve belgeler rapor ekindeki **Delil DVD**'si içerisinde bulunan **"2_Numarali_Delil"** isimli klasöre kopyalanmıştır.

EK – 4 İnceleme Raporu (11. Sayfa)

3 NOLU MATERYALE AİT İNCELEME SONUCU

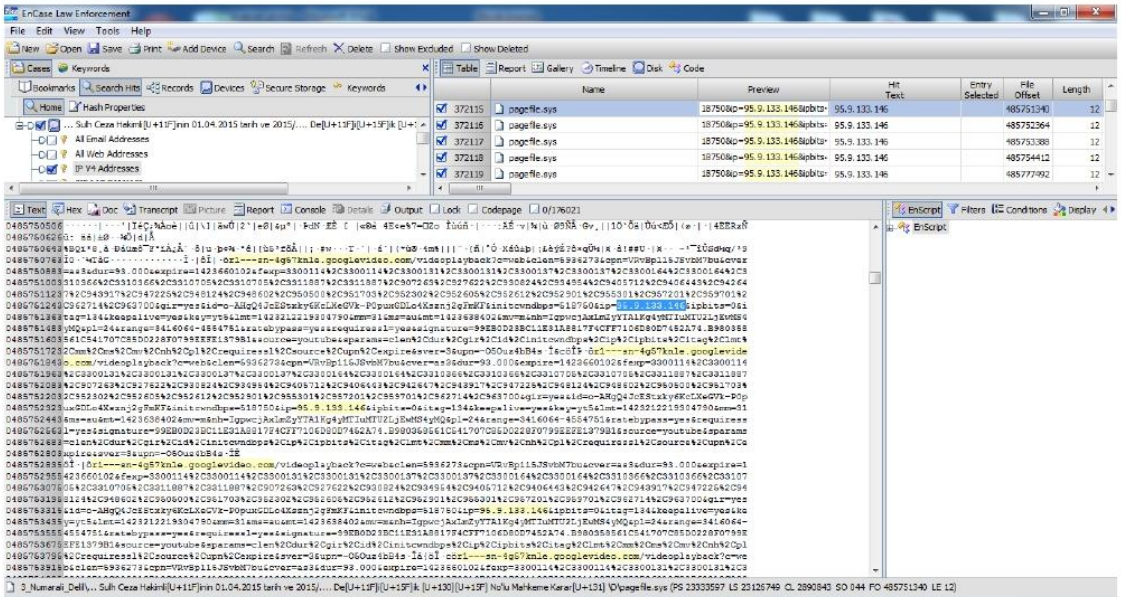
MATERYALE AİT SİSTEM BİLGİLERİ	
Name	3 Numaral[U+131] Delil
File Ext	Sivas Sulh Ceza Hakimli[U+11F]inin 01.04.2015 tarih ve 2015/.... De[U+11F]i[U+15F]ik [U+130][U+15F] No'lu Mahkeme Karar[U+131]
Evidence File	3 Numaral[U+131] Delil
Serial Number	760F-2E3E
Full Serial Number	E8760F5F760F2E3E
Driver Information	NTFS 3.1
Product Name:	Windows 7 Professional
Current Version:	6.1
Registered Owner:	Yasin Başar
System Root:	C:\Windows
Current Build Number:	7601
Path Name:	C:\Windows
Product ID:	00371-177-0000061-85917
Last Service Pack:	Service Pack 1
Install Date:	02/06/15 03:01:48
Last Shutdown Time:	02/12/15 12:29:14
BİLGİSAYARIN İŞLETİM SİSTEMİNE KAYITLI KULLANICI ADI VE ÖZELLİKLERİ	
User name:	Yasin Başar
Type of User:	Local User
Primary Group Number:	513
Security Identifier:	S-1-5-21-3867488891-2578623670-894085549-1000
User belongs to group:	Administrators
Profile Path:	C:\Users\Yasin Başar
Last Logon:	02/12/15 10:32:26
Last Password Change:	02/06/15 03:01:45
Last Incorrect Password Logon:	02/12/15 08:51:27
VOLUME	
File System	NTFS
Sectors per cluster	8
Bytes per sector	512
Total Sectors	624.932.864
Total Capacity	319.965.622.272 Bytes (298GB)
Total Clusters	78.116.607
Unallocated	286.286.147.584 Bytes (266,6GB)
Free Clusters	69.894.079
Allocated	33.679.474.688 Bytes (31,4GB)
Volume Offset	206.848
Drive Type	Fixed

