**TÜRKİYE CUMHURİYETİ**
**ANKARA ÜNİVERSİTESİ**
**SAĞLIK BİLİMLERİ ENSTİTÜSÜ**

# BİLİŞİM SUÇLARINDA ELDE EDİLEN DELİLLERİN OLAY YERİNDEN TOPLANMASI VE LABORATUVARDA İNCELENMESİ

**Kubilay SAY**

**DİSİPLİNLERARASI ADLİ TIP ANABİLİM DALI**
**FİZİK İNCELEMELER VE KRİMİNALİSTİK BİLİM DALI**
**YÜKSEK LİSANS TEZİ**

**DANIŞMAN**
**Doç. Dr. Mehmet ÖZCAN**

**2006 – ANKARA**

Ankara Üniversitesi Sağlık Bilimleri Enstitüsü

Disiplinlerarası Adli Tıp Anabilim Dalı

Fiziki İncelemeler ve Kriminalistik Bilim Dalı

çerçevesinde yürütülmüş olan bu çalışma,
aşağıdaki jüri tarafından
Yüksek Lisans Tezi olarak kabul edilmiştir.

Tez Savunma Tarihi: 27/11/2006

Prof. Dr. Tülin SÖYLEMEZOĞLU
Ankara Üniversitesi
Jüri Başkanı

Prof. Dr. Kayhan MUTLU
Orta Doğu Teknik Üniversitesi

Doç. Dr. Mehmet ÖZCAN
Polis Akademisi

Doç. Dr. Yaşar BİLGE
Ankara Üniversitesi

Yrd. Doç. Dr. Mehmet ARICAN
Polis Akademisi

# İÇİNDEKİLER

# ÖNSÖZ

Yapmış olduğum tez çalışmasında, bilgi ve zamanını benden esirgemeyen, çalışmamın her aşamasında bana yol gösteren, kendisinden çok şey öğrendiğim değerli danışmanım Sayın Doç. Dr. Mehmet Özcan'a teşekkürlerimi sunarım.

Adli Bilimler ile tanışmamı ve sevmemi sağlayan, bir bilim insanının nasıl olduğunun en güzel örneği olan değerli öğretmenim Sayın Prof. Dr. Tülin Söylemezoğlu'na özel teşekkürlerimi sunarım.

Dallarında Türkiye'nin önde gelen isimlerinden olan Sayın Prof. Dr. Kayhan Mutlu ve Sayın Doç. Dr. Yaşar Bilge'ye vurguladıkları yapıcı eleştirilerden dolayı teşekkür ederim.

Çalışmakta olduğum kurum olan Kriminal Polis Laboratuvarları Daire Başkanlığı Merkez Emniyet Müdürlerinden Sayın Dursun Kerimoğlu'na, polislik mesleği ve laboratuvar çalışma etiği konularında verdiği bilgilerden dolayı teşekkür ederim.

Tezimin araştırma safhasında gerekli istatistiki bilgi ve belgeleri kullanmam konusunda izin veren Ankara Kriminal Polis Laboratuvarı Müdürü Sayın Cem Ahmet Dönmez'e teşekkür ederim.

Birlikte çalışmaya başladığım andan itibaren kendilerinden çok şey öğrendiğim şube müdürüm Levent Bayram ve büro amirim Yunus Balı'ya teşekkür ederim.

Hayatımın her anında sonsuz sevgisini sunan aileme teşekkür ederim.

# ŞEKİLLER

# ÇİZELGELER

# 1. GİRİŞ VE AMAÇ

## 1.1. Genel Bilgiler

### 1.1.1. Suç Nedir?

Bilişim teknolojilerindeki gelişmeler, insan hayatını olumlu olduğu kadar olumsuz da etkilemektedir. Teknolojik cihaz ve sistemlerin suçluların kullanımına da açık olması, bu olumsuzlukları oluşturan etmenlerden biridir. Suç olgusu, varoluşun başlangıcından itibaren vardır. Suçlular ise başlangıçtan beri teknolojiyi kötü niyetlerini gerçekleştirmek amacıyla kullanmışlardır. Tarih içerisinde bıçakların, silahların, arabaların, suçluların amaçlarına ulaşmak için kullandıkları birer araç olabildiklerini görmekteyiz. (Brown, 1989)

Suçun farklı bilimler tarafından oluşturulmuş farklı tanımları vardır. Bu tanımların hukuk, sosyoloji ve kriminoloji bilimleri tarafından sık yapılan tanımları aşağıda irdelenmiştir. Suç kavramını anlamak, bilişim suçu kavramını tanımlarken yardımcı olacaktır.

“Suç kavramı medeniyetimizin başlangıcından günümüze kadar her devirde önemini korumuştur. İnsanoğlunun ortak kaynaklardan yararlanmak amacıyla toplum olarak bir arada yaşamak istemesi bazı problemleri de beraberinde getirmiştir. Sınırlı doğal kaynakların tükenmesi, çevre kirliliği, toplum baskısı

gibi unsurların yanında bu problemlerden biri de suç olmuştur. Genel olarak, ceza hukukuna göre suç: Yasanın cezalandırdığı harekettir." (Polat, 2004, s.:33)

Suçun ceza hukukuna göre yapılmış olan hukuki tanımına benzer olan kriminolojik tanımı, Türkiye'de Kriminoloji'nin kurucusu sayılan, Dönmezer tarafından aşağıdaki gibi yapılmıştır:

"Suç, evrensel, genel bir olaydır. Suç tarihin en eski devirlerinden itibaren var olmuştur ve ileride de var olmaya devam edecektir. Suçsuz bir toplum bir ütopyadan başka bir şey değildir. İnsanların içinde ihtiraslarla birlikte toplum halinde yaşamanın ortaya çıkardığı çeşitli sosyal çelişkiler, uyumsuzluklar bulundukça suçta var olacaktır. Suç bir bakıma, bazı kişilerin davranışları ve tutumları ile bunların içinde yaşadıkları grupta yerleşmiş davranış örnekleri ile arasında bir çelişkidir. Bu çelişki her zaman ve her yerde zorunlu olarak var olacağından, suç genel ve evrensel bir olay teşkil eder ve adam öldürme, hırsızlık gibi çeşitli suçların farklılığına rağmen bir çeşit bilimsel yönden gözlemin yapılması kabil ve bilimin konusunu oluşturan bir olay niteliği ile varlığını korur." (Dönmezer, 1994, s.:49)

"Suç kavramı, ceza hukukunda tanımlandığı gibi basit ele alınamayacak kadar karmaşık ve çok yönlüdür. Suç olgusuna; psikolojik, sosyolojik, ekonomik ve hukuksal yönleri kapsayacak bir anlayışla bakmak gerekir. Biraz daha açarsak, ceza normlarının bazı menfaatleri korumak için koymuş olduğu kuralları ihlal etmek, suç teşkil eden eylemi oluşturur. Bu konuda Michael ve Adler (1933) suçun yasal tanımını "Suçun en kesin ve en az belirsizlik içeren tanımı, onun

ceza kanunu tarafından yasaklanan davranış olduğudur.” şeklinde yapmışlardır.” (Polat, 2004, s.:31)

Suç olgusunun sosyologlar tarafında yapılan bazı tanımları izleyen paragraflarda belirtilmiştir.

“Suçluluğun sosyolojik görünümünün incelenmesi, 20. yüzyılda geniş ölçüde bir Amerikan yaklaşımı olmuştur. Sutherland, Sellin, Cohen gibi yazarlar suçun oluşmasında öğrenme, kültür çatışması, suçlu alt kültürünün etkileri üzerinde durdular.” (Dönmezer, 1994, s.:71)

“Son yirmi yıl içinde kriminolojik ve sosyolojik teori, giderek suçun, boyutları belli, bireysel ve sosyal patolojilerin sevk ettiği insan davranışının bilimsel bir kategorisini teşkil ettiği hususundaki faraziyeleri bertaraf etmektedir. Bugün sebepleri bulmaya yönelik modellerin keşfinin çok güç olduğu, suç kavramının çok karmaşık nitelik taşıdığı kabul edilmektedir.” (Dönmezer, 1994, s.:68)

“Edwin Sutherland suçun iki açıdan tanımlanabileceğini söylemiştir. Bir hareketin sosyal açıdan zararlı olarak yasal tanımı ve söz konusu hareket için verilecek cezanın yasal açıdan oluşması. Sutherland, bu fikrin oluşmasında beyaz yakalı suçu işleyenlerin, hem yakalandıklarında daha yumuşak muamele görmeleri hem de bu tip suçluların çoğunun asla tutuklanmaması olarak açıklamıştır.” (Polat, 2004, s.:33)

Konuya suçlu hakları açısından bakıldığı zaman ise suçun tanımı aşağıdaki gibi değişmektedir.

“Herman ve Julia Schwendinger (1970) suçu tanımlama yolu olarak yasal kurallardan çok temel insan haklarını belirleme yaklaşımı içerisindeydiler. Bu yazarlara göre, suçun tanımı kaçınılmaz olarak politiktir. Devletçe tanımı yapılan, kanuna tıpatıp riayet eden suç yaklaşımını kabul edenler belli bir devlet, statüko ve hizmet ettiği menfaatlerin işine yarama riskini almış olurlar. Örneğin, belli grupların insan haklarına saldırıda bulunulduğu 1930’ların Nazi Almanyası’ndaki bir kriminologun konumu buna iyi bir örnektir. İnsan hakları bakış açısından, devlet suçu tanımlayan bir otorite değil, suçun faili olarak kabul edilebilir.” (Polat, 2004 s.:32)

01.06.2005 tarihinde yürürlüğe giren yeni Türk Ceza Kanunu’nun 2. maddesinin 1. fıkrasına göre, “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.”

“Suç, bir hukuki değer ihlalini ifade eder. Temelinde hukuki değer koruması olmayan bir suç tanımı olamaz. Hukuki değer, bir hukuk toplumunda geçerli olan değerleri ifade eder ve dayanağını, davranış normları oluşturur. Belli bir kişiden soyut olan hukuki değer; ceza kanununda suçların tasnifi açısından kanun koyucuya yol gösterir ve uygulamacı açısından, suç tanımının yorumunda baş vurulacak en önemli enstrümanı oluşturur.” (Özgenç, 2005)

“Ceza Hukukunda suç, teknik - hukukî yani normatif maksatları karşılar şekilde değişik yazarlar tarafından çeşitli biçimlerde tarif edilmektedir. Ancak bu nevi hukukî nitelikli tariflerin bir olay, bir sapıcı davranış olarak suçun, kriminoloji yönünden de ele alınmasına esas teşkil edip edemeyeceği tartışmalıdır. Teknik-hukukî nitelikteki tariflerin sosyolojik bakımından itibarları daha az olmak gerekir; zira bu tariflere göre bir gün bu kanunlar ilga edilecek olursa toplum içinde suçun da kalkacağını kabul etmek gerekecektir. Oysa topluma zarar veren hareketler, kanunlar bunları tarif etmeden önceden de, mevcuttur. O halde önce çözümü gereken problem belirli hareketleri suç haline getirirken kullanılacak ölçüdür. Bu hususta ölçüler verilmesine çalışılmıştır. Sözgelimi Jhering’e göre suç “toplum halinde yaşama şartlarına yönelmiş her türlü saldırılardır”.” (Dönmezer, 1994, s.:45)

“Bu maksatla sosyolojik nitelikte tariflerin verilmesine de girişilmiştir. Durkheim’e göre “suç kolektif bilincin kuvvetli ve belirmiş tutumlarını (dispositions) ihlâl eden fiillerdir”. Thomas ve Znaniecky eserinde sosyal psikoloji yönünden meseleyi almak suretiyle şöyle bir tarif vermektedir: “Suç kişinin kendisini mensubu saydığı grupta, varlığı toplum dayanışması ile çelişki gösteren fiildir”. Taft’ın görüşü ise şöyledir: Topluma zarar veren hareketler ya örf ve âdetlerce belirlenmiştir yada grup içinde egemenliği elinde tutanlar, diğer kişilerin, tavır ve hareketlerini uydurmaları için modelleri, örnekleri ve bu suretle moral kuralların tümünü tespit ederler; bu kurallara uyanlara sosyal itibar verir, bunları ihlâl edenlere söz konusu mevkii reddederler.” (Dönmezer, 1994, s.:46)

Görüldüğü gibi bilim adamları tarafından, farklı açılardan bakıldığında, suçun farklı tanımları yapılmıştır.

“Stanciu’a göre, kriminolojide suç şu suretle tarif olunabilir: “Sosyal toplumun çoğunluğu tarafından tehlikeli sayılan ihmal yada icra niteliğinde hareketler”. Suç teşkil eden fiillere karşı kolektif müeyyideyi zorunlu kılan husus, bu hareketin ortaya koyduğu tehlikedir. Ceza Kanunun yasakladığı, müşterek hayat için zararlı olan bir harekettir. Bu tarif ele alınacak olursa, yazara göre Kriminolojinin konusuna, yalnız Ceza Kanunlarının tarif ettikleri değil ve fakat bunlarla beraber kanunların suç saymadığı ve fakat toplum için zararlı diğer hareketleri de girer.” (Dönmezer, 1994, s.:48)

Suç kavramının açıklanmasından sonra bilişim suçu kavramı, izleyen bölümde izah edilmeye çalışılacaktır.

### 1.1.2. Bilişim Suçu Nedir?

Bilgisayarların insanlar tarafından kullanılmaya başlaması çok eski bir tarihe dayanmamaktadır. Sadece çeyrek asırdır kullanılagelen bilgisayarlar, günümüzde insan hayatının hemen her alanına girmiştir. Evimizde, ofisimizde, bankalarda, marketlerde veya hava alanlarında bilgisayarlara rastlamak modern insanlar için artık günlük hayatın sıradan tesadüflerinden biri haline gelmiştir. Bu kadar kısa süre içerisinde bilgisayarların hayatımızın her alanına bu denli girmelerinin sebebi, insan hayatını fazlasıyla kolaylaştırmalardır. Banka veznelerinde sıra beklemektense, ATM’lerden[1] para çekmek hepimize daha kolay gelmektedir. ATM’ler ise sadece bankacılık ağlarına bağlantıları olan bilgisayarlardır. İnsanlar gibi bilgisayarlar da hata yapabilirler. Fakat bilgisayarlar, insanlar tarafından yasal olmayan işlerde kullanılırsa, suç oluşur.

[1] ATM (Automated Teller Machine), Otomatik Vezne Makinesi, Bankamatik.

Suçun oluşmasında insan iradesi şarttır. Bilgisayar dolaylı yollardan da suça azmettirilebilir. Bir virüs kontrolündeki bilgisayar tarafından başka bir hedefe saldırı olursa, elbette ki bu suçu işleyen virüs yazarıdır. Bilgisayar sahibi değildir.

Aynı ortamda bulunan bilgisayar sayılarının artmasıyla beraber, ortak kaynakları (yazıcı, tarayıcı, ağ diski vb.) kullanmak amacıyla ağ teknolojileri geliştirilmiştir. Bir kurumdaki bilgisayarlar birbirleriyle iletişim kurarlarsa ortak iş gücüne katkıda bulunabilirler.[2] Artan bilgisayarlararası iletişim ihtiyacını karşılamak ve olası bir ulusal güvenlik tehdidi ortaya çıktığında savunma birimleri arasındaki koordinasyonu sağlamak amacıyla Amerikan Savunma Bakanlığı[3], 1968 yılında ARPANET[4] adlı bir iletişim ağı geliştirdi. Adından da anlaşılacağa üzere ilk paket anahtarlamalı[5] ağ olan ARPANET, İnternet'in atası sayılmaktadır.[6] Yani İnternet'in doğuşu savunma amacına dayanmaktadır. Öncelikle Amerika Birleşik Devletleri'nde üniversite ve kamu kuruluşlarındaki bilgisayarlar ARPANET aracılığıyla birbirlerine bağlanmaya başladı.[7] Fakat bu kontrolsüz büyüme bazı problemleri de beraberinde getirdi. İlk başlarda bilgisayarlar arası iletişiminde kullanılan protokoller ve işletim sistemleri güvenlik faktörü gözetilmeden, sadece iletişimin hızlı olması faktörü düşünülerek geliştirilmişti. Bu zafiyet bir bilgisayardan diğer bilgisayara yetkisiz erişime zemin hazırlıyordu. O yıllarda İnternet küçük bir ağ olduğu için, bu yolla işlenen suçların sayısı önemsenmeyecek kadar azdı. Ancak İnternet geliştikçe, suç oranı da arttı. İnternet'in uluslararası kulvara taşınmasıyla suçların boyutu da sınır aşan suçlar kapsamına girdi. İnternet'in uluslararası cazibe merkezi haline gelmesi ve üzerinde ticari uygulamaların

[2] http://en.wikipedia.org/wiki/Computer_networking, Erişim Tarihi: 10.06.2006
[3] U.S. Department of Defense
[4] Advanced Research Projects Agency Network
[5] Paket anahtarlamalı ağlarda veriler, devre anahtarlamalı ağlarda olduğu gibi sadece iki nokta arasında değil, daha fazla nokta arasında iletilebilmektedir.
[6] http://www.websters-online-dictionary.org/definition/arpanet, Erişim Tarihi: 21.04.2006
[7] http://en.wikipedia.org/wiki/Arpanet, Erişim Tarihi: 10.06.2006

işletilmeye başlanması, suçluların iştahını kabartmaya yetti. Terör örgütleri de İnternet'in önemini anlayarak sanal ortam sayılan İnternet'te yerlerini aldılar. Yani suçlusuyla, mağduruyla gerçek dünyanın kopyası sadece 1 ve 0'lardan oluşan dijital bir ortama taşınmış oluyordu.

İlk kişisel bilgisayarların, 1981 yılında seri üretilmeye başlanmasıyla beraber, bu sistemlerin insan hayatı üzerindeki nüfuzu artmaya başlamıştır.[8] Bilgisayarlar erken dönemlerinde sadece gelişmiş laboratuarlar, büyük şirketler ve üniversiteler gibi yüksek bütçeli kurumlarda bulunmaktaydı.[9] Bilgisayarların evlerde, okullarda ve ofislerde kullanılması fikri, ilk başta insanların tepkisine yol açmış, hacmen ve maddi olarak yüksek değerlerde olan bu cihazların kişisel kullanıma geçmesinin gereksiz olduğu düşünülmüştü. Bu konuda büyük bilişim şirketi yöneticileri bile şöyle söylemişlerdir:

> "İnsanların evde bilgisayar kullanmaları için hiçbir sebep göremiyorum."[10]

> "640 Kilobayt hafıza, bütün insanlar için yeterlidir."[11]

Ancak elektronik sanayisindeki gelişmeler sonucu, kısa süre içerisinde bilgisayarların küçük boyut ve düşük maliyetlere mal edilmesi, bilgisayarların

[8] http://en.wikipedia.org/wiki/Personal_computer
[9] http://www.webopedia.com/TERM/P/personal_computer.html
[10] OLSEN, Ken, Digital Corporation Başkanı, 1977, "There is no reason anyone would want a computer in their home."
http://en.thinkexist.com/quotation/there_is_no_reason_for_any_individual_to_have_a/213208.html, Erişim Tarihi:10.06.2006
[11] GATES, Bill, Microsoft Corporation Başkanı, 1981, "640K ought to be enough for anybody."
http://whatis.techtarget.com/definition/0,,sid9_gci534467,00.html, Erişim Tarihi: 10.06.2006

insan yaşamına girme süresini kısalttı. Geçen kısa süre boyunca, insanlık şimdiye dek hiçbir çağda görülmemiş bir yükseliş ivmesine tanık oldu ve böylece bilgisayar sistemleri hayatın her alanında kullanılmaya başlandı.[12]

IBM firması, ilk kişisel bilgisayarı, 1981'in Ağustos ayında piyasaya sundu.[13] Bu tarihten önce üretilmiş olan Apple, MITS, TRS ve Bell marka bilgisayarlar üretilmişti. Ancak bu bilgisayarlar, yüksek fiyat ve seri üretime geçilmemesi gibi nedenlerden dolayı kişisel bilgisayar olarak değerlendirilmemektedir. Bu nedenle dünya tarafından, ilk kişisel bilgisayar IBM firmasının PC5150 modeli olarak kabul edilmektedir. Bu yıllarda üreticiler de dahil herkeste bilgisayarların kişisel kullanıma kolay kolay geçemeyeceği düşüncesi hakimdi. IBM PC geliştirme takımının lideri William Lowe: "PC5150'nin fiyatının $1,565'a gerilemesi sadece 8 ay içerisinde dünya çapında 50,000 adet kişisel bilgisayarın satılmasına neden oldu."[14] demiştir. Kişisel bilgisayarlara PC[15] denmesinin nedeni, seri üretime geçen ilk bilgisayarın IBM'in PC5150 modeli olmasındandır. Bu nedenle günümüzde üretilen bilgisayarlar hâla "IBM PC Compatible Computer[16]" olarak adlandırılmaktadır.