EK – 4 İnceleme Raporu (12. Sayfa)

PARTITIONS	
ID	07
Type	NTFS
Start Sector	206.848
Total Sectors	624.932.864
Size	298GB

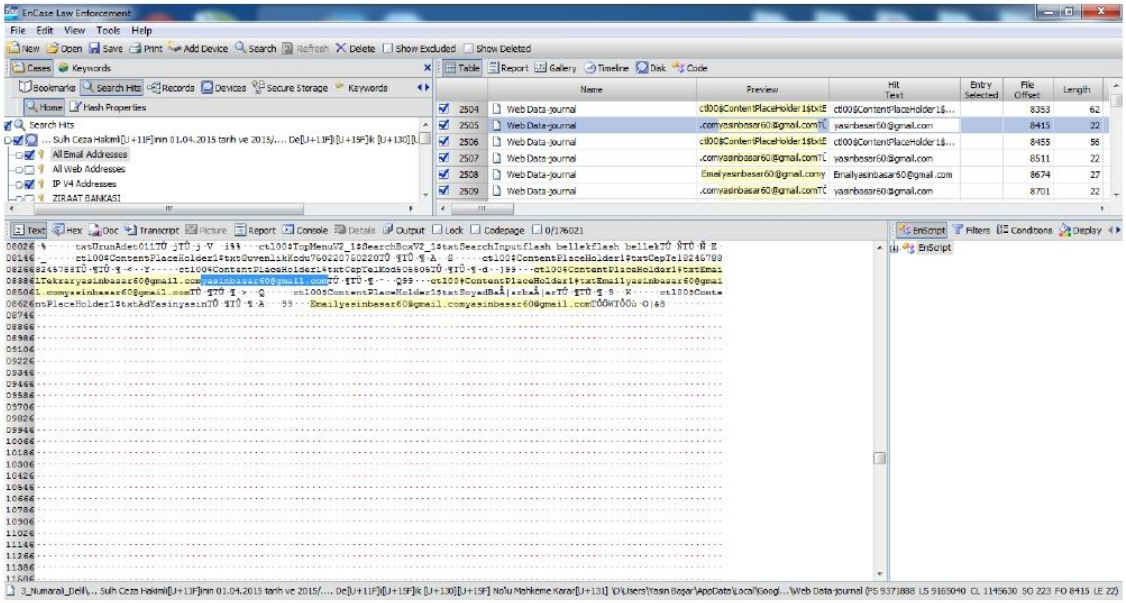
HP marka **Pavilion DV6** model seri numarası tespit edilemeyen siyah renkli laptop tabir edilen taşınabilir bilgisayar içerisinden sökülen **Hitachi** marka **HTS725032A9A364** model **100414PCKC04VPHZU8MJ** seri numaralı **320 GB** kapasiteli harddiskin alınan imajı üzerinde yapılan inceleme neticesinde; işletim sistemi yüklü harddiskin içerisinde kayıtlı bulunan ve soruşturma kapsamında suç unsuru olduğu değerlendirilen bilgi ve belgeler aşağıya çıkartılmıştır.

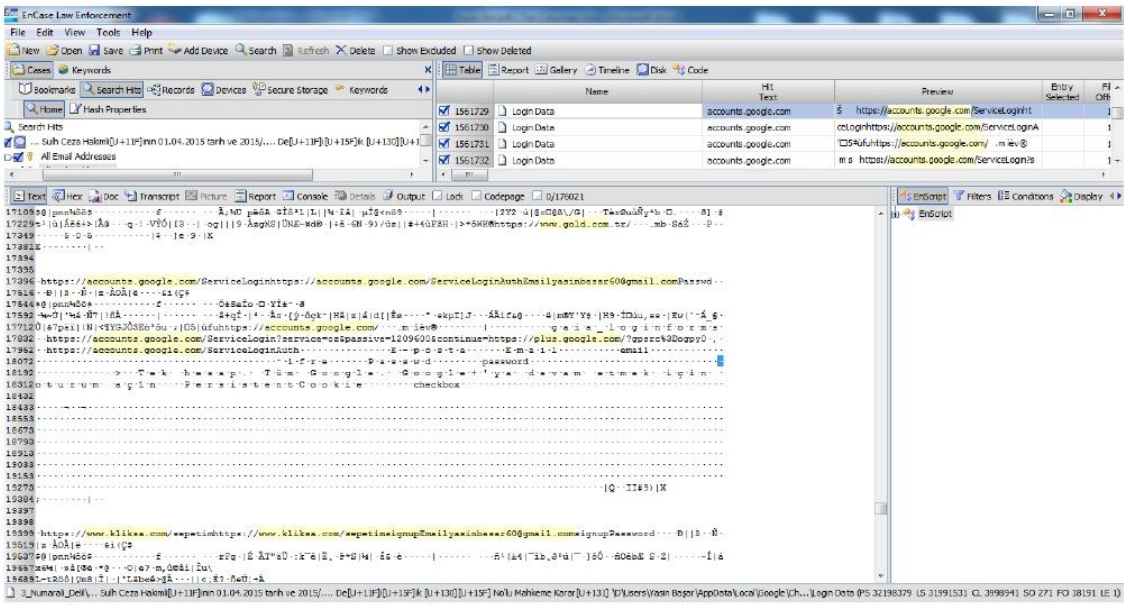
❖ Bilgisayarda kullanılan IP numaralarının tespiti yapılmış ve soruşturma kapsamında tespit edilen **95.9.133.146** IP numarasının bu bilgisayarda kullanıldığını gösterir ekran çıktısı aşağıda gösterilmiştir. IP numarasına ait kaydın "pagefile.sys" isimli sistem dosyası içerisinde yer alması, bu bilgisayarın çalıştığı zaman zarfında bu IP numarasını kullandığı ve bu IP numarası ile internete bağlantı sağladığı anlaşılmaktadır.



Suça Konu 95.9.133.146 IP Numarasına Ait Ekran Çıktısı

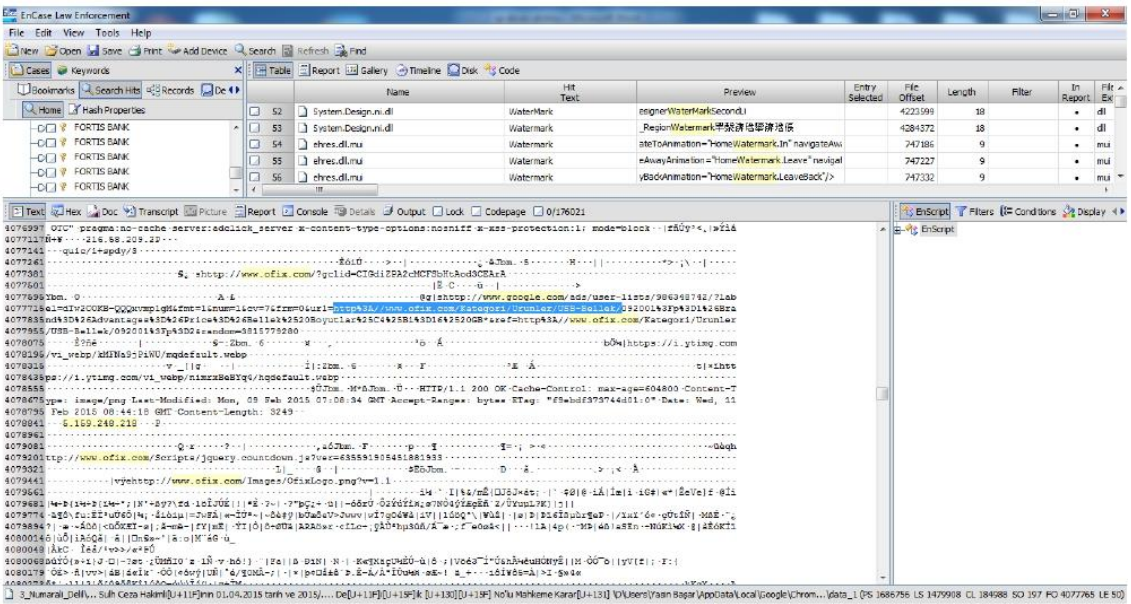
❖ Yine soruşturma kapsamında tespiti yapılan ve sipariş işlemi esnasında beyan edilen **yasinbasar60@gmail.com** isimli mail adresinin de bu bilgisayarda kullanıldığı tespit edilmiş ve ekran çıktıları aşağıda gösterilmiştir.