Aslında IBM firması sadece kendi ürettiği bellek, sabit disk, anakart gibi bileşenler ile uygun olan bileşenleri bir araya getirerek bir ürün ortaya çıkartmıştı. Microsoft firmasından MS-DOS[17] işletim sistemini, Intel firmasından 8088[18] işlemcisini kullanarak IBM PC5150'yi üretmişti.

---

[12] Internet Society (ISOC) All About The Internet: History of the Internet http://www.isoc.org/internet/history/brief.shtml
[13] IBM (International Business Machines) Archives, http://www-03.ibm.com/ibm/history/exhibits/pc/pc_1.html
[14] http://www.reference.com/browse/wiki/IBM_PC Erişim Tarihi: 11.02.2006
[15] Personal Computer
[16] IBM PC uyumlu bilgisayar
[17] Microsoft Disk Operating System
[18] http://en.wikipedia.org/wiki/8088, Erişim Tarihi: 10.06.2006

“IBM’in 1981 yılında ilk kişisel bilgisayarı piyasaya sunmasıyla beraber yeni bir çağ başlamış oluyordu: Bilişim Çağı.”[19]

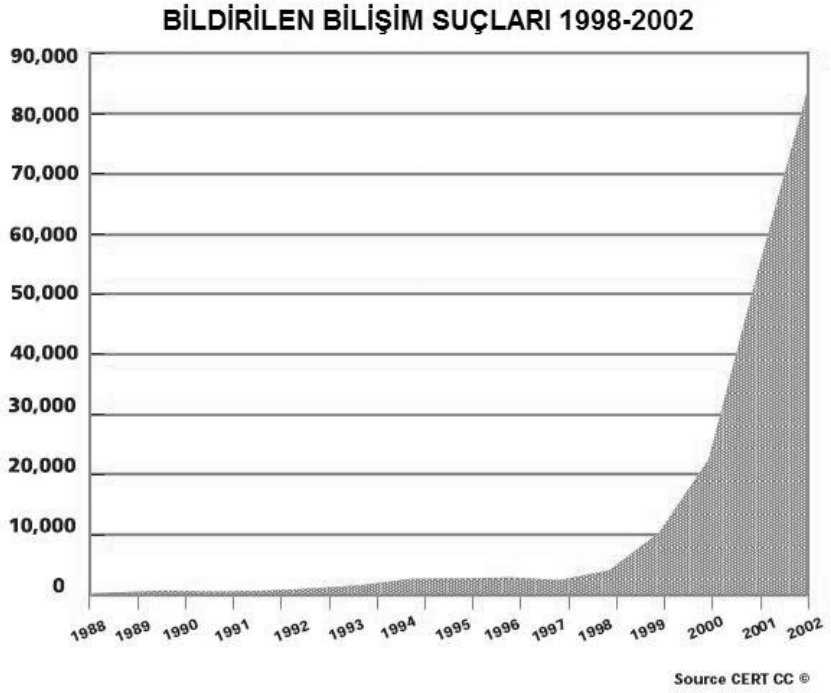
Transistörlerin entegre devrelere, entegre devrelerin işlemcilere, işlemcilerin bilgisayarlara olan evrimi, tarih boyunca görülmüş, insan toplumunu etkileyen en önemli olaylar aşamasından biri olmaya adaydır.

“Bu gelişmelerin tam aksine insanlığın ilk günü ile birlikte ortaya çıkan “iyi” ve “kötü” kavramları hiç değişmeden günümüze kadar gelmiştir. Sanayi devrimi ile ortaya çıkan teknolojik gelişmeler özellikle savaş sanayindeki buluşlar, “iyilere” olduğu kadar “kötülere” de olanaklar sunmuş, insanlığın mahvına neden olabilecek yeni silahlar ortaya çıkmıştır.” (Özcan, 2004, s.:178)

İnsanoğlunun var oluşu kadar eski olan, iyi ve kötü kavramları günümüzde de geçerliliğini korumaktadır. Bir bıçağın, yemek yapmak kadar insan yaralamakta da kullanılması gibi, bir bilgisayar da işlerimizi kolaylaştırmak ya da insanlara zarar vermek amacıyla kullanılabilmektedir. Suçlular, teknolojiyi aynen iş adamlarının kullandığı gibi kullanmaktadırlar. (Curtis, 2000, s.:3)

Geçen çeyrek asırda teknolojik gelişmelerde yaşanan değişimler, suç oranlarında artışa neden olmuştur. Yirmi yıl önce “bilişim suçları” tabiri, suç terminolojisinde sık rastlanılan bir olgu değildi. Bilişim suçlarının dünya çapında artışına ilişkin istatistiki veriler aşağıdaki grafiklerde görülmektedir.

[19] http://en.wikipedia.org/wiki/Information_age, Erişim Tarihi: 11.02.2006




Şekil-1.1: Birleşik Devletler, Carnegie Mellon Üniversitesi, CERT-CC (Community Emergency Response Team - Coordination Center), Dünya Çapında Bilişim Suçu İstatistikleri.[20]

| | Vakalar | Suçlar | Mağdurlar | Bilinen Suçlar | Bilinmeyen Suçlar |
|---|---|---|---|---|---|
| **TOPLAM** | 5428613 | 5856985 | 5845031 | 4078106 | 2025419 |
| Sahte e-mail ile dolandırıcılık | 61230 | 61230 | 66095 | 63304 | 6888 |
| Kredi kartı dolandırıcılığı | 23308 | 23308 | 26492 | 20568 | 6303 |
| Sosyal mühendislik dolandırıcılığı | 8689 | 8689 | 9500 | 8980 | 1019 |
| Bağış dolandırıcılığı | 1289 | 1289 | 1300 | 1344 | 27 |
| Telefon faturası dolandırıcılığı | 984 | 984 | 1074 | 808 | 281 |
| Rüşvet | 191 | 191 | 198 | 233 | 5 |
| Sahtecilik | 91697 | 91697 | 110545 | 85797 | 21201 |
| Zimmet | 20694 | 20694 | 21356 | 24506 | 1738 |
| Sabotaj | 10 | 20 | 5 | 23 | 0 |

Şekil-1.2: Birleşik Devletler, Adalet Bakanlığı, Federal Soruşturma Bürosu, Ceza Adaleti Bilgi Servisi, Birleşik Devletlerde Beyaz Yaka Suçları İstatistikleri.[21]

[20] The White House, Washington, The National Strategy To Secure Cyber Space February, 2003
[21] Federal Bureau of Investigation,, The Measurement of White-Collar Crime, 2004

Bilgisayarların daha fazla ucuzlaması ve iletişim imkânlarının gelişmesi, devletleri ve insanları "bilişim suçları" tehdidiyle karşı karşıya bıraktı. Bilişim suçlarının işlenme oranı, küreselleşmenin verdiği ivmeyle artmaktadır. Küreselleşen dünyanın sinir sistemi olan İnternet, bilişim suçlarının artmasına müspet katkılarda bulunmaktadır. Bu nedenle İnternet tek başına ele alınması gereken bir fenomen haline gelmiştir.

Suç olgusunun bir çok tanımı olduğu gibi bilişim suçunun da bir çok tanımı yapılmıştır. En kısa tanımıyla "bilişim sistemleri kullanılarak işlenen suça" denir. Ancak bilişim sistemlerinin çok farklı tiplerde olmasından ve bu sistemler ile işlenebilecek suç türlerinin de bir o kadar çeşitli olmasında 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 konularak, tanımlanması gerekmektedir.

Birleşik Devletler, Colorado Eyaleti, bilgisayar suçları hakkındaki kanuna[22] göre;

> "Bilgisayar, bilgisayar sistemi, bilgisayar ağı ya da elektronik herhangi bir donanım kullanılarak; dolandırıcılık, haksız kazanç ya da mal elde etmek, veya bir bilişim sisteminin akışına yetkisiz erişim ile etki etmek ya da durdurmak eylemine bilişim suçu denir." Bu tanımda; Bilgisayar: Mantıksal, aritmetiksel ve hafıza fonksiyonlarını, elektronik ve manyetik özelliklerini kullanarak, giriş birimlerine uygulanan bilgileri, işleyerek veya depoladıktan sonra çıktı birimlerine ileten cihazdır. Bilgisayar sistemi: Bilgisayarla ilgili, ona bağlı ve bağlı olmayan cihazlar veya

[22] Colorado State, U.S. Law 18-5.5-102, Title 18: Criminal Code, Article 5.5: Computer crime

> yazılımlardır. Bilgisayar ağı: İletişim ağları (mikrodalga, kablosuz vb. iletişim teknolojileri dahil) yoluyla birbirine bağlanmış uç terminaller ve bilgisayarların oluşturduğu sistemdir. Yetkisiz erişim: Bilgisayar veya bilgisayar sisteminin asıl sahibinin rızası olmadan söz konusu sistemlerin diğer kişi tarafından kullanılması veya kullanıma açılmasıdır.”

Birleşik Devletler, Adalet bakanlığına göre, bilişim suçu; Bilişim teknolojisi kullanılarak yapılan her türlü yasadışı eylemdir.

Avustralya, Sydney Üniversitesi, Bilişim Sistemleri Fakültesi öğretim üyesi, Dr. Jim Underwood, bilişim suçunu; “Geleneksel suçlardan olan, hırsızlık, dolandırıcılık, sahtecilik ve cinsel istismar gibi suçların, bilgisayar veya bilgisayar ağı kullanılarak işlenmesi” olarak tanımlamıştır.

“Bilişim suçlarıyla ilgili olarak karşımıza birçok tanım çıkmaktadır: bilgisayar suçları, dijital suçlar, İnternet suçları, siber suçlar, ileri teknoloji suçları gibi. Aslında her tanım bize bir açıklık getirmektedir. Çünkü bu tür suçlar, bir bilgisayar vasıtasıyla işlenebileceği gibi yerel bilgisayar ağları veya İnternet’e bağlı birden fazla bilgisayar üzerinden de işlenebilmekte ya da basit bir elektronik devre veya kredi kartı da kullanılabilinmektedir. Bilişim kavramı bilgisayar teknolojileri ile iletişim teknolojilerini kapsadığından bu suçlar “Bilişim Suçları” adı altında tanımlanmıştır. Dolayısıyla bilişim suçları terimi kullanıldığında, bahsedilen bu teknolojileri kullanarak işlenen bir suç unsuru olduğu unutulmamalıdır.” (Yılmaz, 2001)

Suç ve cezada kanunilik ilkesi bilişim suçlarında da geçerlidir. Ancak, bu ilkeye bağlı kalınırken, bilişim suçlarının kendine özgü bünyesi mutlaka göz önüne alınmalıdır. Bilişim suçlarının işlenebilmesi için; a) bilgisayar veya benzeri bir aygıt, b) Enerji (güç) kaynağı; (bilişim ağı var ise ayrıca) c) Ağ bağlantısı ve bunu sağlayan telekomünikasyon hattı gerekmektedir. Bu yapı içerisinde, bilişim suçu sayılan fiiller, bizzat bilişim sisteminin içerisinde veya bilişim sisteminden etkilen pek çok sahada sonuç doğurabilir. Genellikle, bilişim suçlarında, bilişim sistemine girerek, bilişimden etkilenen diğer alanlara zarar vermek amaçlanmaktadır. (Karagülmez, 2005, s.:31)

Görüldüğü gibi bilişim suçları kavramı hakkında birçok tanımlamaya gidilmiştir. Konunun özü itibarıyla geniş bir çalışma sahasını kapsaması nedeniyle yapılan her tanım, bilişim suçlarının farklı bir yönünü ortaya koymaktadır. Türkçemizin güzelliği sayesinde, dilimizde bulunan “bilişim” sözcüğünü kullanarak adlandırılan “bilişim suçu” kavramı, bilişim ile ilintili her tür suçu kapsamaktadır.

Geleneksel suçların da bilişim sistemleri kullanılarak yapılıyor olması olayın vahametini arttırmaktadır. Yeni yürürlüğe giren modern ceza kanunlarında bilişim suçları, “nitelikli suçlar” kapsamına alınmaktadır. Yeni Türk Ceza Kanunu’nun 142. maddesinde “(1) Hırsızlık suçunun; ... e) Bilişim sistemlerinin kullanılması suretiyle, ... İşlenmesi hâlinde, üç yıldan yedi yıla kadar hapis cezasına hükmolunur.” Aynı kanunun 158. maddesine göre, “(1) Dolandırıcılık suçunun; ... f) Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle, ... İşlenmesi hâlinde, iki yıldan yedi yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur.” maddelerinde belirtilerek bilişim sistemleri ile işlenen suçlara caydırıcılık getirmek amacıyla, yaptırımının arttırılması sağlanmıştır.

Bilgisayarlar insanın günlük yaşamının her alanında yer almaktadır. Bir zamanlar bir oda büyüklüğünde olan bilgisayarlar, günümüzde elde taşınabilmektedir. Bu avantaj masum insanlar için kolaylık anlamına geldiği gibi, suçlular için de aynı anlamı taşımaktadır.

Bilgisayarların gelişiminin yanında bir çok devrim yaşandı. Bunlardan en etkili olanlarından biri de İnternet'dir. Bu süper bilgi otoyolu ticari işlemlerin gerçekleştirildiği en önemli ortamlardan biri haline geldi. Diğer bir gelişme ise bilgisayarların depolama kapasitelerinde gerçekleşti. 1980 öncesinde, dahili depolama kapasitesi olmayan bilgisayarların, kayıt kapasitesi sadece 360 Kilobayt'lık harici disketlerle sınırlıydı. Bugün ise standart bir bilgisayarın depolama kapasitesi 50 milyon Kilobayt'a ulaşmıştır. Akademik, kamu ve iş kurumları tarafından kullanılan bilgisayarların kapasiteleri ise 100 milyon Kilobayt'larla ölçülmektedir. 64 Kilobayt'lık taşınabilir hafıza kartlarından 64 milyon Kilobaytlık hafıza kartlarına geçildi. Kişisel dijital asistan olarak adlandırılan el bilgisayarları, milyonlarca Bayt bilgi depolayabilirler.[23] Ayrıca bu tür asistanlar adres defterleri, randevu takvimleri, dokümanlar, e-posta mesajları, şifreler, telefon defterleri, metin belgeleri ve ses mesajlarını saklayabilme özelliğine sahipler. Hatta GPS (Global Positioning System, Küresel Konumlandırma Sistemi) özelliğine sahip sistemler nerede kullanıldıkları bilgisini belli ederler. Teknolojideki bu büyük patlamalar adli bilişim alanında yürütülen çalışmaları daha karmaşık bir hale sokmuştur. (Whitcomb, 2002, s.:2)

[23] http://en.wikipedia.org/wiki/Personal_digital_assistant (PDA: Personal Digital Asistant, Kişisel Dijital Asistan)

### 1.1.3. Adli Bilişim

Adli bilişim, adli bilimler gibi geniş bir çalışma sahasını kapsamaktadır ve sahanın genişleme ivmesi bilişim teknolojisinin modern yaşamı etkilemesiyle doğru orantılıdır. Basitçe adli bilişim disketlerden, sabit disklerden ve çıkarılabilir disklerden veri kurtarmaktır. (Schweitzer, 2003) Bu veriler, bilgi saklamak amacıyla kullanılan medyaların aktif alanlarında, silinmiş alanlarında veya artık alanlarında bulunabilir. Bu tür medyalarda bulunan bilgiler gün geçtikçe artmaktadır.

Adli bilişim, dijital delillerin muhteva ettiği bilgileri; delil inceleme prosedürlerini, hukuki ve etik sorumlulukları göz önünde bulundurarak; delilin bütünlüğünü koruyarak ve gerçeği açığa çıkarmak amacıyla; kopyalama, belirleme, çözümleme, yorumlama ve belgeleme sürecidir.

Adli bilişim sürecinde:

Kopyalama, elde edilen delilin kontamine olmaması için orijinal delilin birebir kopyasının oluşturulmasını,

Belirleme, olay yerlerinde bulunan bilişim ile ilintili bulguların tespit edilerek, tüm incelemeler yapılana kadar delil kabul edilmesini,

Çözümleme, kopya delil üzerinde, olayla ilgili anahtar kelime gibi mantıksal aramaların yapılmasını,

Yorumlama, dijital delil içerisinde bulunan verilerin olayla ilişkisini belirlemeyi,

Belgeleme, olay konusu ve bulunan veriler arasındaki ilişkiyi açıklayan rapor yazılmasını,

kapsamaktadır.

Adli bilişim incelemelerinin yürütülmeye başlandığı ilk zamanlarda, elde edilen dosyalar genellikle metin dosyaları, çalışma sayfaları veya resimler gibi basit dosyalardı. (Whitcomb, 2002, s.:3) Günümüzde kullanılan dosya türleri ise şifrelenmiş, sıkıştırılmış veya stenografik tekniklerle işlenmiş dosyalardır. Bilgisayarlarda bulundurulan dosyaların çeşitliliği artmıştır. İşletim sistemlerine ait, ayar, hafıza veya geçici dosyalar bunlara örnektir. Modern yazılımlar kendi geçici dosya dizinlerine sahiptirler. Mesela bir dokümanı kağıda yazdırma işlemi sırasında sayfalar, işletim sistemi tarafından yazdırma sırasına konulmaktadır. Sıraya konulmuş olan bu dosyalar muhtemel bir suçun delilleri olabilir. Aynı şekilde İnternet tarayıcıları ise kullanıcı tarafından ziyaret edilmiş olan sayfaları ve kullanıcı bilgilerini tutmaktadırlar. Birçok sıradan kullanıcı çalışırken genellikle bu dosyaların farkına bile varmamaktadır. Tüm işlemler, işletim sistemi tarafından arka planda yapılmaktadır.