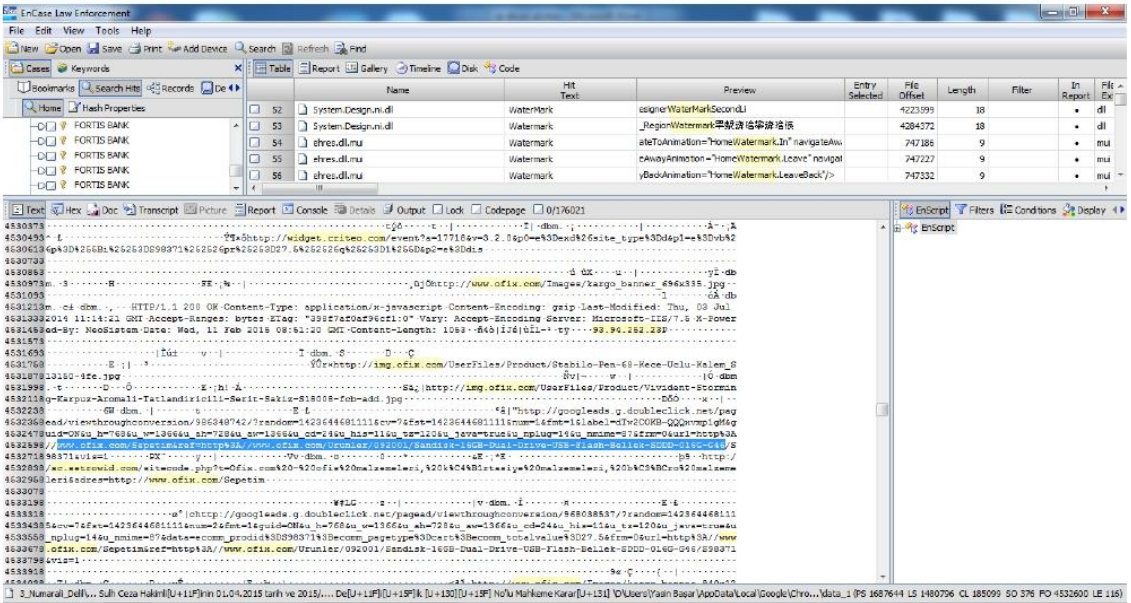




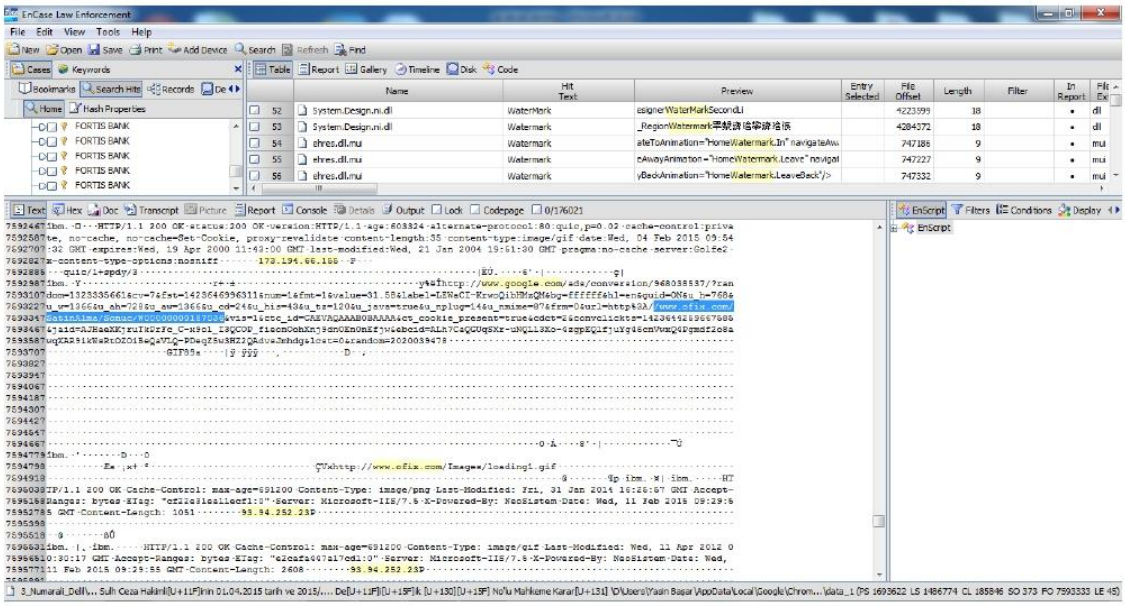
Suça Konu Mail Adresine Ait Ekran Çıktıları

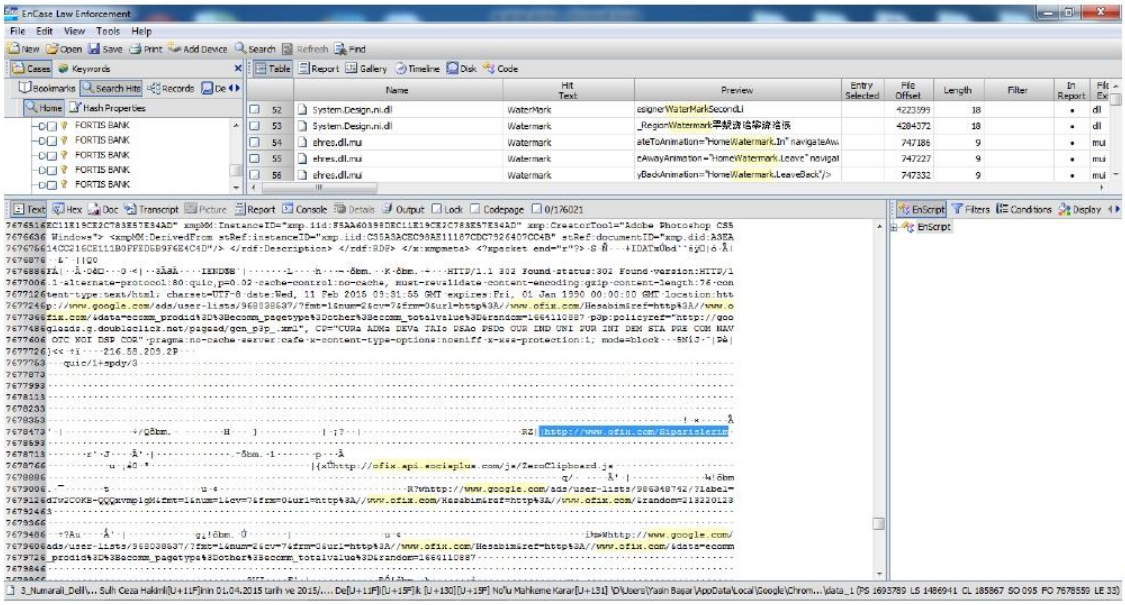
❖ **www.ofix.com** isimli web sitesi ile ilgili soruşturmaya konu alışveriş işlemine ait ekran çıktıları aşağıda gösterilmiştir. Tespit edilen alışveriş işleminde, aynı zamanda incelemeye konu 2 numaralı delil (Sandisk marka 16 GB USB bellek) siparişi yapıldığı anlaşılmıştır.





Sipariş Edilen USB Belleğe Ait Ekran Çıktıları

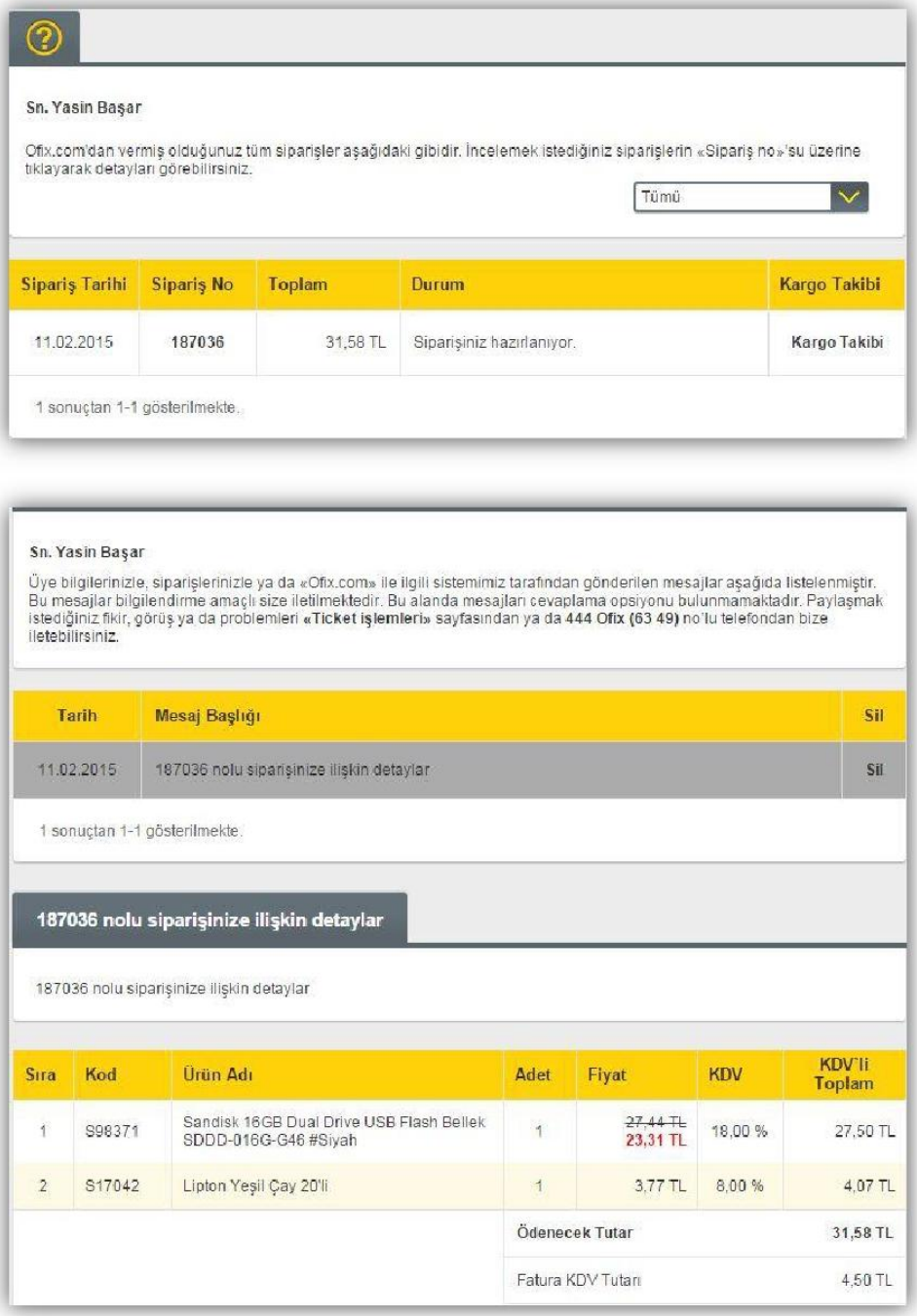




Suça Konu Sipariş İşleminin Tamamlandığına Dair Ait Ekran Çıktıları

❖ Sipariş neticesinde bilgilendirme amacıyla, **www.ofix.com** isimli web sitesi tarafından müşteriye bildirilen siparişe ait detay bilgileri ise, bilgisayarın fotoğraflar bölümünde kayıtlı olduğu tespit edilmiş olup, ekran görüntüleri aşağıda gösterilmiştir.