“Adli bilişim'in kökleri ilk olarak bir sistem yöneticisinin, sistemine giren davetsiz bir misafirin, ne zaman ve nasıl girdiğini araştırması ile başlamıştır. O zaman, bu olayın araştırılmasına bir suç araştırmasından çok söz konusu sistemin zayıf taraflarını ortaya çıkaran bir test olarak bakılmıştı. Bilgisayarların akademik dünyadan, iş ve kamu dünyasına girmeye

başlamasıyla beraber risk faktörünün de ne kadar büyük olduğu görüldü. Çünkü teşebbüs edilen izinsiz girişler bilişim sistemlerini kontrol etmekten ziyade bilgi hırsızlığına veya zimmete para geçirmeye yönelikti. Daha fazla sistemin birbirine bağlanması bu tür vakaların gerçekleşmesi ihtimalini arttıran diğer bir faktördür. Bilgisayar kullanıcılarının, işlerini bilgisayarlar ile halletmek istemeleri bilgisayar yazılımlarına olan ihtiyacın artmasına neden oldu. Daha fazla yazılım ise bilgisayarda depolanan daha fazla dijital delil demektir." (Potaczala, 2001, s.:3)

"Amerika Birleşik Devletleri'nde dijital delillerin mahkemeler tarafından kabulü yaklaşık 30 yıl öncesine kadar dayanmaktadır. İlk başlarda hakimler gelen dijital delilleri kabul etmekte diğer deliller ile bir farklarının olmadığını düşünerek tereddüt etmediler. Bilişim teknolojileri geliştikçe kabul edilen dijital delillerin geleneksel diğer delil türlerine (kan, kovan, DNA, vs.) göre farklılıklarının olduğu anlaşıldı. 1976 yılında Birleşik Devletler Federal Delil Kuralları bu farklılıkları kapsayan bazı revizyonlar geçirdi." (Potaczala, 2001, s.:4)

"Dijital delillerin bulunabileceği muhtemel diğer yerler de yazıcılardır. Bazı türleri dokümanları saklayabilecek kapasitede belleklere sahiptir. Hatta büyük ağ yazıcılarının yazdırılacak sayfaları kaydeden sabit diskleri vardır. Yazıcı kafaları, tonerleri ve kartuşları bir belgenin hangi yazıcıdan çıktığı konusunda fiziksel belirteç izlere sahip olabilirler." (Marcella ve Greenfield, 2002, s.:23)

Bilgisayarların birbirine bağlanmasıyla oluşturulan ve ortak kaynaklara erişimi kolaylaştıran bilgisayar ağları, bir suça ait delilleri tespit etmek için araştırılacak olası yerlerden biridir. Ağların büyümesi ve İnternet'e

bağlanması, suçluların bulunmasını ve delil toplama sürecini zorlaştırmaktadır. Ağların fiziksel olarak geniş bir alana yayılması nedeniyle muhtemel sanık sayısı artmaktadır. Fakat ağ üzerinden işlenen suçları önlemek için ön tedbirlerin alınması daha kolay olmaktadır. Mesela bir hizmetin yerine getirilmesi amacıyla kurulan ana bilgisayarın üzerinde gerçekleşen girdi ve çıktıların başka bir bilgisayar sistemi tarafından izlenmesi, suç fiilinin oluşmasının ardından ele geçirilecek delillerin maddi geçerliliğini arttıracaktır. Bilgisayar ağları üzerinden işlenen suçlar genellikle: dolandırıcılık, cinsel istismar, bilgisayar sistemine izinsiz giriş, sahtecilik, tehdit, şantaj, hakaret, kumar, kimlik hırsızlığı ve telif hakları ihlali olmaktadır.

Bilişim suçlarını araştırırken iki tür inceleme yöntemi kullanılabilir: eşzamanlı ve eşzamansız inceleme. Bunlardan hangisinin seçileceği vakaya bağlıdır. Ağ üzerinden işlenmiş bir suçu araştırmak için eşzamanlı inceleme yöntemini kullanmak gerekmektedir. Çünkü suç halen işlenmekte olabilir. Eğer suç konusu bilgisayar tamamen kontrol altına alınmış ise eşzamansız inceleme yöntemini kullanmak mümkündür. Eşzamanlı bir inceleme yürütürken genellikle hedefimiz ağ üzerinde gerçekleşen aktivitenin izini sürmektir. Bu süreç ağda işlenen suçun gerçekten işlenmiş olduğu kararıyla başlatılır. Daha sonra nasıl ve ne zaman olduğunu tespit araştırmasına gidilir. Tespit etmesi zor olan fakat araştırmacının işini kolaylaştıracak diğer bir bilgi de saldırının nerden gerçekleştirilmiş olduğudur. Eğer saldırı veya izinsiz giriş İnternet üzerinden yapılmış ise şüpheli dünya üzerinde herhangi bir yerde olabilir. Bu tür suçları soruşturmak bazen birden fazla birimin veya ülkelerin polis gücünün ortak çalışmasını gerektirir ve sınır aşan suçlar kapsamına girer. İzinsiz girme teşebbüsünü destekleyen deliller bilişim sistemlerinin log[24] dosyalarından elde edilebilir. Log dosyaları her işletim sistemine veya yazılıma göre değişebilir. Bu tür araştırmalara başlamadan önce gerekli

[24] Log: Kütük, günlük, Saja English-Turkish Dictionary

hazırlıkların yapılmış olması gerekir. Eşzamanlı araştırma yönteminin diğer bir dezavantajı ise muhtemel delillerin bulunabileceği sistemlerin servis dışı bırakılırsa, maddi ve prestij kaybı yaratabilecek olmasıdır. Bu tür sistemler büyük firmalara veya kuruluşlara ait sunuculardır. Böyle durumlarda araştırıcı tarafından gerekli görülen dosyalar, sistemin işleyişi değiştirilmeden başka bir ortama kopyalanmalıdır. Suçla ilgili bilgileri toplamaya başlamadan önce yapılması gereken ilk adım elde edilen delillerin birebir kopyasını almak olmalıdır. Bazı durumlarda delilin kopyasının optik disk ortamlarına aktarılması gerekebilir. Bunun nedeni delilin kontrolümüz dışında (bilgisayar virüsleri) her hangi bir şekilde değiştirilmemesini sağlamak içindir. Değiştirilmemesi gereken bilgiler, dosyaların oluşturulma, değiştirilme zamanları ve sahip haklarıdır.

Araştırmalar yürütülürken dikkat edilmesi gereken bir önemli diğer husus delile uygulanan tüm işlemlerin araştırıcı tarafından kaydedilmesidir. Delil zinciri prensibine göre kayıtlar; delillere nasıl el konulduğunu, değiştirilmemesi için neler yapıldığı ve kopyasının alınması için ne tür işlemler yapıldığı bilgilerini içermelidir. Ayrıca kopya alma işlemi sırasında ne tür medyaların kullanıldığı, kullanılan işletim sistemi ve yazılımlar belirtilmelidir. Bu prensiplere dayanılarak oluşturulan kayıtlar yardımıyla, adli rapor yazmak daha kolay olacaktır.

## 1.2. Bilişim Suçlarında Olay Yeri İncelemesi

### 1.2.1. Olay Yeri İncelemesinin Hukuki Boyutu

Adli ve Önleme Aramaları Yönetmeliği'nin 5. maddesine göre: "Adlî arama, bir suç işlemek veya buna iştirak veyahut yataklık etmek makul şüphesi altında bulunan kimsenin, saklananın, şüphelinin, sanığın veya hükümlünün yakalanması ve suçun iz, eser, emare veya delillerinin elde edilmesi için bir kimsenin özel hayatının ve aile hayatının gizliliğinin sınırlandırılarak konutunda, işyerinde, kendisine ait diğer yerlerde, üzerinde, özel kâğıtlarında, eşyasında, aracında 5271 sayılı Ceza Muhakemesi Kanunu ile diğer kanunlara göre yapılan araştırma işlemidir." Bu yönetmelik, kolluk tarafından, kişilerin üstlerinin, eşyasının, araçlarının, özel kâğıtlarının, konut, işyeri ve eklentilerinin aranmasında uyulacak esas ve usulleri kapsamaktadır.

Aynı yönetmeliğin 9. maddesine göre: "Suç işlenen yerlerde, sebep ve sonuç ilişkisini ortaya koyacak delillerin aranması, bulunması ve el koyulması için geliştirilmiş bilimsel ve teknik araştırma işlemlerinin, herkesin girip çıkabileceği kamuya açık alanlarda yapılması için bir emir veya karar gerekmez."

"Adli Önleme ve Aramaları Yönetmeliği'ne göre hâkim kararının olması şartıyla suç yerlerinde veya suç yeri olması muhtemel yerlerde incelemeler yürütme yetkisi kolluk kuvvetlerine verilmiştir. Yönetmeliğe göre, adli aramaya karar verme yetkisi, hâkimde olacak. Kolluk, arama kararı alınmasını

talep ettiği durumlarda, makul şüphe sebeplerini belirten ayrıntılı ve gerekçeli bir rapor hazırlayacak ve Cumhuriyet savcısına başvuracaktır.” (Atasoy, 2006)

Adli Önleme ve Aramaları Yönetmeliği’ne dayanarak olay yeri incelemesini; suçun aydınlatılması amacıyla olay yerlerinde her türlü iz, eser, emare ve delil niteliği taşıyabilecek bulguların uzmanlaşmış personelce, çeşitli bilimsel, teknik yöntem ve metot kullanarak araştırılması, elde edilen bulguların tespit edilmesi ve kayıt altına alınması (belgelenmesi), toplanması, muhafazası ve incelenmek üzere ilgili yerlere gönderilmesini sağlayan özel amaçlı bir araştırma işlemi olarak tanımlayabiliriz.

Olay yeri incelemesinde amaç;

- Meydana gelen bir olayın adli bir suç olup olmadığını tespit etmek,
- Olayın öngörülen şekil ve şartlarda meydana gelip gelmediğini belirlemek,
- Olay yeri-fail-mağdur(veya maktul) arasındaki ilişkiyi kuracak maddi suç delillerini bulmak,
- İşlenen suçun aydınlatılması ve adli mercilerin doğru karar vermesini sağlamak amacıyla olay yerini belgelemek,
- Olay soruşturmasında ve çözümünde olay yeri-fail-mağdur ilişkisinin ortaya çıkarılmasıdır. (Bayer ve Kaygısız, 2002, s.:10)

Her araştırmanın bir amacı vardır. Bir araştırmayı neden yürütmemiz gerektiğini anlamak için olay yerinde bulunan delilleri toplamadan önce bir hareket planı yapmalı ve delilleri nerelerde aramamız gerektiğini bilmemiz gerekir.

Genel olarak tüm olay yeri inceleme prosedürleri, bilişim suçları vakalarında da uygulanabilir. Bunların yanında elektronik delillerin diğer delillerden farklı olarak sahip oldukları yapılarından dolayı bazı hususlara dikkat etmek gerekir.

Birleşik Devletler, Polis Meslek Grubu, Bilişim Suçlarını Araştırma Ekibi'ne göre bilişim suçlarında olay yeri incelemesi yürütülürken dikkat edilmesi gereken ana prensipler aşağıda belirtilmiştir:

1. Bilgisayar veya diğer ortamlar üzerinde verilerinin değiştirilmesi veya yok edilmesi nedeniyle mahkemeler tarafında kabul edilmeyecek deliller oluşmaması için polis bile olsa yetkisiz kişilerin olay yerine girmesine izin verilmemelidir.

2. Bazı özel durumlarda, orijinal delile erişmek gerekiyorsa, erişecek kişinin konu hakkında ehil ve elektronik delillere gösterilecek ilgi konusunda bilgi sahibi olması gerekir.

3. Üçüncü şahısların delil üzerinde inceleme yapabileceği düşünülerek, delile uygulanan işlemler daha önceden belirlenmiş denetleme prosedürlerine uygun olarak yapılmalı ve yapılan işlemler kayıt altına alınmalıdır.

4. Olay yerinden sorumlu olan uzman, tâbi olduğu kanunlar ve yönetmelikler hakkında bilgi sahibi olmalıdır. (Acpo, 1999, s.:6)

Günümüzde, olay yerlerinde bulunması muhtemel deliller: kıl, kan, tırnak gibi biyolojik; eroin, kokain, barut gibi kimyasal; parmak izi, ayakkabı izi, alet izi gibi fiziksel; kovan, kovan çekirdeği, tabanca gibi balistiksel; senet, para, broşür gibi belgesel olabilir. Son yıllarda bilişim teknolojisinin insan hayatının her alanında sıkça kullanılmasıyla beraber olay yerlerinde rastlanabilecek deliller arasına bilgisayarlar, disketler, optik diskler, manyetik kasetler, cep telefonları ve bellek kartları gibi bilişim ve iletişim cihazları da girmiştir.

Günümüzde ofis evraklarının çoğunluğu bilgisayar sabit diskleri, disketler, zip diskler ve optik diskler gibi depolama ortamlarında saklanmaktadır. Klasik evrak dolaplarının yerini bilgisayarların almasıyla beraber, olay yerlerinden elde edilen deliller içerisinde bilişim ile ilgili cihazların bulunma oranı artmıştır.

Adli ve Önleme Aramaları Yönetmeliği'nin 17. maddesinde; bilişim ile ilgili delillere el konulması ve sonrasında incelenmesi konusunda "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma" başlığı adı altında;

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

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

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

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

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

paragraflarıyla açıklanmıştır.

Bireye ait kişisel bilgiler üzerindeki hak, temel insan haklarından olduğundan hakkın kısıtlanabilmesi için yasal düzenleme gerekeceği açıktır. Ancak bilgisayarlardaki kayıtların gerçeğin açığa çıkarılması yönünden, ceza davasında delil, iz, eser ve emare oluşturacağı ortadadır. Bu itibarla maddeler hem bu olanağı sağlamak ve hem de bireysel yararları saklı tutmak amacıyla bilgisayar program ve kütüklerinde arama yapılmasını belirli koşullara tâbi kılmış bulunmaktadır.

01.06.2005 tarihinde yürürlüğe giren bu yönetmelik bilişim suçları alanında işlenen suçlara dair maddeler içermektedir. Bu maddelere göre bilişim delillerinin mahkemelerde maddi delil olarak kabul edilebileceği anlaşılabilir. Olay yerlerinden elde edilen elektronik delillerin şifrelerinin kırılabileceği ve kopyalarının alınabileceği ikinci fıkrada belirtilmektedir. El konulacak delil, sahibi olan kurum tarafından kritik bir öneme sahipse, delilin kopyasının, olay yerinde alınması gerekmektedir.

Kişisel bilgisayarların 1981'de ortaya çıkması ve hemen ardından popülaritesinin hızla artması bu cihazların modern hayatın her alanında kullanılmasına neden olmuştur. Günümüzde bilgisayarlar; mesaj yazmak ve yollamaktan finanssal sonuçları hesaplamaya, fon aktarmaktan hisse senedi almaya, uçak bileti rezerve etmekten banka hesaplarını kontrol etmeye kadar hemen her alanda kullanılmaktadır. İnternet, bilgisayarlar ile bu hizmetlere dünyanın her yerinden ulaşılmasını sağladığı için bu cihazlara olan rağbeti arttırmaktadır. Toplumun genelinin kolayca erişebildiği bir cihaz olduğundan suçlular da bilgisayarları kolaylıkla kullanmaktadırlar. Bu nedenle olay yerlerinde bilişim cihazlarına rastlamak normal karşılanmalıdır.

İnternet, bilgisayar ağları ve otomatik veri işlem sistemleri suç işlemek için yeni fırsatlara imkân vermektedir. Bilgisayarlar ve diğer elektronik sistemler, kişilere, kurumlara ve mala karşı işlenen suçlara yüksek oranda imkân vermekte veya desteklemektedir. Bu destek, suçun başka bilgisayarlara karşı işlenmesinden, terörizm, kara para aklama ve yasadışı madde ticareti gibi trajik boyutlara uzanmaktadır.

Elektronik ve bilgisayar teknolojilerinin hızla gelişen doğası, bu teknolojilerin kullanıldığı suç türlerinin de hızla değişmesine neden olmaktadır. Bu nedenle konu hakkındaki bilgiler sürekli güncellenmelidir.

### 1.2.2. Bilişim Suçu Delilleri

Bilişim suçlarında elde edilen deliller, elektronik ve dijital delil olarak ikiye ayrılmaktadır. Genel olarak ikiye ayrılmasının sebebi bir bilişim sistemini oluşturan kavramların donanım ve yazılım olarak ikiye ayrılmasından dolayıdır. Bilişim sistemleri kullanıcılara esneklik sağlaması açısından sabit elektronik devreler üzerinde çalışan, değiştirilebilen ve güncellenebilen yazılımlardan oluşmaktadır. Her insanın ihtiyacına yönelik elektronik devre tasarımı yapmak üreticiler açısından ekonomik değildir. Bunun yerine bilişim cihazı üreticileri standart donanım mimarileri üzerine kullanıcılar tarafından seçilebilecek yazılımlar üretmekte veya üretilmesine imkân vermektedirler. Kullanıcılar piyasada bulunan standart bilgisayar sistemleri üzerine istedikleri işletim sistemini kurmakta serbesttirler. Donanım üreticileri bu konuda destek

vermektedir. PC[25] sistemleri olarak tabir edilen esnek bilgisayar sistemlerinin ortaya çıkmasının altında yatan sebep budur.

Bilişim sistemleri, suç işlemek amacıyla kullanıldığında ortaya çıkan delilleri iki gruba ayırmak mümkündür: elektronik delil ve dijital delil. Dijital delil, bir hipotezi desteklemek veya çürütmek için güvenilir bilgiler içeren dijital[26] verilerdir. (Carrier, 2005, s.:12)

Elektronik delil, elektronik cihazlar üzerinde depolanan veya üzerinden transfer edilen, araştırmaya değer verilerdir. (Ashcroft, 2001, s.:6) Elektronik deliller, biyolojik DNA delilleri gibi latent (gizli) delillerdir. Elektronik delillerin üzerinde nicel incelemeler yapılmadan içeriğinin ne olduğu anlaşılamaz. Donanım sistemlerinin yapısı elektronik delillerin ihtiva ettiği ipuçlarının gözle görülür olmasına imkân vermez. Elektronik delillerin içerisinde bulunan bilgileri açığa çıkarabilmek amacıyla uygun cihaz ve yazılımlarla incelemeler yürütmek gerekmektedir.

"Dijital deliller, dünya için oldukça yeni bir kavramdır. Özellikle bilişim suçlarındaki yoğun artıştan sonra, bilimsel alanda da çok yoğun tartışmaların odak noktası olmuş olan dijital deliller hakkında, farklı tanımlamalar mevcuttur. Shinder'e göre "bir bilişim suçu ile ilgili, elektronik veya manyetik bir ortam üzerinden iletilen veya bu ortamlara kaydedilen bilgilere dijital delil" denilmektedir (Shinder, 2002). Chisum ise dijital delilleri "bir suçun nasıl olduğunu veya suçtaki kritik elemanları adresleyen teorileri destekleyen

[25] Personal Computer (Kişisel Bilgisayar). İzleyen paragraflarda daha detaylı açıklanacaktır.
[26] TDK tarafından dijital kelimesi: "Verilerin bir ekran üzerinde elektronik olarak gösterilmesi" olarak tanımlanmakta ancak teknik anlamda tanımı ise "Bilişim sistemlerinde girdi, işlem, geçiş, depolama ve çıktı işlemleri için kullanılan sayısal veridir.

veya çürüten, bilgisayar sistemleri kullanılarak kayıt edilen veya iletilen veriler" olarak tanımlamıştır (Chisum, 1999). Son olarak Casey'in tanımına bakarsak dijital deliller "bir suçun islendiğini gösteren veya suç ile kurban ya da suç ile faili arasında bir ilişki sağlayan veriler" olarak karsımıza çıkmaktadır (Casey, 2000)." (Uzunay, 2005, s.:43)

Birleşik Devletler, Adalet Bakanlığı, Ulusal Adalet Enstitüsü, dijital delillerin yapısal özelliklerini; (Ashcroft, 2001, s.:6)

- DNA ve parmak izi gibi latenttir.
- Kolaylıkla değiştirilebilir, bozulabilir veya yok edilebilir.
- Dünya çapında bir alana dağılmış olabilir.
- Zamana bağlı olabilir.

olarak tanımlamıştır.

Delillerin latent yapıda olması, onların incelenmesinin uygun cihazlar ve ölçüm aletleri yardımıyla yapılmasını gerektirir. Çünkü muhteva ettiği bilgiler yalnızca insanın duyu organları ile algılanamaz. Olay yerinde bulunan bir bıçağın, gerçekten bir bıçak olup olmadığını anlamak amacıyla nitel gözlem yapmak yeterlidir. Ancak yasa kapsamına girip girmediğini anlamak için bıçağın boyu ölçülmelidir. Yani nicel gözlem yapılmalıdır. Elektronik delillerin içerisindeki dijital verileri anlayabilmek için ise mutlaka alet ve cihazlar ile nicel gözlemler yapılmalıdır. Çünkü genellikle makine dili[27] ile kodlanmış olan bilgiler yine bir makine tarafından yorumlanmalıdır.

[27] Makine dili, bilgisayar sisteminin işlemcisi tarafından yorumlanabilen komutlardır. http://en.wikipedia.org/wiki/Machine_language, Erişim Tarihi: 07.06.2006

Elektronik deliller içerisinde bulunan veriler dijital formatta kaydedilirler. Verilerin dijital formatta kaydedilebilmeleri için elektrik enerjisine ihtiyaç vardır. Elektrik enerjisinin kesilmesi nedeniyle verilerin kaybolmaması için sabit disk gibi dijital depolama medyalarında manyetik saklama teknolojisi kullanılır. Ancak manyetik saklama teknolojinin kullanılması, verilerin silinmesini engellememektedir. Elektronik yöntemlerle yazılan veriler yine elektronik yöntemlerle silinebilir. Bu nedenle elektronik deliller içerisinde bulunan dijital veriler, elektrik enerjisine maruz kaldıkları zamanlarda silinme ihtimaliyle karşı karşıyalardır. Uzmanlar tarafından, uygun aletlerle yapılmayan müdahalelerde elektronik delillerin silinmesi veya değiştirilmesi kaçınılmazdır. Elektronik deliller, hassas yapılarından dolayı mutlaka uzmanlar tarafından incelenmelidir.

Bilişim dünyasının, iletişim dünyası ile insan hayatını kolaylaştırmak noktasında ortak girişimleri, İnternet adlı dünyanın en büyük bilgisayar ağını meydana getirmiştir. İnternet'e bağlı bilgisayarların tümü masum insanlar tarafından kullanılmamaktadır. Suç işlemeye meyilli insanlar bilgisayar ile İnternet aracılığıyla dünyanın diğer ucundaki bilgisayar sistemlerini zarara uğratabilmektedirler. Bu tür sınır aşan suçlarda incelenmesi gereken bilgisayarlar dünyanın diğer ucunda olabilir ve hatta şüphelenilen bilgisayar aslında güvenlik güçlerini yanıltmak için kullanılan masum birinin bilgisayarı olabilir. Böyle durumda olay yeri, İnternet, yani tüm dünya coğrafyasına yayılmış olabilir.

"IP[28] izleme, İnternet suçlarının aydınlatılması konusunda fazla deneyimi olmayan güvenlik birimlerinin hiç ilgisiz kişilerden şüphelenmesine, bunları mağdur etmesine, soruşturmaların çok uzamasına yol açıyor. Ülkelerüstü bir kaçakçılık örgütüne dönüşen ve belki de internet üzerinden uyuşturucu madde pazarlayanlarla işbirliği içinde, hatta belki de aynı kişilerin denetimindeki yasadışı e-eczaneler, bir yandan sağlığa, diğer yandan ekonomiye zarar veriyor." (Atasoy, 2006)

Bilgisayar programları, bilgisayar programcıları tarafından belli görevleri otomatikleştirmek amacıyla yazılırlar. Yazılım endüstrisinin gelişmesiyle beraber, bilgisayar yazılımları da çok çeşitli alanlarda kullanılmaktadır. Bilgisayar devriminin başlangıcında birkaç adet olan bilgisayar yazılımının sayısı, günümüzde sayılamayacak düzeye gelmiştir. İnternet üzerinden serbestçe dağıtılabilen ve indirilebilen yazılımlardaki güvenlik açıkları bilgisayarları sürekli tehdit altında bırakmaktadır. İyi niyetli olarak kullanılan bir yazılımın, kullanıcılar tarafından, bilgisayarın arka alanında yaptıkları bilinmemektedir. Müzik dinlemek amacıyla İnternet'ten indirilen bir yazılım, görevini icra ederken, geri planda dünyanın diğer ucundaki başka bir bilgisayara saldırıyor olabilir. Böyle durumlarla karşılaşmamak için her bilgisayarda mutlaka bir zararlı yazılım tespit ve temizleme yazılımı kullanılmalıdır. Bilgisayarlar üzerinde çalışan yazılımlar güvenilir bir kaynaktan edinilmemiş ise o yazılımın arka alanda ne tür işlemler yürüttüğünü anlamak kolay değildir. Olay yerlerinde karşılaşılan, çalışır vaziyette ve üzerinde herhangi bir programın çalıştığı görülen bilgisayarlar için de aynı durum söz konusudur. Bilgisayar monitöründe herhangi bir işlem yapıyor gibi gözüken bir program aslında o anda bilgisayarın sabit diski üzerinde saklanan, suç ile ilgili verileri siliyor olabilir. Bu, bize elektronik delillerin zamana bağlı

[28] IP (Internet Protocol) Bilgisayarların, İnternet üzerinden haberleşmelerine imkân veren her bilgisayara ayrı ayrı (unique) atanmış sayısal adres değeri.

olduğu durumunu gösterir. Böyle durumlarda hemen delile müdahale edilmezse delilin değiştirilmesi veya kaybolması tehlikesiyle karşı karşıya kalınabilir.

Günümüz ceza yargılamasında, hukuk yargılamasından farklı olarak "vicdani delil sistemi" kabul edilmiştir. Hâkim, her olaya göre vicdanen tamamen serbest bir şekilde deliller araştırıp ispat yoluna gitmektedir. (Bayram, 2005, s.:52) Ancak elektronik delillerin davada etkinlik sağlayabilmesi için, mahkeme önüne getirilmeden önce diğer maddi delillerin sahip olması gereken özelliklere de sahip olması gerekir. Bu özellikler:

- “Kabul olunabilir: Yasal yollardan elde edilmiş olmalıdır.
- Gerçeklik: İddiamızı doğrulayan gerçeklikte olmalıdır.
- Tamlık: Tek bir bakış açısından değil tüm açılardan bakıldığında aynı sonucu göstermelidir.
- Güvenilirlik: Delilin elde edilmesi konusunda herhangi bir kuşkuya yer vermemelidir.
- İnanılırlık: Mahkeme tarafından kolaylıkla inanılabilir ve anlaşılabilir olmalıdır.” (Anderson ve Mohay, 2003, s.:35)

Elektronik delillerin keşfinde, olay yeri inceleme uzmanları, savcılar, adli bilişim uzmanları ve yöneticiler ayrı ayrı rol sahibidirler. Olay yeri inceleme uzmanları delillerin tanımlaması, toplanması, paketlenmesi ve taşınmasından sorumludurlar. Savcılar delillerin data inceleme laboratuvarlarına gönderilmesi ve delil üzerinde ne tür araştırmalar yapılacağının belirlenmesi konusunda görevlidirler. Adli bilişim uzmanları delillerin incelenmesi, bulunan veriler konusunda rapor yazmak ve delilleri muhafaza etmekle

yükümlüdürler. Yöneticiler ise yönetimlerindeki kişileri koordine etmek, eğitimlerini sağlamak ve delillerin karartılmaması için gerekli olan motivasyonu sağlamakla görevlidirler. Farklı birimlerin koordinasyonunu gerektiren delil incelemelerinde, delil güvenlik zinciri (chain of custody) sağlanmalıdır. Delil güvenlik zinciri, delilin her el değiştirildiğinde yapılan işlemlerin kayıt altına alınması ve bunun bir form ile belgelenmesidir. (Brown, 2001, s.:5)

Delillerin karartılmaması konusunun önemi tüm kademe personeli tarafından kesinlikle anlaşılmalıdır. Tüm adli süreç personeli, elektronik delillerin kolaylıkla değiştirilebilir olduğunu anlamalı ve delillerin toplanması ve incelenmesi süreci boyunca alınan prensip ve prosedürlere uymalıdır. Delillerin karartılmasına neden olabilecek yanlış uygulamalar mahkemeler tarafından delillerin reddedilmesine yol açacaktır.

Elektronik delillerle uğraşırken diğer adli delillere uygulanan prensipler unutulmamalıdır. (Ashcroft, 2001, s.:25)

- Delile uygulanan hareketler, delilin bütünlüğünü bozmamalıdır.
- Delillerle uğraşan kişiler konularında uzman kişiler olmalıdırlar.
- Tüm adli süreç ilgili kişi tarafından kaydedilmelidir.

Elektronik deliller, yapılarından dolayı, yanlış taşıma veya yanlış inceleme sonucunda kolaylıkla değiştirilebilir, bozulabilir ya da yok edilebilir. Bu nedenle, elektronik delilleri toplamak, taşımak, muhafaza etmek ve incelemek

için özel önlemler alınmalıdır. Aksi takdirde elektronik delil kullanılamaz veya sonuca götüremez duruma gelebilir.

Elektronik deliller yapıları nedeniyle mahkemeler tarafından delil olarak kabul edilmeleri konusunda çeşitli tartışmalara neden olmaktadır. Bu tartışmaları engellemek için özel adli prosedürler takip edilmelidir.

### 1.2.3. Olay Yeri İncelemesinin Uygulama Yöntemi

Olay yeri incelemesi aslında bir arama işlemidir. Arama işlemi eş zamanlı bir safha olduğu için muhtemel delillerin kaybolmasına en fazla neden olunan safhadır. Bu nedenle, arama safhası en fazla öneme sahip olan süreç olarak değerlendirilebilir. Bu nedenle olay yeri incelemesi sırasında özel önlemler alınmalıdır.

Olay yeri inceleme süreci muhtemel delillerin bulunması ve orijinal kaynağın tespit edilmesine yardım eder. Bu süreçte dikkat edilmesi gerekli bazı noktalar vardır. İlk olarak olay yerinde rastlanan delillerin bütünlüğü bozulmadan ve delillerin bulunduğu durumda uygun yöntemlerle kaydedilmeleri gerekmektedir. Çünkü yapılan kayıtlar delil muhteviyatının bulunması konusunda laboratuar incelemeleri yapılırken adli bilişim uzmanlarına yardımcı olur. Olay yerinin uygun yöntemlerle kayıt altına alınması, olay yerindeki gizli bilgileri, ileride yapılacak inceleme safhasında ortaya çıkarır. Olay yerinde bulunan delillerin kaydedilmesi, video kamera veya fotoğraf makinesi ile yapılabilir. Bunların olmaması durumunda mutlaka olay yerinin

krokisi çizilmeli ve bulunan delillerin olay yerinin neresinde bulunduğu gösterilmelidir. Arama kayıtları ileriki aşamalarda tanıklık sağlayacağı için saklanmalıdır. Bir olay yeri inceleme uzmanı, prosedürlere uyarak arama sürecini yürütmenin kendi bilgi ve yeteneklerine bağlı olduğunu da bilmelidir. Kayıt işlemi bittikten sonra sıra karşılaşılan bulguların seçilerek delil haline getirilmesine gelir.

Arama süreci ürünlerinin değerlendirilmesi analiz sürecinde olur. Bu süreçte olay yeri inceleme uzmanının teknik bilgisi önem arz eder. Çünkü muhtemel delillerin olay yerinde kalacağı veya laboratuvara taşınacağı bu safhada kesinlik kazanır.

“Kriminal araştırmalar yürütülürken birçok bilişim sistemi ile karşılaşılabilir. Bunlar delil toplama prosedürlerine uygun olarak toplanırsa araştırmanın gidişatını değiştirebilir.” (Ashcroft, 2001, s.:9)

Olay yeri aramaları neticesinde rastlanılan bilgisayarların büyük çoğunluğu IBM PC ailesindendir. Genellikle bu tür bilgisayarlar, bir ekran, bir klavye ve bir kasadan oluşur. Bilgisayarlar dışındaki bilişim veya iletişim cihazları çok geniş bir yelpazeye dağılabilir. Böyle sistemler kapasitelerinden dolayı, araştırmacılara diğer delillerde bulunamayacak kadar fazla bilgi sunar.

Olay yerlerinde rastlanabilecek muhtemel bilişim delilleri:

- bilgisayar kasası,
- ekran,
- klavye ve fare,
- tüm kablolar,
- güç üniteleri,
- harici sabit diskler,
- güvenlik kartları,
- modemler,
- diğer harici sürücüler ve cihazlar,
- disketler,
- yedekleme kasetleri,
- zip kasetleri,
- optik diskler,
- PCMCIA kartları,
- elektronik devreler,
- anahtarlar,
- şifrelerin yazılı olduğu kağıtlar,
- donanım ve yazılım kitapçıkları

olarak sayılabilir.

Olay yerinde rastlanılması durumunda delillere uygulanacak prosedürler, bulunan sistemden sisteme göre değişir. Genellikle bilişim sistemi deyince akla ilk gelen cihaz olan bilgisayarlara uygulanması gereken el koyma, toplama ve paketleme prosedürleri aşağıdaki gibi sıralanabilir. (Acpo, 1999, s.:10) Diğer bilişim cihazları için de benzer prosedürler uygulanabilir.

A) Olay yerinde rastlanılan bilgisayarın kapalı
olması durumunda;

1. Delilin bulunduğu alanı güvenlik ve kontrol altına alın.
2. Diğer insanları bilgisayardan ve güç ünitesinden uzaklaştırın.
3. Hiçbir koşul altında bilgisayarı açmayın.
4. Bilgisayarın tam olarak kapalı olduğundan emin olun. Bazı ekran koruyucular bilgisayarın kapalıymış gibi gözükmesine neden olabilir. Bunu anlamak için Kasa üzerideki sabit disk aktivite ışığını kontrol edin. Aktivite varsa bilgisayar çalışıyordur.
5. Dizüstü bilgisayarların kapağı açıldığı zaman çalışmaya başlayabileceği için kapağını açmayın.
6. Güç kablosunu öncelikle bilgisayar kasasından, daha sonra duvardaki prizden sökün.
7. Kasaya bağlı olan iletişim hatlarını ve diğer kabloları uygun şekilde çıkarın.
8. İmkânlar el veriyorsa olay yerini kameraya alın, fotoğraflarını çekin veya krokisini çizin.
9. Bilgisayara bağlı olup da sökülen kablolar etiketlenmelidir.
10. Parçaları taşımak için uygun kutular ve delil torbaları (anti statik) kullanınız ve hareket sırasında dikkatli olunuz.
11. Bilgisayarın toplandığı alanın etrafında bulunan kâğıtları, not defterleri ve günlükleri şifrelerin bulunabileceğini düşünerek inceleyiniz.
12. Bilgisayar sahibine bilgisayarın herhangi bir yerinde şifre olup olmadığını varsa ne olduğunu sorunuz ve not alınız.
13. Delillerin toplanması aşamalarını basamak basamak yazınız.

B) Olay yerinde rastlanılan bilgisayarın açık
olması durumunda;

1. Delilin bulunduğu alanı güvenlik ve kontrol altına alın.
2. Diğer insanları bilgisayardan ve güç ünitesinden uzaklaştırın.
3. Modem'in kablosu bağlı ise sökünüz.
4. Bilgisayarın kablosuz bir ağa bağlı olduğunu düşünüyorsanız bir uzmandan yardım alınız.
5. Bilgisayar sahibinden yardım almayınız ve yardım teklifini kabul etmeyiniz.
6. Klavyeye dokunmayınız ve fare ile tıklamayınız.
7. Ekran kapalıysa farenin tuşlarına tıklamadan hareket ettirin. Eğer ekran görüntüsü gelir ve şifre sorarsa sonraki adıma geçin. Şifre sorulmaz ise ekranın görüntüsünü fotoğraflayın. Hiçbir programı kapatmayın veya açmayın.
8. Kasanın arkasında bulunan güç kablosunu yavaşça çıkarın. Daha sonra duvardan sökün. Bu adım eğer bilgisayara bağlı bir UPS (kesintisiz güç kaynağı) var ise sabit diske veri yazılmasını engellemek içindir.
9. Kasaya bağlı olan iletişim hatlarını ve diğer kabloları uygun şekilde çıkarın.
10. İmkânlar el veriyorsa olay yerini kameraya alın, fotoğrafını çekin veya krokisini çizin.
11. Bilgisayara bağlı olup da sökülen kablolar etiketlenmelidir.
12. Parçaları taşımak için uygun kutular ve delil torbaları (anti statik) kullanınız ve hareket sırasında dikkatli olunuz.

13. Bilgisayarın toplandığı alanın etrafında bulunan kâğıtları, not defterleri ve günlükleri şifrelerin bulunabileceğini düşünerek inceleyiniz.
14. Bilgisayar sahibine bilgisayarın herhangi bir yerinde şifre olup olmadığını varsa ne olduğunu sorunuz ve not alınız.
15. Delillerin toplanması aşamalarını basamak basamak yazınız.

“Bilişim suçu vakalarında, olay yeri incelemesi yapıldıktan sonraki aşama el koyulan delillerin data inceleme laboratuarına sevk edilmesidir. Elde edilen delillerin laboratuara taşınırken her hangi bir zarara uğramamaları için azami gayret gösterilmeli ve her delil için ayrı ayrı aşağıdaki tedbirler alınmalıdır.” (Acpo, 1999, s.:17)

Bilgisayar Kasası

- Dikkatli taşınmalıdır.
- Karayolu ile taşınacaksa dik tutulmalı ve sarsıntılara maruz kalmamalıdır.
- Manyetik alanlardan (hoparlör, telsiz, ısı) uzak tutulmalıdır.

Ekran

- Cam kısmı yumuşak bir yere konarak taşınmalıdır.

Sabit Disk

- Manyetik alanlardan uzak tutulmalıdır.

- Anti statik torba, sert kâğıt kesekâğıdı veya hava alan plastik torbalarda taşınması gerekir.

Disket ve Kaset

- Manyetik alanlardan uzak tutulmalıdır.
- Katlamayınız veya bükmeyiniz.
- Disketlerin üzerine etiket yapıştırmayınız.

El Bilgisayarı

- Manyetik alanlardan uzak tutulmalıdır.
- Anti statik torbalarda taşıyınız.

Klavye, Fare ve Kablolar

- Delikli plastik torbalarda taşınabilir.
- Ağır nesnelerin altına koymayınız.

Parmak izi alınacak delillerin korunması

- Elektronik deliller üzerinde yüksek voltaj oluşturduğu ve delillerin zarar görmesine neden olacağından, parmak izi almak için alüminyum tozu kullanılmamalıdır.
- Normal oda şartlarında saklanmalıdır.
- Sıcak, soğuk, nemli veya rutubetli ortamlarda bırakılmamalıdır.