EK – 4 İnceleme Raporu (16. Sayfa)



Sn. Yasin Başar

Ofix.com'dan vermiş olduğunuz tüm siparişler aşağıdaki gibidir. İncelemek istediğiniz siparişlerin «Sipariş no»'su üzerine tıklayarak detayları görebilirsiniz.

Tümü

Sipariş Tarihi	Sipariş No	Toplam	Durum	Kargo Takibi
11.02.2015	187036	31,58 TL	Siparişiniz hazırlanıyor.	Kargo Takibi

1 sonuçtan 1-1 gösterilmekte.

Sn. Yasin Başar

Üye bilgilerinizle, siparişlerinizle ya da «Ofix.com» ile ilgili sistemimiz tarafından gönderilen mesajlar aşağıda listelenmiştir. Bu mesajlar bilgilendirme amaçlı size iletilmektedir. Bu alanda mesajları cevaplama opsiyonu bulunmamaktadır. Paylaşmak istediğiniz fikir, görüş ya da problemleri **«Ticket işlemleri»** sayfasından ya da **444 Ofix (63 49)** no'lu telefondan bize iletebilirsiniz.

Tarih	Mesaj Başlığı	Sil
11.02.2015	187036 nolu siparişinize ilişkin detaylar	Sil

1 sonuçtan 1-1 gösterilmekte.

187036 nolu siparişinize ilişkin detaylar

187036 nolu siparişinize ilişkin detaylar

Sıra	Kod	Ürün Adı	Adet	Fiyat	KDV	KDV'li Toplam
1	S98371	Sandisk 16GB Dual Drive USB Flash Bellek SDDD-016G-G46 #Siyah	1	~~27,44 TL~~ 23,31 TL	18,00 %	27,50 TL
2	S17042	Lipton Yeşil Çay 20'li	1	3,77 TL	8,00 %	4,07 TL
			Ödenecek Tutar			31,58 TL
			Fatura KDV Tutarı			4,50 TL

Siparişin Tamamlandığına Dair Bilgilere Ait Ekran Çıktıları

❖ İnceleme işlemi neticesinde bahse konu **4556 45** **** 2976** numaralı kredi kartının sipariş işlemi esnasında kullanılıp kullanılmadığı yönünde herhangi bir bilgi tespit edilememiştir.

EK – 4 İnceleme Raporu (17. Sayfa)

❖ Yukarıda tespiti yapılan ve soruşturma kapsamında delil olarak değerlendirilen bilgi ve belgelerin tamamı rapor ekindeki **Delil DVD**'si içerisinde bulunan **"3_Numarali_Delil"** isimli klasöre kopyalanmıştır.

SONUÇ VE KANAAT : 3 adet dijital materyal incelemesi neticesinde, 1 ve 2 numaralı deliller içerisinde bahse konu Banka ve/veya Kredi Kartlarının Kötüye Kullanılması suçu kapsamında bilgi ve belgelere rastlanılmış, 3 numaralı delil içerisinde ise her ne kadar doğrudan suçta kullanılan kredi kartı numarası bilgisinin tespiti yapılamasa da, suçta kullanılan IP numarası ile mail adresi bilgisinin bu delilde kullanıldığı tespit edilmiştir.

İnceleme işleminin tamamı değerlendirildiğinde, siparişe ait tespit edilen ve yukarıda belirtilen bilgi ve belgeler doğrultusunda şüpheli …….. …….. isimli şahsın suça konu eylemi gerçekleştirmiş olduğu yönünde kuvvetli kanaat oluşmuştur.

Arz ederim. 15/06/2015

Yasin BAŞAR
Polis Memuru
Adli Bilişim Uzmanı

E K İ : Delil DVD'si (1 Adet)