Piller

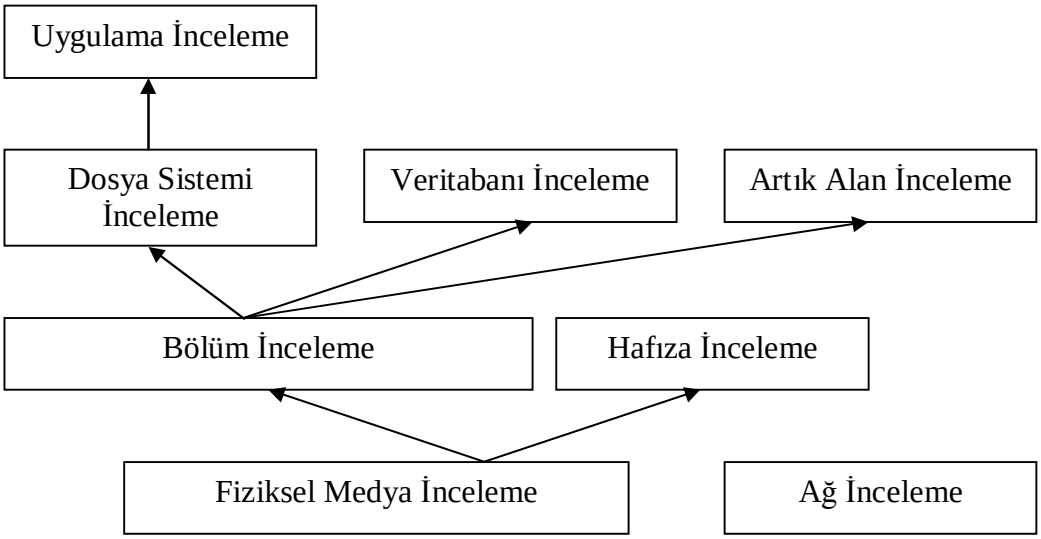
- Birçok bilgisayar, sistem ayarlarını saklamak için dahili piller kullanırlar. Piller kısa devre edilir veya biterse bu ayarlar yok olacaktır. Pillerin ömürlerinin ne kadar olduğunu anlamak tam olarak mümkün değildir. Modern bilgisayarların pillerinin raf ömürleri ortalama 24 aydır. Bu nedenle modern bilgisayarlardan daha ziyade eski model bilgisayarlara bu konuda dikkat etmek gerekir. Bazı adli kopyalama yazılımları CMOS (Complementary Metal Oxide Semiconductor) ve ROM (Read Only Memory) bilgilerini kopyalayabilmektedir. Eğer bu bilgiler adli bilişim uzmanı tarafından kopyalanırsa bu konuda endişelenmeye gerek kalmaz. Dizüstü bilgisayarlara özel önem verilmelidir. Çünkü bu tür bilgisayarların hem ana pil ünitesi hem de CMOS pil ünitesi vardır.

## 1.3. Bilişim Suçlarında Laboratuvar İncelemeleri

### 1.3.1. Dijital Sistemler

Bilişim sistemleri genellikle katmanlı yapı mimarisinde üretilirler. (Carrier, 2005, s.:18) Yani basit teknolojiler üzerine kurulmuş, giderek artan daha yüksek teknolojiler inşa edilir. Adli bilişimin inceleme alanına giren 2 farklı tür sistemden bahsetmek mümkündür: depolama sistemi ve ağ sistemi. (Carrier, 2005, s.:18) Ağ sistemleri birden fazla bilgisayarın birbirine bağlanmasıyla ortaya çıkan iletişim yapılarıdır. Ağ sistemlerinin birbirine bağlanılması ile İnternet meydana gelir. Ağ sistemleri üzerinden işlenen suçları araştırmak tek bir bilgisayar kullanılarak işlenen suçları araştırmaktan

farklıdır ve daha karmaşıktır. İncelenmesi gereken daha fazla faktör ve farklı yer vardır. Bu araştırmada depolama sistemleri üzerinde adli bilişim incelemeleri yapılması konusu üzerinde çalışılacaktır.



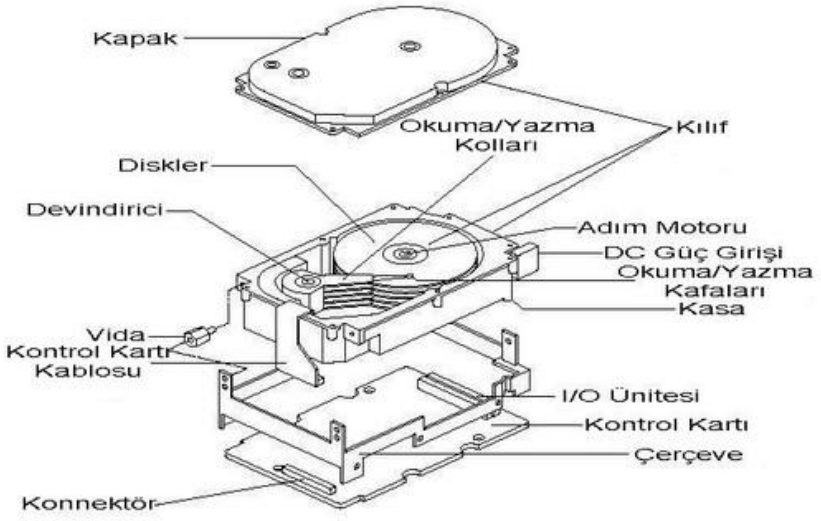

Şekil-1.3: Adli Bilişimde Fiziksel Medya İncelemesi

Yukarıdaki şekil, bir sabit diskin incelenebilecek farklı alanlarını göstermektedir. Fiziksel depolama medyaları "elektronik delil" olarak adlandırdığımız delil türleridir. Yani elle tutulup gözle görülebilen maddi delil çeşididir. Bu tür delillere örnek olarak sabit diskler, bellekler ve optik diskleri sayabiliriz.

Modern bilgisayar sistemlerinin hepsi en az bir adet sabit diske sahiptir. (HTCI, 2004, s.:313) Çünkü işletim sisteminin[29] ve kullanıcı dosyalarının

[29] Bilgisayar sistemini oluşturan donanım ve yazılım birimlerinin birbirleriyle iletişim kurmasını sağlayan yazılımdır. İşletim sisteminin temel görevleri: çevresel donanımları kontrol etmek, hafıza kontrolünü sağlamak, işlemleri önem sırasına koymak, giriş ve çıkış cihazlarını kontrol etmek, ağ

yükleneceği kalıcı bir depolama birimine ihtiyaç vardır. Sabit disk dijital verileri kalıcı olarak manyetik ortamda saklayan elektronik bilgi saklama birimidir. Bir sabit diskin önemli parçaları: kontrol kartı, plakalar (diskler), okuma/yazma kolları, okuma/yazma kafaları, adım motoru ve devindiricidir. Kontrol kartı, sabit diskin üst tarafında yer alan elektronik devredir. Bilgisayarın işletim sistemi, sabit diske okuma/yazma komutları gönderirken arabirim olarak kontrol kartını kullanır. Plakalar, silindir şeklinde alüminyum tabakaların genellikle ferrit manyetik madde ile kaplanmasıyla oluşmuş disklerdir. Sabit diskin dijital veri depolamasını sağlayan asıl bileşen plakalardır. Okuma/yazma kolları, devindiricideki hareketi okuma/yazma kafalarına ileten metal parçalardır. Okuma/yazma kafaları, plakalar üzerinden veri okurlar ve yazarlar. Her plaka için iki adet (alt ve üst) okuma/yazma kafası bulunur. Adım motoru plakaların hareketinden sorumludur. Modern sabit disklerde genelde dakikada 3600–7200 devir dönüş sağlar. Devindirici ise okuma/yazma kollarını plakalar üzerinde ileri-geri hareket ettirmek amacıyla kullanılır.




Şekil-1.4: Bir sabit diskin iç yapısı [30]

iletişimini kontrol etmek ve dosyaları organize etmektir. Bazı işletim sistemleri: Windows, Linux ve Solaris.

[30] Copyright Seagate Technology

“Bilişim sistemleri 1 ve 0 rakamlarından meydana gelen ikilik (binary) sayı sistemi ile çalışırlar. En alt seviyede, elektrik akımının olması, 1 durumunu, olmaması ise 0 durumunu ifade eder. Fiziksel depolama medyaları geçici ve kalıcı depolama medyaları olarak ikiye ayrılır.”

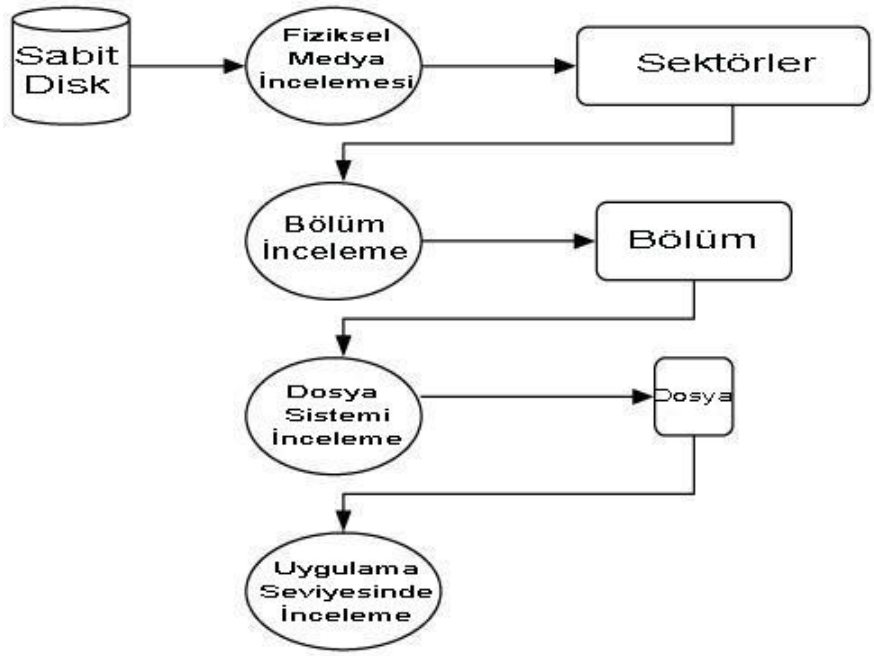
Bellekler (RAM) geçici depolama medyalarıdır ve elektrik akımının kesilmesi halinde üzerlerindeki bilgiler yok olur. RAM’in üretim amacı zaten bilgileri kalıcı olarak saklamak değildir. Bilgisayar sisteminin performansını arttırmak için işlemci tarafından veriler sabit diskten RAM’e aktarılır.[31] Kalıcı bilgi saklama özelliğine sahip oldukları için, adli bilişimin ilgilendiği medya türleri genellikle sabit disk, optik disk ve disket gibi kalıcı depolama birimleridir.

“Sabit diskler, daha kullanışlı olmaları için ve sistem çökmelerinde, sistemi kısa sürede çalışır duruma getirmek amacıyla birden fazla bölüme ayrılırlar. Bölümler, kullanıcının verilerini yazabileceği yerlerdir. NTFS (Windows), EXT3 (Linux), HFS (Mac OS) sık kullanılan bölüm formatlarıdır. Adli bilişimde sabit disk bölümlerini incelemeye geçmeden önce, bölümlerin formatını tespit etmek gerekir. Silinmiş veya gizlenmiş bilgileri bulabilmek için bölüm formatı tam olarak tespit edilmeli ve incelemeler bu formatın özelliklerine göre yürütülmelidir.” (Carrier, 2005, s.:41)

“Sabit diskin üzerinde kayıtlı bulunan bir dosyayı incelemek için, uygulama seviyesine geçmeliyiz. Her dosyanın yapısı, bölüm formatını belirleyen işletim sistemi tarafından oluşturulur. Mesela dosya sistemi perspektifinden bakıldığı zaman, bir Windows kayıt girdisi ile bir HTML sayfası arasında fark yoktur.

[31] http://en.wikipedia.org/wiki/Random_access_memory, Erişim Tarihi: 11.03.2006

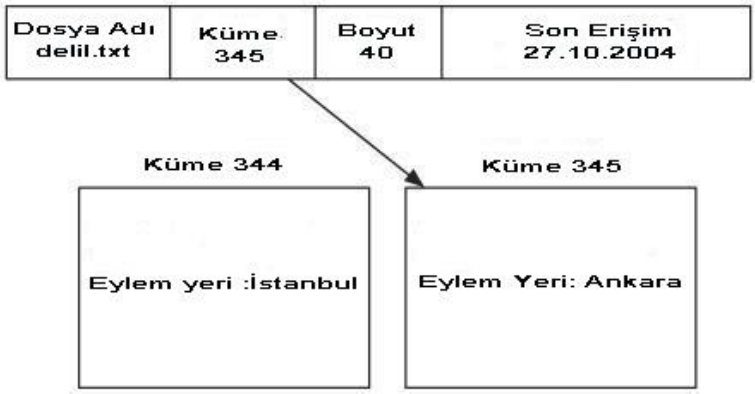
Çünkü ikisi de 1 ve 0'lardan oluşan birer dosyadır." (Casey, 2002, s.:133) Daha yakından bakıldığında ise farklı yapıya sahip oldukları görülür.




Şekil-1.5: Veri Analiz Süreci

Şekil-3.3'de veri analiz süreci görülmektedir. Şekilde elektronik bir delilin, fiziksel yapısından başlanarak uygulama seviyesine kadar olan inceleme aşamaları gösterilmektedir. Daha önce bahsedilen katman kavramına göre depolama birimlerinde bulunan mantıksal yapıların bir sistemi vardır. Dosya sisteminin görevi boş olan bölümü organize ederek, dosyaları yönetmemize imkân vermektir. (Carrier, 2005, s.:12) Dosya adı ise söz konusu dosyaya ait uygun içeriğe karşılık gelir. Yani dosya sisteminin görevi, dosya ismini doğrulamaktır. Bilinen dosya yöneticileri ile yapılan çalışmalarda bir dosyaya erişebilmek için; o dosyanın adını, başlangıç adresini ve uzunluğunu bilmemiz gerekir. (Carrier, 2005, s.:13) Adli bilişim yazılımlarında ise dosyaya erişebilmek için dosyanın, dosya sistemi üzerinde olması yeterlidir. Mesela dosya adı veya erişim tarihi yanlış veya yok ise dosya içeriği okunabilir.

Örneğin şekil-3.4'de açıklandığı gibi adli bilişim yazılımlarında, dosya adının ve son erişim tarihinin, dosyanın bulunması açısından önemi yoktur.




Şekil-1.6: Bir dosyanın disk üzerinde yerleşimi

Bilişim sistemleri üzerinde bulunan dijital veriler kolaylıkla değiştirilebilir. (Stephenson, 2000, s.:97) Çünkü bu sistemler yapıları gereği elektrik enerjisiyle çalışırlar ve enerjinin kesilmesiyle beraber bilgi kaybına uğrayabilirler. Bu nedenle dijital deliller üzerinde çalışırken bu durumu göz önünde bulundurmak gerekir. Mesela bir dosyanın, dosya sistemi üzerinde başladığı adres doğru olmak zorundadır. Çünkü aksi durumda sistemi kullanan kişi dosyaya erişemezdi. Fakat dosyanın son erişim zamanının doğru olması gerekmez. İşletim sistemi, dosya değiştirildikten sonra dosyanın tarihini güncellememiş olabilir veya bilgisayar uzun süre açılmadığı zaman içerisindeki pil biteceğinden tarihler silinmiş olabilir. Bunun yanında bir dosyanın başlangıç adresine güvenmek demek o dosyanın içeriğine güvenmek demek değildir. Örneğin silinmiş bir dosyanın adres değeri doğru, fakat dosya içeriği farklı ise dosya diğer bir adreste olabilir. Çünkü eski adresine yeni bir dosya yazılmıştır. Dijital veriler çoğu zaman doğrudur. Ancak bu hipotezi doğrulamak için başka verilere de ihtiyacımız vardır.

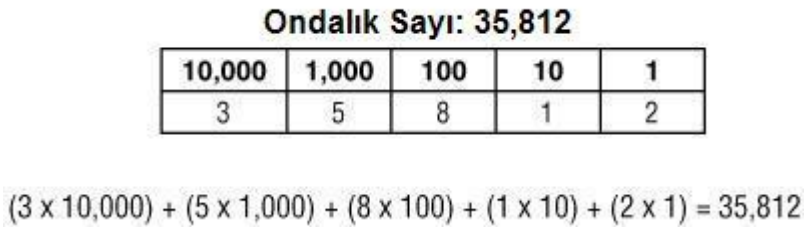
Bilişim sistemlerinin görevi dijital verileri işlemektir. (Stephenson, 2000, s.:103) Dijital verilerin olduğu her yerde ikilik sayı sistemi kullanılır. İkili sayı (binary) sistemi bilişim sistemlerinin çalışması için gerekli altyapıyı sağlar. Daha önce bahsedilen katmanlı yapı sayesinde daha karmaşık sistemler bu temel üzerine inşa edilmişlerdir. İkili sayı sistemiyle işlem yapmak insanlar açısından zor olduğu için onun yerine onaltılık (hexadecimal) sayı sistemi kullanılır.

### 1.3.2. Sayı Sistemleri

Günlük yaşamımızda onluk sayı sistemini kullanırız. Bu sistemi kullanmamızın sebebi, aritmetik işlemleri daha kolay yapabilmemizdir. Bilgisayarlar ise ikilik sayı sistemini kullanırlar. Bu sistem sadece 0 ve 1 rakamlarından oluşur ve her basamak “bit” olarak adlandırılır. 8 bit’in bir araya gelmesiyle bilişim sistemleri için anlamlı parçacıklar olan, tek karakter ifade eden “Byte” (Bayt) meydana gelir.

Onluk sayı sisteminde her basamağın bir değeri vardır. Sayıların en sağındaki basamak "en değersiz basamak" olarak adlandırılır. En soldaki basamak ise "en değerli basamak"tır. En değersiz basamağın değerini, kendisini 1 ile çarparak bulabiliriz. İkinci basamağın değerini ise kendisini 10 ile çarparak bulabiliriz. Üçüncü basamak 100 ile, dördüncü basamak 1000 ile çarpılmak suretiyle 10'nun katları olarak devam eder. Sayının değerini bulmak için ise tüm çarpımlar toplanır.

İkilik sistemde ise en değersiz basamağın değerini yine kendisini 1 ile çarparak bulabiliriz. İkinci basamağın değeri kendisinin ile 2'nin çarpımıdır. Üçüncü basamağın değeri kendisini 4 ile, dördüncü basamağın değeri kendisini 8 ile çarparak bulunur. Çarpımların toplamı bize ikilik sayının ondalık sistemdeki karşılığını verir.



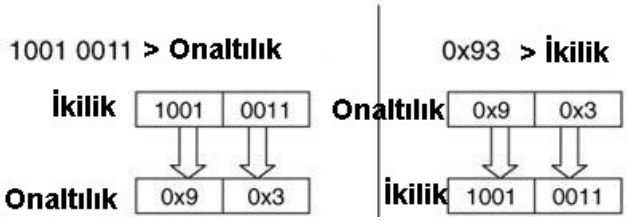

Şekil-1.7: Bir sayının basamaklarına ayrılması

Bilişim sistemlerinde kullanılan ikilik sistemin yanında bir de onaltılık (hexadecimal) sayı sistemi vardır. Bu sistemin kullanılmasının nedeni ikilik sistemle işlem yapmanın zor olması ve gerektiğinde onaltılık sistemi, ikilik sisteme çevirmenin kolay olmasındandır. Onaltılık sayı sistemindeki sayılar genellikle önlerine "0x" takısını konularak yazılırlar. Örneğin 0x5A9C gibi. Onaltılık sayı sistemi adından da anlaşılacağı üzere 16 rakamdan oluşur: 0–9 arası rakamlar ve A, B, C, D, E, F harfleri. Bu rakamların ikilik, onluk ve onaltılık sistemdeki karşılıkları tablo 2.1'de gösterilmiştir.

| İkilik | Onluk | Onaltılık |
|---|---|---|
| 0000 | 00 | 0 |
| 0001 | 01 | 1 |
| 0010 | 02 | 2 |
| 0011 | 03 | 3 |
| 0100 | 04 | 4 |
| 0101 | 05 | 5 |
| 0110 | 06 | 6 |
| 0111 | 07 | 7 |
| 1000 | 08 | 8 |
| 1001 | 09 | 9 |
| 1010 | 10 | A |
| 1011 | 11 | B |
| 1100 | 12 | C |
| 1101 | 13 | D |
| 1110 | 14 | E |
| 1111 | 15 | F |

Şekil-1.8: 0-15 sayılarının ikilik, onluk ve onaltılık sayı sistemlerinde karşılıkları

Onaltılık sayı sistemden ikilik sayı sistemine dönüşüm yapmak çok kolaydır. Yapılması gereken sadece onaltılık sayının her basamağını dört basamaklık ikilik sistem sayıları halinde yazmaktır. Bunun bir örneği şekil 3.6'da görülmektedir.




Şekil-1.9: Onaltılık sayı sistemindeki bir sayının ikilik sayı sistemindeki karşılığının bulunması

### 1.3.3. Adli Bilişim Ekspertiz Raporu Yazmak

Adli bilimcilerin önemli görevlerinden biri de uyguladıkları adli süreçleri ilgili kişilere aktarmaktır. İşlerini başarıyla tamamlamak için, teknik olarak doğru ve anlaşılması kolay rapor yazmalıdırlar. Eğer adli rapor yetersiz ise mükemmel giden bir soruşturma hezeyana sürüklenebilir. Ayrıca iyi düzenlenmemiş ve doğru yazılmamış bir rapor olayın aydınlanmasını engelleyebilir. Buna rağmen rapor yazmak, çoğu asistan ve uzman tarafından zor olarak değerlendirilir.

**Rapor Hazırlamak**

Adli bilgiler, eğer düzgün raporlanmaz ve sunulmaz ise değerleri sınırlandırılmış olur. (Maher, 2004) Genellikle bütün raporlarda basitçe; delilin neden incelendiği, nasıl incelendiği ve sonuç bilgileri bulunur. Adli bilişim ekspertiz raporu yazmak, delile uygulanan süreçlerin kaydedilmesini ve daha önceden belirlenmiş olan standartlara uyulmasını gerektirir. Ekspertiz raporu aşağıdaki bilgileri de kapsamalıdır. (Maher, 2004)

- Olayın detaylarını doğru olarak tanımlamalıdır.
- Yargı organlarının anlayacağı basitlikte olmalıdır.
- Yasal inceleme prosedürlerine uygun nitelikte olmalıdır.
- Cümleler tek anlamlı olmalı, yanlış anlaşılmaya meydan vermemelidir.
- Cümlelere kolayca referans gösterilebilmelidir. Gerekli yerlerde madde işaretleri ve numaralandırma kullanılmalıdır.

- Rapor, sonucunu tam olarak kapsayan bilgiyi içermelidir.
- Gerektiğinde uygun fikirler ve tavsiyeler belirtilmelidir.
- Tüm raporu özetleyen bir sonuçla bitirilmelidir.

Ekspertiz raporu yazılırken beş ana safhaya ayrılan genel bir metodoloji izlenir. Bu safhalar rapora özel detaylar eklemektedir. Rapor Hazırken belli safhalar içerisinde hareket etmek gerekir. Bu safhaları; (Maher, 2004)

1. Veri toplamak
2. Sonuçları analiz etmek
3. Raporu taslak haline getirmek ve organize etmek
4. Rapora Son halini vermek
5. Raporun Son halini kontrol etmek

olarak 5 gruba ayırmak mümkündür.

**1-Veri toplamak**

Ekspertiz raporu yazmaya uygun bir planlama ile başlanmalıdır. Daha önceden yürütülmüş olan bir soruşturma, ekspertiz raporunun yazılması için bir gerektir. Ekspertiz raporunun başarılı olması, adli sürecin başlangıcındaki araştırmaların doğru yapılmasıyla ilgilidir.

Önceden toplanmış bilgileri gözden geçirmek esas alınmalıdır. Olay yeri inceleme safhasında yapılan işlemler kaydedilmiş olmalıdır. Bu safhada yapılan işlemler, rapor yazımı sırasında önem arz etmektedir. Önceden yapılan

ve veri incelemesi sırasında yapılan işlemler kolaylıkla anlaşılabilecek şekilde birleştirilmelidir. Bilinen noktalama işaretleri dışında başkaları tarafından yanlış anlaşılabilecek işaretler kullanılmamalıdır. Anlatılmak istenenler açıkça ve kısaca yazılmalıdır. Gereksiz cümleler kullanılmamalıdır. Böyle yapmak zaman tasarrufu sağlayacaktır. Bu safha sırasında, teknik rapor yazarken sonuçların nasıl sunulacağı göz önünde bulundurulmalıdır. Böylece, ihtiyaç halinde rapor yazmanın gelecek safhalarında geri dönerek yapılanlar tekrar gözden geçirilebilir.

**2-Sonuçları analiz etmek**

Bu safha tamamlaması en zor olan kısımdır. Çünkü raporun sunulacağı kitleye vermek istenilen mesaja bu bölümde karar verilir. Sonuçları analiz etme safhası, veri toplama safhasında elde edilen bilgilerin pekiştirilmesi ile başlar. Veri toplama safhasında belirlenen hedefler doğrultusunda incelemeler yürütülür.

İncelemeler sırasında ulaşılan sonuçlar not edilmelidir. Bu safha aynı zamanda, rapor hazırlama sürecindeki en önemli adımdır. Çünkü teknik rapor hazırlamanın temelleri neden-sonuç ilişkisine dayanır. Burada dikkat edilmesi gereken bir nokta, ulaşılan sonuçların oluş sıralamasına göre listelenmesidir. Veri toplama safhasından önce elde edilen eksik bilgiler, bu safhada anlaşılabilir ve düzeltilebilir. Yanlış varılan sonuçlar mahkemede sorun yaratır.

Ulaşılan sonuçlar rapor içerisinde, tablo veya grafik şeklinde gösterilebilir. Bu tür şekiller, varılan sonucu vurgulamak ve desteklemek amacıyla kullanılır. Şekiller hazırlandıktan sonra yapılması gereken, her şeklin açıklayıcısı olan ifadeler yazmaktır. İfadeler anlam olarak: şeklin ne söylemek istediğini, bilgilerin nasıl elde edildiğini, ek olarak diğer bilgilerin olup olmadığını ifade etmelidir.

Rapor eki kullanmak, rapor yazmanın diğer önemli bir unsurudur. Ekspertiz raporu hazırlanırken, bir konu hakkında çok derin bilgi vermek raporun akışını bozabilir ve konu bütünlüğünü dağıtabilir. Bu nedenle raporun ilgili yerlerinde referans verilerek, detaylı konular ek kısmında açıklanabilir.

Son olarak analiz edilen veriler tutarlılık algoritmalarıyla (hash) hesaplanmalı ve bu değerler kaydedilmelidir. Kullanılacak algoritmalar, ülke hukuku tarafından belirlenmemiş ise, uluslararası olarak kullanılan MD5 ve SHA–1 gibi algoritmaları kullanılabilir. Algoritma sonuçlarının bir veritabanında tutulması, rapor sunulan makamlara, delilin uygun yöntemlerle incelendiğini ispatlar.

**3-Raporu taslak haline getirmek ve organize etmek**

Rapor taslağı hazırlamak, ekspertiz raporu yazmanın temelidir. Taslak olmadan hazırlanan raporlarda cümleleri yanlış anlamak veya hiç anlamamak çok olasıdır. Bu safha da veri inceleme safhası gibi olması gereken bir safhadır. Analiz safhasında sonucun ne olacağı üzerine yoğunlaşılmıştı. Bu safhada ise sonuçların nasıl sunulacağı üzerinde yoğunlaşılır.

Yazılan raporu düzene koymak ayrı bir öneme sahiptir. Rapor yazmaya başlarken daha çok karmaşık konulardan daha az karmaşık konulara doğru ilerlemek iyi bir tavsiye olabilir. Çünkü raporun önemli yerlerini okumak isteyen birisi sadece ilk sayfaları okuyabilir. Detay içeren diğer kısımlar onun için önemli olmayabilir.

Diğer taraftan adli bilimler ile uğraşan birimler genellikle standart rapor şablonları kullanırlar. Böyle bir yöntem zaman tasarrufu açısından kullanılabilir. Aynı zamanda çıkarılan raporların ölçeklenebilir ve gerekli düzenlemelerin daha kolay uygulanmasına imkân verir.

Oluşturulan her rapor aşağıdaki bölümleri içermelidir:

a) İdari özet
b) Hedefler
c) İncelenen deliller
d) Diğer bulgular
e) Destek bilgileri
f) Soruşturma bilgileri
g) Diğer bilgiler ve tavsiyeler

**a. İdari özet**

Bu bölüm soruşturmadan elde edilen bilgileri barındırır. Genellikle idari kimseler tarafında takibi yapılan kısımdır. Aşağıdaki bilgileri kapsamalıdır.

- Soruşturmanın hangi birim tarafından yürütüldüğü
- Veriler üzerinde ne tür bilgilerin arandığı
- Ek olarak istenen bilgiler

**b. Hedefler**

Bu bölüm adından da anlaşılacağı üzere incelemenin tamamlanması neticesinde elde edilecek bilgilerin neler olması gerektiğini belirtir.

**c. İncelenen deliller**

Suçla ilgili toplanan tüm deliller bu bölümde belirtilir. Delillerin neler olduğunu ve türlerini içeren bir tablo ilgili makamlar ve raportörlerin anlaşması açısından daha uygun olabilir. Aynı zamanda alınan ve teslim edilen delilleri içeren bir kontrol listesi muhtemel karışıklıkları engelleyecektir.

**d. Diğer bulgular**

Soruşturma sırasında, ilk başta delil olarak nitelendirilmeyerek, uzman görüşü altında delil olması muhtemel bulguların belirtildiği bölümdür. Olayda bulunuş şekli ve durumu ifade edilebilir.

**e. Destek bilgileri**

Veri inceleme uzmanına, delilleri incelerken izleyeceği yol konusunda bilgi verebilecek bölümdür. Olay yeri incelemesi sırasında karşılaşılan delillerin nasıl bir ortamda bulundukları tasvir edilebilir. Veri inceleme uzmanlarının her olay yerine gitme ihtimallerinin olmamasından dolayı, buralardan elde edilen delillerin detaylı olarak anlatılması, araştırmacının işini kolaylaştırarak karşılaştığı çıkmaz durumlarda yeni fikirler sağlayacaktır.

**f. Soruşturma bilgileri**

Soruşturmayı özetleyen bölümdür. Araştırmacı, araştırmasını yürütürken bir yerde durmak zorundadır. Her delil üzerinde, her türlü incelemeyi yapmak büyük bir zaman kaybıdır. Bu nedenle uzmanın incelemeye başlamadan önce ne tür incelemelerin yapılacağına karar vermesi hayati öneme sahiptir. Ne tür incelemelerin yapılacağı sorusu uzmanın tecrübelerine göre değişebilir.

**g. Diğer bilgiler ve tavsiyeler**

Bu bölüm hedef kitlenin niteliğine göre değişebilir. Örneğin, ilgili makam tam olarak delil üzerinde tüm incelemelerin yapılmasını istemiş olabilir. Bu nedenle daha teknik bilgilerle donatılmış bir rapor yazmak uygun olur.

**4-Rapora son halini vermek**

Mantıksal olarak organize edilmiş ekspertiz raporlarına son şeklini vermek daha kolaydır. Aynı konuyu anlatan ve aynı sonuca sahip bir uzman raporu

birden fazla yolla yazılabilir. Her birinin diğerine göre avantaj ve dezavantajları vardır. Taslak hali gözden geçirildikten sonra meydana gelen son rapor önemlidir. Çünkü ilgili makama gidecek olan bu halidir.

Ekspertiz raporu gönderilmeden önce işi incelemeyen diğer veri inceleme uzmanları tarafından gözden geçirilirse, olası hatalar önceden fark edilebilir. Burada dikkat edilmesi gereken nokta, raporun teknik veya teknik olmayan kişiler tarafından okunup anlaşılabilmesidir. Genellikle rapor talebinde bulunan makamlar, teknik bilgiden yoksundurlar. Bu nedenle teknik olmayan bir gözle incelenen verilerin herkes tarafından kolaylıkla anlaşılabilecek bir formatta sunulması gereklidir.

**5-Raporun son halini kontrol etmek**

Genellikle tecrübesiz veri inceleme uzmanları tarafından en sık göz ardı edilen kısımdır. Bu bölümde raporun yapısını değiştiren değişikliklerden ziyade görünümü okumayı kolaylaştıran değişiklikler yapılabilir. Asıl kontrol edilmesi gereken sonucun doğru olup olmadığıdır. Raporun hazırlanması konusunda yapılan tüm işlemler sonucun doğru olması içindir. Bu hiçbir zaman unutulmamalıdır. İkinci olarak raporun yapısının düzgün olup olmadığı kontrol edilmelidir. Konu ve amaçlar tam olarak belirtilmiş midir? Başlangıcından sonuna kadar akıcı mıdır ve anlaşılabiliyor mu? Üçüncü olarak raporun imla hataları, dilbilgisi ve noktalama işaretleri gibi yazınsal durumu kontrol edilmelidir. Gereksiz cümlelerden ve işaretlemelerden kaçınmalıdır.

Ekspertiz raporları, uzmanların adli incelemeler konusundaki düşüncelerini diğer insanlara aktarmaya yarar. Resmi raporlar, mahkemelerde, delillerden

sonuç elde etmiş birer tanıktır. Bu tanıkların, tanıklıklarını güçlendirmenin tek yolu düzgün hazırlanmalarına bağlıdır.

**Amaç**

Adli bilişim inceleme yöntemleri olan eşzamanlı ve eşzamansız incelemelerden, ülkemizin kolluk kuvvetlerinin en sık başvurduğu yöntem eşzamansız incelemedir. Adli bilişim disiplinin ülkemizde yeni kurulmaya başlamış olması ve bu alanda çalışan bilgi birimine sahip personelin yeterli sayıda olmamasından dolayı bilişim suçlarında eşzamansız incelemeler yürütmek muhtemel yanlış neticelere ulaşmayı engelleyecektir. Çalışmada, ülkemiz kolluk kuvvetlerinin adli bilişim alanında sahip olduğu bilgilere katkısı olması açısından eşzamansız inceleme yöntemi incelenecektir. Bu araştırmanın amacı; bilişim suçlarının niteliklerinin belirlenmesi, vuku bulduğu olay yerlerinden elde edilen delillerin sınıflandırılmasına göre el konulması ve laboratuvara gönderilmesi aşamalarında uygun yöntemlerin geçerlilik ve güvenirlilik durumlarını saptamaktır.

Araştırma konusuna benzer çalışma ve tezlerin daha öncesinde yapılmış olduğu görülmüştür. Ancak bilişim suçlarını genel olarak tanımlamaya yönelik bu çalışma ve tezler, bilişim suçlarında olay yeri incelemesi ve data incelemeleri konusunda detaylı bilgilere haiz değildir.

# 2. GEREÇ VE YÖNTEM

Bilişim sistemlerinin doğası gereği, adli bilişim alanında kullanılan gereçler iki kısım altında toplanır.

## 2.1. Adli Bilişimde Kullanılan Yazılımlar

Yazılımlar genel olarak donanım sistemleri üzerinde çalışmaya programlanmış kod dizileridir. Bilgisayar programcıları tarafında belli bir amacı gerçekleştirmeye yönelik olarak üretilirler. Birkaç satır kodla oluşturulmuş yazılımlar olabileceği gibi milyonlarca satır koddan oluşmuş yazılımlar da olabilir. Adli bilişimde kullanılan yazılımlar genellikle en alt seviye donanım birimleri ile iletişim kurmaya yetenekli kompleks yazılımlardır. Genel olarak toplumun kullandığı yazılımlar olmadıkları için çoğunlukla kanun kuvvetlerinin ihtiyaçları ve talepleri doğrultusunda hazırlanırlar. Bu nedenle fiyatları diğer popüler programlara göre daha fazladır.

Adli bilişim dalında kullanılan yazılımlar bazen kendilerini has donanım kullanılmasını gerektirirler. Bu tür yazılımlar kullanım sırasında gereken esnekliği azalttıkları için pek tercih edilmezler. Bazı tür yazılımlar ise ortak bir dosya formatı (mesela imaj) standardı oluşturmaya çalışırlar.

Adli bilişimde kullanılan yazılımlar; veri kurtarma yazılımları, veri inceleme yazılımları, veri depolama yazılımları ve veri koruma yazılımları gibi gruplara

ayrılırlar. Farklı gruplara ayrılmalarının sebebi her tür grubun farklı fonksiyonları yerine getirmeleridir.

Veri kurtarma yazılımları adli bilişimde en çok kullanılan yazılım türüdür. Çünkü genellikle şüpheli delil üzerinde bulunan normal yazılımlar ile görülemeyen silinmiş verileri bu tür yazılımlar ile kurtarmak mümkündür. Bilişim piyasasında genellikle iki tür kullanıcıya hitap eden veri kurtarma yazılımları mevcuttur. Alt seviye kullanıcılara yönelik olan yazılımlar genellikle fazla teknik bilgi gerektirmeyen, işlemleri otomatik olarak yapan ve kullanıcılara pek fazla seçenek sunmayan yazılımlardır. Üst seviye yazılımlar ise kullanıcısına birçok opsiyon sunmaktadır. Bu opsiyonları anlamak genellikle derinlemesine bilgisayar bilgisini gerektirmektedir. Adli bilişim profesyonelleri tarafından kullanılan veri kurtarma yazılımları donanım sistemleriyle iletişime doğrudan geçerek incelemeler sırasında diğer sistemlerin olaya müdahalesini engellemektedir.

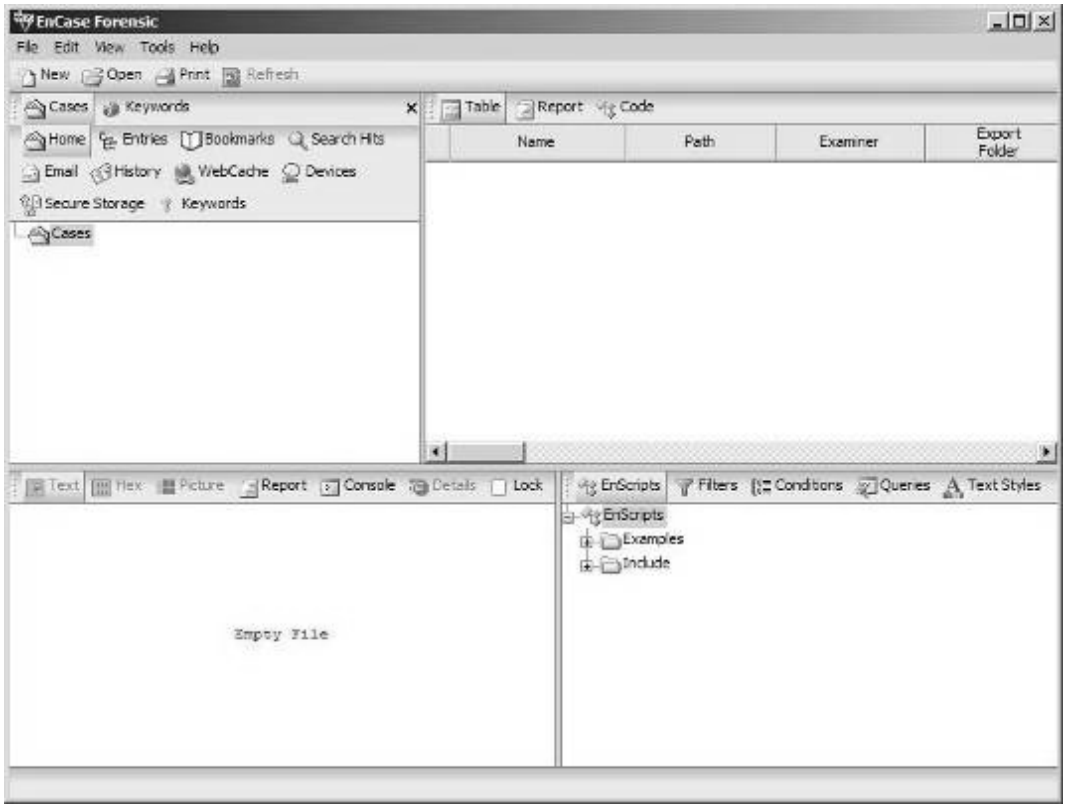
### 2.1.1. Encase

Adli Bilişim dünyasında en çok kullanılan veri kurtarma yazılımı Encase'dir. Dünya çapında 15,000 araştırmacı tarafından kullanılmaktadır. En büyük 50 bilişim firmasının 40'ı Encase yazılımını aktif olarak çalışanlarının bilgisayarlarında kurulu bulundurmaktadır. Encase yazılımı genellikle kanun kuvvetleri, hükümetler ve kurumsal şirketler tarafından kullanılmaktadır. Dünya ülkelerindeki birçok mahkemeler tarafından resmi veri kurtarma ve raporlama yazılımı olarak kabul görmektedir.

Encase yazılımı ile birçok farklı dijital medyanın imajı alınabilir. Bunlardan en sık kullanılan medya türü bilgisayar sabit diskleridir. Günümüzde yüksek kapasitelere sahip olan modern sabit diskler Encase tarafından kolaylıkla imajlanabilmektedir. Adli bilişimde, elektronik delillerin mutlaka kopyaları üzerinde çalışılması gerektiğinden elde edilen delillerin güvenilir bir yöntemle imajlarının alınması gerekmektedir. Encase sahip olduğu özellikler ve doğrulama algoritmaları sayesinde bu görevi profesyonel bir şekilde yerine getirebilmektedir.

## Encase İle İmaj Alma İşlemi

Encase yazılımı çalıştırıldığında aşağıdaki dört bölümlü ekran görünür.

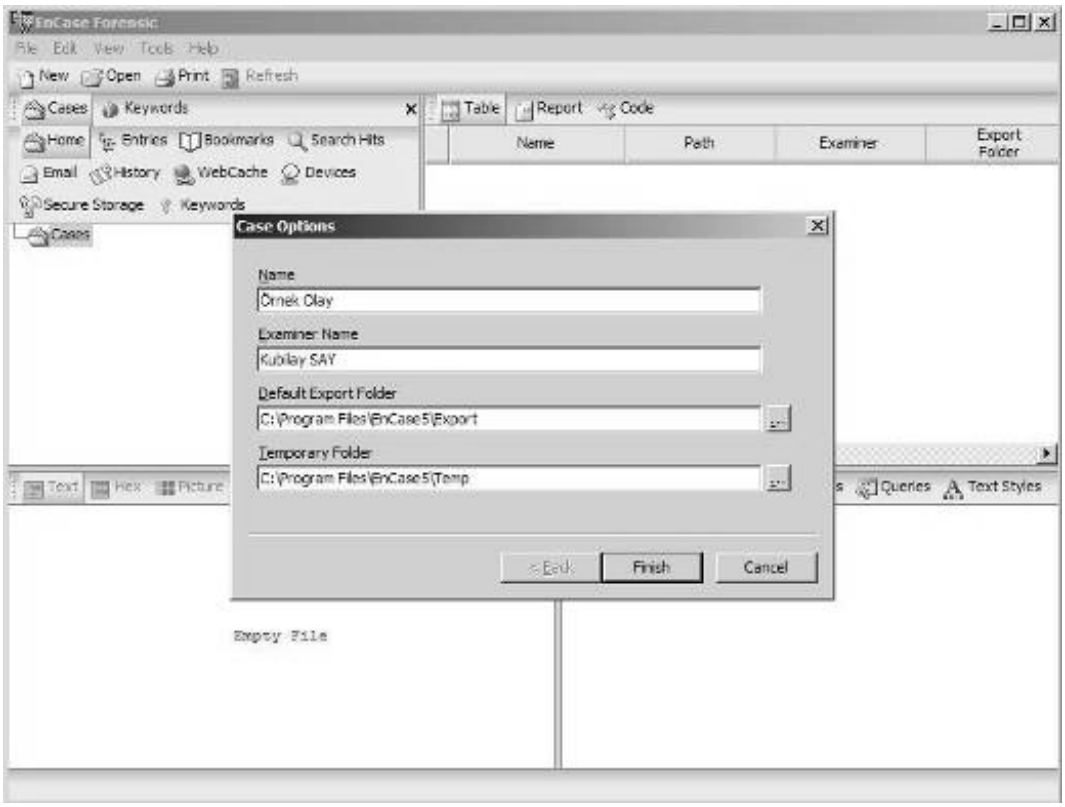


Şekil-2.1: Encase Ana Ekranı

Yukarıdaki şekilde görünen kavramların açıklamaları aşağıdaki gibidir.

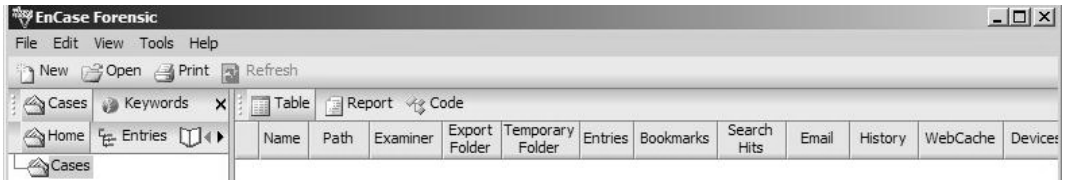
**New**

Windows işletim sisteminde imaj alma işleminde öncelikle bir olayın açık olması gerekir. Yeni bir olay oluşturulacaksa, bu işlem File/New menüsünden veya New butonu üzerinden yürütülebilir. Encase felsefesi ilke olarak değiştirilemeyen imajlarla eşleştirilmiş bir olay dosyasını içerir.




Şekil-2.2: Vaka Opsiyonları

Bunu takip eden diyalogda önce olay adı (ör. terör olayı), incelemeyi yapanın adı, imajdan kopyalanacak olan dosyalar için standart klasör ve de geçici olarak başka programlar altında kullanılacak dosyalar için bir klasör (ör. üçüncü bir program ile resim görüntüleme) belirtilmelidir.



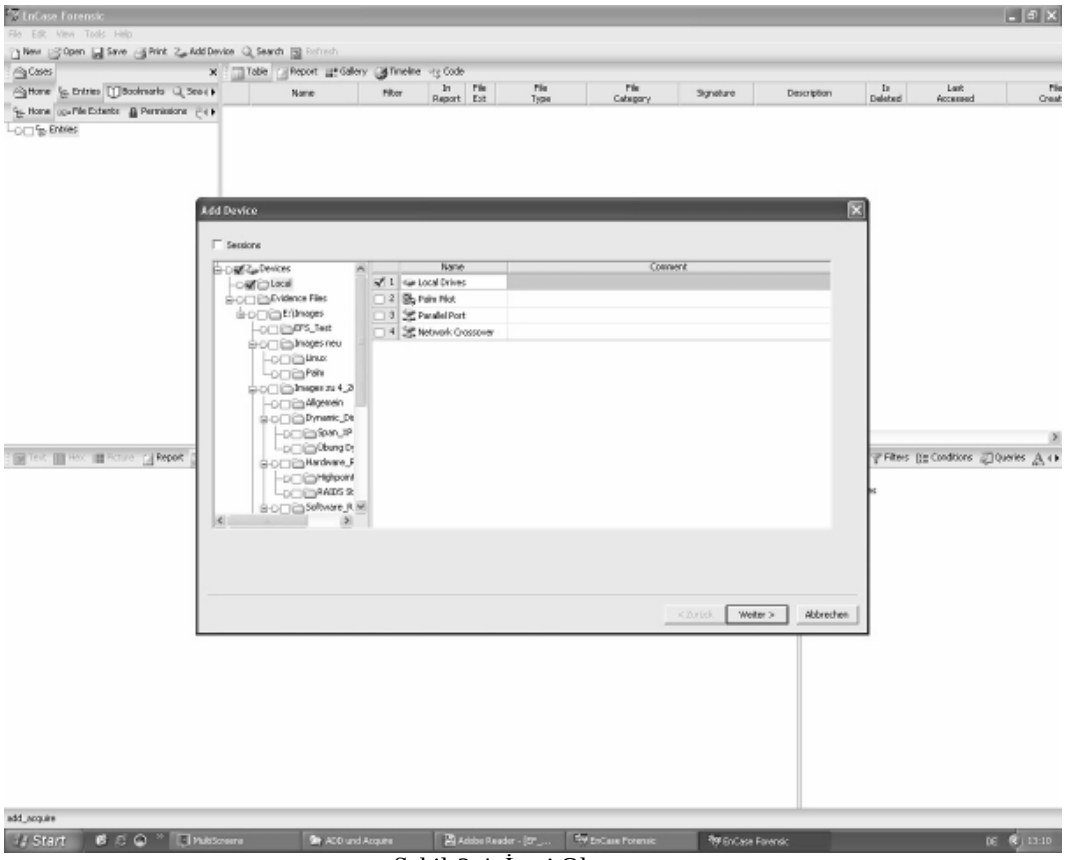
Şekil-2.3: Menüler

Açık olaylar Cases/Home/Cases altında gösterilir.

Bir imaj oluşturmak için öncelikle seçilen bellek üzerinde bir Preview gösterilir.

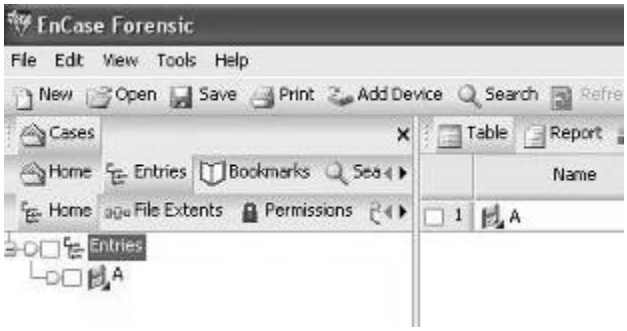
## İmaj oluşturma

Bunun için Add Device işlevi kullanılır.




Şekil-2.4: İmaj Oluşturma

İşlem yapılacak ortam seçildikten sonra, bu bellek ağaç (Tree) görünümünde Entries altında ön izleme şeklinde gösterilir (mavi üçgenden anlaşılır).



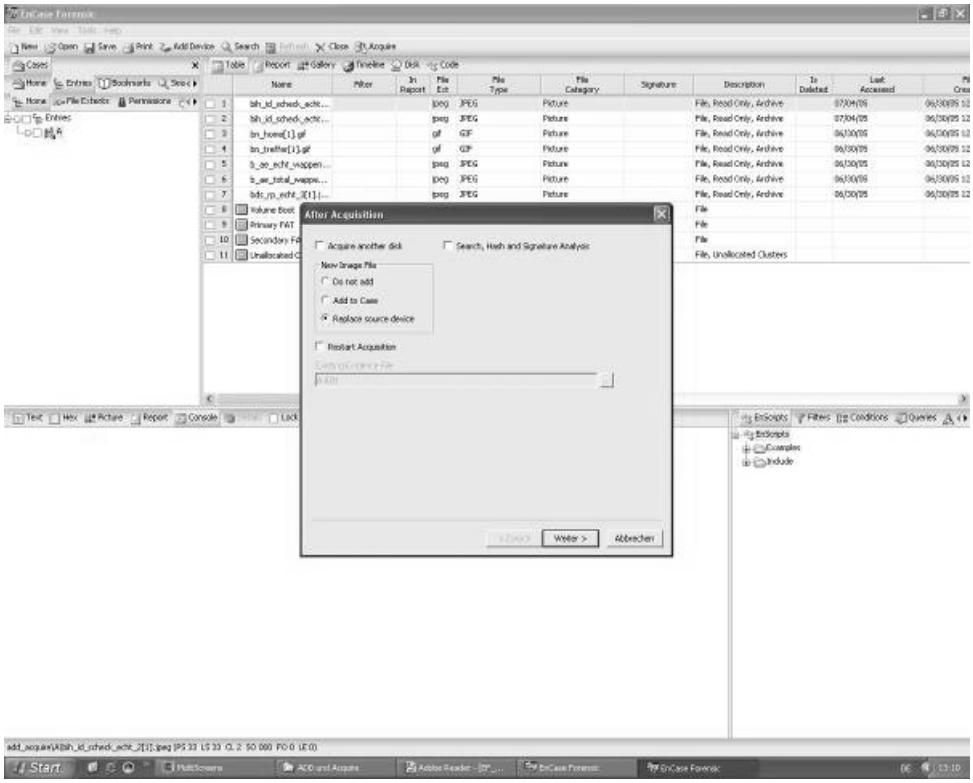

Şekil-2.5: Girdiler

**Önemli:**
Şimdiye kadar herhangi bir imaj oluşturulmamıştır. Yalnızca ön izleme şeklinde verilere erişim vardır! Bu nedenle bellek simgesinde küçük, mavi bir üçgen belirir.

**Önemli:**
Windows için Encase dongle (güvenlik lisansı) olmadan kullanılıyorsa, şimdiye kadar anlatılan adımlar uygulanabilir. Ancak bunun farkı, güvenceye alınacak ortam üzerinde bir ön izleme (preview) yapılamamasıdır. Program güvenli kipte çalışmaktadır.

## Acquire

Acquire komutu ile imaj alma işlemi başlatılabilir.




Şekil-2.6: Acquire işlemi

**Acquire another disk**

Acquire another disk kutusu işaretlenirse, işlem bittikten sonra, başka ön izleme yapılmadan başka imajlar da oluşturulabilir.

**Do not add**

Bu seçenek imajın kaydedilmesine izin verir, şimdilik bir erişim olmayacaktır.

**Add to Case**

İmaj oluşturulur, kaydedilir ve ön izlemeye paralel olarak olay içinde gösterilir.

**Replace source device**

İmaj oluşturulur, kaydedilir ve daha önce ön izlemede gösterilmiş olan belleğin yerine geçer.

## 2.2. Adli Bilişimde Kullanılan Donanımlar

### 2.2.1. Yazma-Koruma Sistemleri (Writeblocker)

Yazma-koruma kitleri elektronik delillerden dijital delil oluşturma işlemi sırasında, delilin bilgisayara bağlanması nedeniyle kontamine olma ihtimalini ortadan kaldırmaya yarayan sistemlerdir. Tüm adli bilim dallarında olduğu gibi adli bilişimde de delillerin incelemeler sırasında değiştirilmemesi esastır. Bu esas doğrultusunda adli bilişim uzmanlarının gerekli tedbirleri alması gerekmektedir. Yazma-koruma sistemleri delillerin üzerindeki muhtemel değişiklikleri engelledikleri için kullanılması zaruri sistemlerdir.

Yazma-koruma sistemleri genellikle bir giriş, bir çıkış ve bir güç ünitesinden oluşurlar. Giriş kısımlarında imajı alınacak olan elektronik deliller, çıkış kısmına ise ya diğer bir sabit disk veya bilgisayarlar bağlanır. Güç ünitesi ise giriş ve çıkış kısımlarına bağlanan cihazların çalıştırılmasını sağlar.

Şekil-2.21: Yazma-Koruma Sistemi

Yazma-koruma sistemlerinin giriş üniteleri genellikle IDE, SATA veya SCSI formunda olabilir. Elektronik delillerin arabirim formuna göre uygun olan yazma-koruma sistemi kullanılmalıdır. Formun türüne göre cihazlar arasındaki iletişim hızı değişmektedir. Standart şartlar altında;

IDE = 133 MegaBayt/saniye

SATA = 150 MegaBayt/saniye

SCSI = 320 MegaBayt/saniye

olarak düşünülebilir. SCSI arabiriminin aktarım hızı daha yüksek olduğundan imaj alma işlemi daha kısa sürecektir.

Yazma-koruma sistemlerinin giriş üniteleri ise genellikle USB veya Firewire türünde olurlar. Günümüzde bütün bilgisayar sistemlerinde bulunan bu tür bağlantılar farklı hızlara sahiptirler.
Firewire = 400 Megabit/saniye
USB = 480 Megabit/saniye

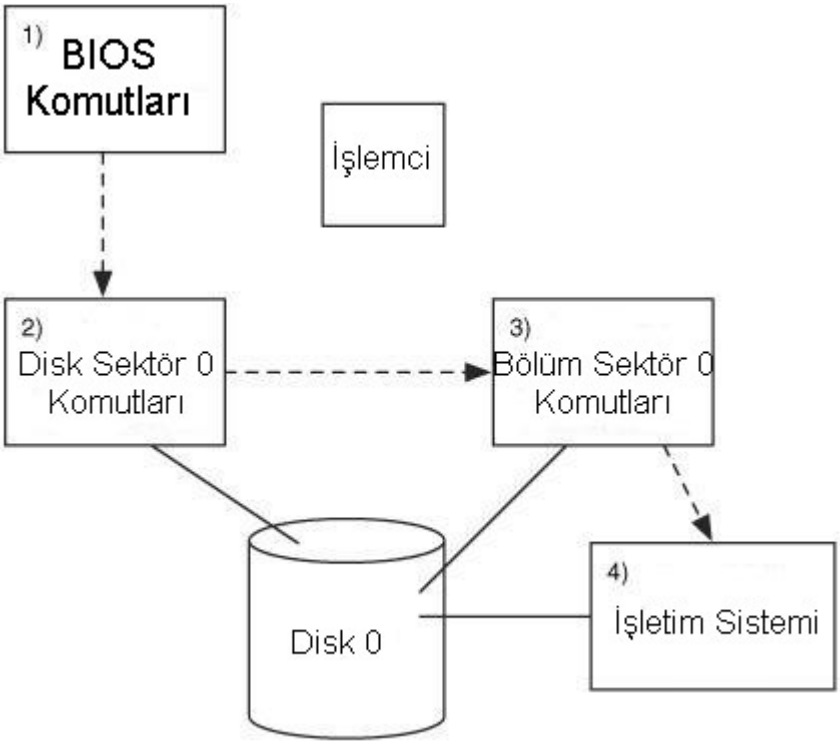
### 2.2.2. Sabit Diskler

Bilgisayarların kalbi sayılan işlemciler bir bilgisayarda bir ya da daha fazla sayıda olabilir. Intel'in Pentium, AMD'nin Athlon, Motorola'nın PowerPC ve Sun'ın UltraSPARC'ı bilinen işlemci modelleridir.[32] İşlemciler kendilerine iletilen komutları yerine getiren hesap makineleri olarak düşünülebilir. Hesap makineleri ne kadar karmaşık işlemleri yerine getirme kabiliyetine sahip olurlarsa olsunlar, ona ne yapmasını söyleyecek bir insana ihtiyaçları vardır. Aynen bunun gibi işlemciler de yürütecekleri komutları bellekten alırlar. Bu komutlar makine dilindedir ve insanların kolayca anlayabileceği türde değildirler.

Bilgisayarların açma düğmesine basarak çalışır hale getirilmesi için işlemcinin bir tür komut dizisini yerine getirmesi gereklidir. Bilgisayarın güç düğmesine bastığımız zaman işlemci devreye girerek işleteceği komutları belli bir yerden almaya başlar. Bu yer genellikle ROM (Read Only Memory) olarak tabir edilen ve elektrik kesildiğinde üzerindeki bilgilerin kaybolmadığı BIOS'tur. (Basic Input Output System). BIOS kendi başına küçük bir bilgisayar gibidir. Ana bilgisayarın donanım bilgilerini hafızasında tutar. İşlemci tarafından işleme konulan BIOS üzerindeki bilgiler, bilgisayar donanımını kontrol ederek

[32] http://en.wikipedia.org/wiki/Central_processing_unit, Erişim Tarihi: 15.03.2006

gerekli ayarlamaları yapar. Bir bakıma bilgisayarın ayağa kalkmasına yardımcı olur. Daha sonra işlemci BIOS'taki komutları yürüttükten sonra sıradaki diğer komutları işleme alır. Bunlar genellikle sabit diskin ilk sektöründeki başlangıç komutlarıdır. İlk sektörde bulunan komutlar, işlemcinin işletim sistemini bulmasına ve onu yüklemesine yardımcı olur. Sıra işletim sistemini yüklemeye geldiği zaman açılma işlemi tamamlanmıştır ve bilgisayar çalışmaya başlamıştır.

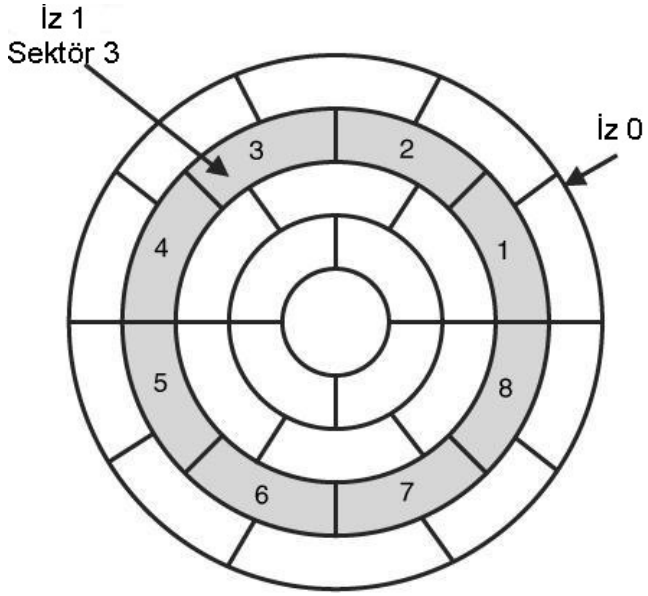



Şekil-2.22: Bilgisayarın Açılış Süreci

Sabit diskler, bilgisayarlardaki en önemli delil kaynaklarıdır. Sabit diskler birbiri üzerine yerleştirilmiş silindirik plakalardan oluşurlar. Diskin içerisinde, her plaka için ileri-geri hareket eden kollar bulunur. Bu kolların ucunda veri okuma ve yazmaya yarayan kafalar bulunmaktadır. Sabit disklerin çalışma mekanizması aynen pikaplara benzer. Ancak sahip olduğu yüksek teknoloji

sayesinde mikron yakınlaşma mesafesinden okuma ve yazma yapabilmektedirler.

Sabit diske uygulanan formatlama (biçimlendirme) işlemi boş olan plakalar üzerindeki izleri (track) ve sektörleri (sector) belirler. İzler, plakalar üzerinde bulunan dairesel çizgiler olarak düşünülebilir. İzlerin numaralandırılması dıştan içe doğrudur. Yani en dıştaki izin numarası 0 olarak kabul edilir. Birbirinin aynısı olan üst üste bulunan plakaların 0. izleri 0. silindiri oluşturur. Aynı şekilde tüm plakaların 1. izleri 1. silindiri oluşturur.




Şekil-2.23: Sabit Disk İz ve Sektörleri

Her iz anlamlı parçalara bölünmüştür. Disk üzerinde adreslenebilen en küçük birim olan bu parçalara sektör adı verilir. Genellikle sektörlerin boyutu 512 Bayttır. Her sektörün bir adresi vardır. Bir sektörü, bulunduğu silindirin (C), kafanın (H) ve sektörün (S) kendi numarası ile belirtebiliriz. Ancak yeni nesil

sabit disklerde bu adresleme metodu yerine sektörlerin mantıksal yerini belirten LBA adresleme yöntemi kullanılmaya başlanmıştır.

Sabit diskin plakaları üzerinde bulunan sektörler bazen fiziksel olarak bozulur ve kullanılmaz hale gelebilirler. Bu tür bozuklukları bazı ileri seviye disk yönetici programlar ile düzeltmek mümkün olabilir. Ancak genellikle tam olarak düzeltilemezler. Çünkü meydana gelen bozukluk fizikseldir. Modern işletim sistemleri sabit diskte meydana gelen bozuklukları tespit ederek onları kullanılmaz sektörler (bad sector) olarak işaretler ve o sektörlere daha sonra herhangi bir bilgi yazmaz.

Diskten bilgi okuyup yazabilmek için işletim sisteminin sabit disk sektörlerini adresleyebilmesi gerekmektedir. Sabit diskler her bölümlendiğinde veya dosya sistemini değiştirildiğinde, sektörlerin adres numaraları değişir.

Sabit disklerde kullanılan 2 tür adresleme yöntemi vardır. İlki ve eski olanı CHS yöntemidir. Bu yöntem sabit diskte bulunan sektörleri, silindir, kafa ve sektörün adresini kullanarak tanımlar. Ancak bu parametrelerin (C, H, S) kombinasyonlarını kullanarak yapılan adresleme ile maksimum 8,1 Gigabayt[33] (GB) kapasitedeki sabit diskleri adresleyebiliriz.

8,1 GB'lık kapasite limitini aşabilmek amacıyla LBA (Logical Block Addresses) yöntemi geliştirilmiştir. LBA yöntemi sabit diskin fiziksel yapısı ile ilgili değildir. Her sektör için 0'dan başlayan ve birer birer artan bir adres vardır. CHS sisteminde 0,0,1 olan sektörün adresi LBA sisteminde 0'dır.

[33] 1 GB = $10^9$ Bayt

## 2.3. Sabit Disk İmaj Alma Yöntemi

Data incelemeleri her zaman şüpheliden elde edilen delillerin kopyaları üzerinde çalışılarak yapılır. (Casey, 2002, s.:73) Tipik bir kopya alma işlemi, sabit diskler için 512 Baytlık birimlerin ardı sıra başka bir medyaya kopyalanmasıdır. (Carrier, 2005, s.:38) Çünkü genellikle sabit diskler üzerinde bulunan veriler, 512 Baytlık sektörler halinde bulunurlar.

Bilgisayar sistemlerinde kopyalama işlemi genellikle 3 seviyede yapılır. Bunlar: disk seviyesi, bölüm seviyesi ve dosya seviyesidir. Bölüm seviyesinde ve dosya seviyesinde yapılan kopyalamalar, her hangi bir dosyayı normal bir kullanıcı olarak kopyalamaktır. Bu durumda diskte bulunan silinmiş veya kısmen silinmiş dosyalar kurtarılamayacaktır. Ancak disk seviyesinde yapılan kopyalama ile orijinal diskin birebir kopyası alınabilir. Bu tür kopyalamaya en alt seviye kopyalama veya fiziksel kopyalama da denilebilir.

Teorik olarak, şüpheli delil üzerinde bulunan her sektör aradığımız ipucunu içeriyor olabilir. Bu nedenle bölüm seviyesi ve dosya seviyesinde yaptığımız yüzeysel (sadece aktif dosyalar) kopyalamalar veri kaybına neden olur. Bölüm ve dosya seviyesinde yapılan kopyalamalarda silinmiş ve gizlenmiş bilgilere ulaşılamaz.

Adli bilişimde kullanılan kopyalama yöntemi, disk seviyesidir. Bu kopyalamanın literatürde geçen diğer adı “bit-by-bit” kopyalamadır. Çünkü orijinal disk ile kopya disk her anlamda birbirine denk olur.

Disk seviyesinde kopyalama yapma işlemi önemli bir adımdır. Bu nedenle, bu tür kopyalama yapan sistemler ve yazılımlar Amerikan Ulusal Teknoloji Standartları Enstitüsünce test edilmektedir. Konuyla ilgili test sonuçlarına kurumun İnternet sitesinden[34] ulaşılabilir.

Şüpheli diskin imajı iki şekilde alınabilir: aktif ve pasif kopyalama. Aktif kopyalamada hâlihazırda çalışan sistemlerin kopyaları alınır. Kritik iş akışlarının olduğu (e-bankacılık işlemleri gibi) sistemlerde ağ kartı gibi arabirimler vasıtasıyla yapılan kopyalama işlemidir. Çalışan sistem uygulanan işlemlerden etkilenmez. Ancak inceleme sırasında değişen dosyalar kopyalanamaz. Pasif kopyalamada ise bilgisayarın gücü kesilir ve sabit disk üzerinde yazmaya karşı korumalı yazılım ve donanımlar ile çalışılır. Bu durumda sabit disk üzerinde kurulu bulunan işletim ve dosya sisteminin bir önemi yoktur. Çünkü disk üzerinde bulunan sektörlerin imajını alan yazılım veya donanımlar sadece 1 ve 0 bilgilerini tanırlar.

İmaj alma işlemi sırasında yapılan 2 işlem vardır. Kaynak (orijinal) diskten okuma ve hedef diske yazma. Kaynak diskin okunması sırasında iki farklı metot kullanılabilir. Birincisinde kullanılan yazılım sabit diske doğrudan erişmektir. Bunu yapabilecek yazılımın, sabit disk kontrol komutlarına göre programlanmış olması gerekmektedir. Diğer metot ise BIOS aracılığıyla diske erişmektir. BIOS ile diske erişmek daha kolay gibi görünmektedir. Çünkü kullanılan yazılımın gerekli komutları kullanmasına gerek kalmaz. Ancak sabit disk incelemelerinde bu yöntem önemli bir dezavantaja sahiptir. Yapılan incelemenin seyrini değiştirmemek için adli bilişimde birinci yöntem tercih edilmelidir.

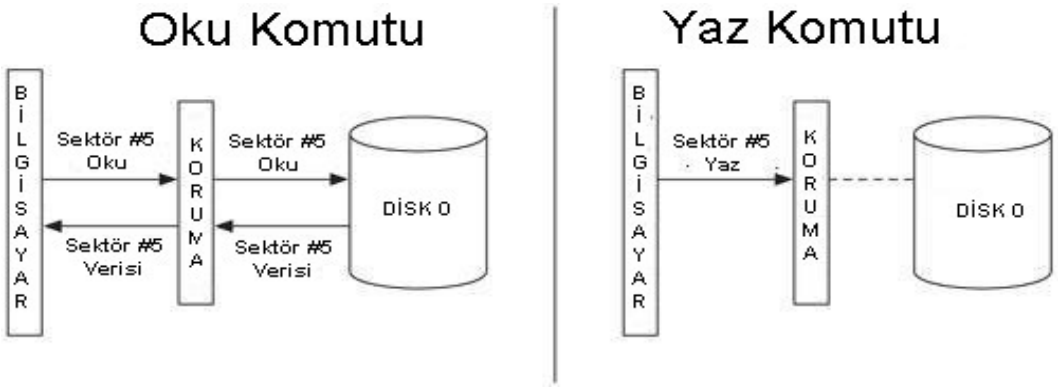
[34] http://www.cftt.nist.gov/disk_imaging.htm, Erişim Tarihi: 02.04.2066

Kopyalama sırasında BIOS kullanılacak olursa, inceleme sırasında BIOS'un verdiği tüm veriler doğru kabul edilir. Ancak öyle olmayabilir. Mesela bir sabit diskin boyutu 40 GB ise ve BIOS onu 30 GB olarak görür ise, geriye kalan 10 GB'lık kısım değerlendirilmemiş olur ve kopyalanmaz. Bu da araştırmanın seyrini değiştirmek demektir. BIOS'un sabit diski yanlış tanımasının birkaç sebebi olabilir. BIOS öntanımlı bir kapasitede değeri okumaya ayarlanmış olabilir veya disk yapısını okumak için yanlış bir okuma yöntemi seçebilir. Bu durumda kaynak diskin kapasitesi yanlış anlaşılacaktır.

Kaynak diskten okuma işlemi yürütülürken kullanılan yazılım, okuma hatalarını tolere edebilmelidir. Genellikle okuma hataları disk yüzeylerinde meydana gelmiş olan fiziksel arızalardan kaynaklanır. Arızalı olan sektörler ihmal edilerek okuma işlemi tamamlanabilir.

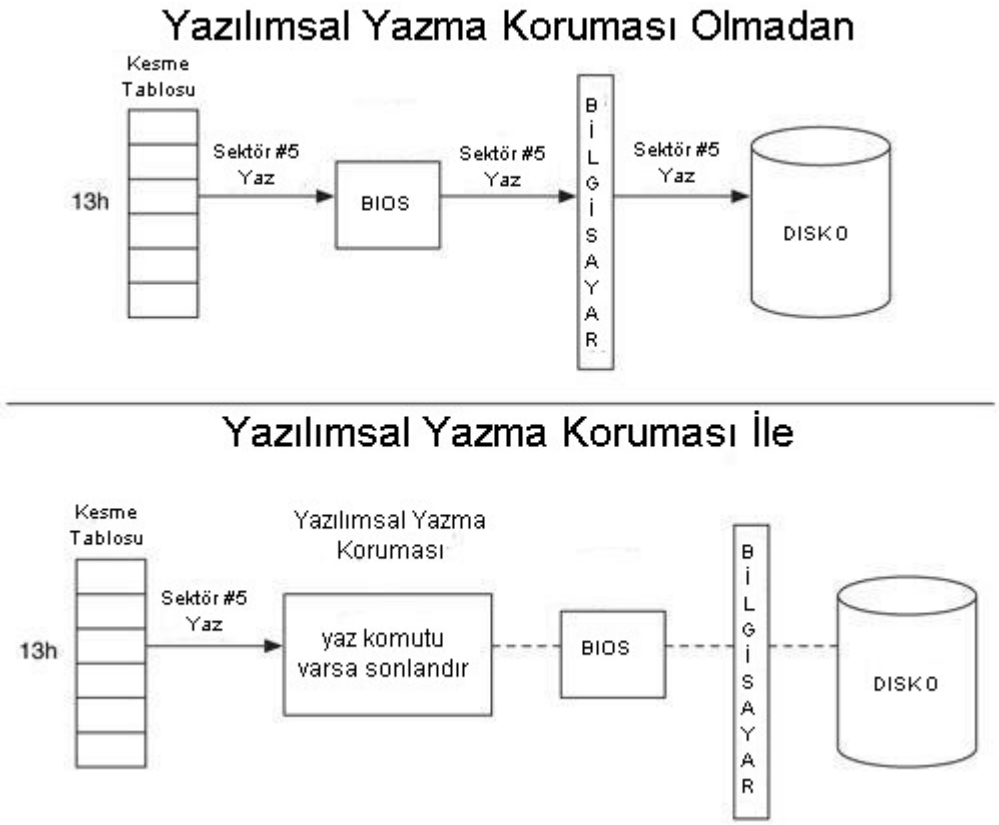
Adli bilişim incelemeleri sırasında dikkat edilmesi gereken önemli bir nokta, incelenen delilin kesinlikle değiştirilmemesidir. Yazma koruması genellikle kaydedilebilir medyalarda kullanılan bir koruma önlemidir. Örneğin disketlerin köşelerinde bulunan kare şeklindeki çentikler ile yazma koruması aktif veya pasif yapılır. Kopyalama sırasında kullanılan yazma koruması ise biraz daha farklıdır. Bu tür korumalar tek yönlüdür. Yani orijinal medyaya doğru tüm yazma işlemleri engellenir. Orijinalden hedefe doğru olan iletişim ise yazmaya elverişlidir. İşletim sisteminin sabit diske veri yazabilmesi için sabit diskin kontrol kartı ile iletişim kurabilmesi gerekir. İletişim ise kontrol komutlarını söz konusu karta iletmesidir. Yazma korumaları, işletim sisteminden gelen "yaz" komutlarını kontrol kartına iletmez. Böylece arada bir tampon bölge oluşturur. Sabit diskten işletim sistemine doğru olan "oku"

komutlarına ise izin verilir. Yani tek yönlü bir seçici-geçirgenlik söz konusudur.




Şekil-2.24: Yazma koruması sistemlerinin genel çalışma prensibi

Donanımsal yazma-koruma sağlayan sistemlerin yanı sıra yazılımsal yazma-koruması sağlayan yazılımlar da vardır. Bu yazılımlar işletim sistemlerinin bilgimiz dışında yürütmek istediği yazma işlemlerini engellemek için DOS işletim sistemi altında çalışırlar. Yazılımsal yazma-korumaları işletim sisteminin diske yazmak için kullandığı komutları (kesmeler) değiştirerek koruma sağlarlar. Diske gönderilen her kesme BIOS tarafından kontrol edilir. Mesela INT13h kesmesi diske, yazma yapmak için kullanılır. Yazılımsal yazma-korumaları BIOS'taki kesmeleri değiştirerek kaynağa doğru olan yazma komutlarını iptal ederler. İşletim sistemi INT13h fonksiyonunu kullanmak istediği zaman, yazma-koruma yazılımı bunu değiştirerek sadece okuma yapılmasını sağlar.




Şekil-2.25: Yazılımsal yazma koruma sistemlerinin çalışma prensibi

Daha önce de bahsedildiği gibi BIOS'u kullanmadan, kontrol kartıyla iletişim kurmaya programlanmış yazılımlar, diske kolayca yazma yapabilirler. Böylece BIOS devre dışı kalır. Bundan dolayı adli bilişim incelemeleri için yazılımsal yazma-koruması kullanmak doğru değildir. Her zaman, kontrol kartıyla iletişim yeteneğine sahip bir programın orijinal delili değiştirme ihtimali vardır.

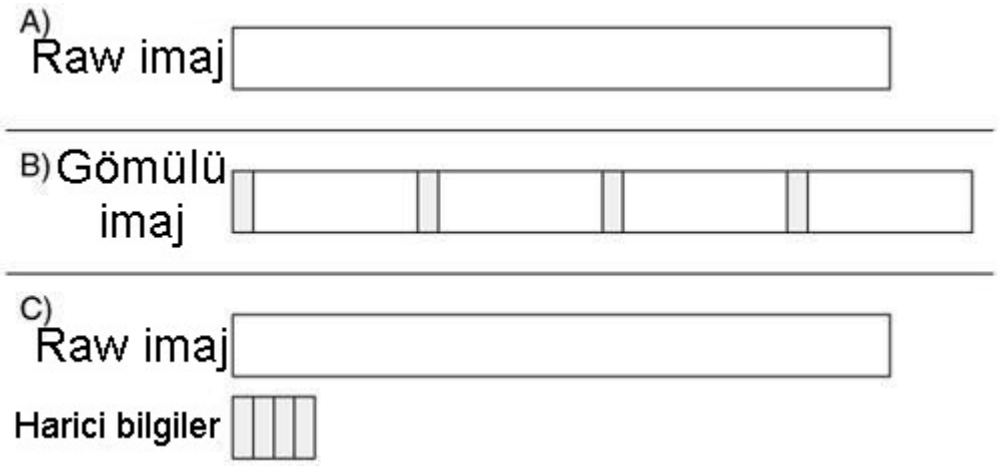
Kaynak diskten okuma işleminden sonra sıra hedef diske yazma işlemine gelir. Yazma işleminde verilerin kopyalanacağı medya ve saklama formatı önem arz eder. Orijinal diskten okunan veriler daha önceden sadece 0 bit ile doldurulmuş olan medyaya kopyalanmalıdır. Her imaj alma işlemi için farklı

medyalar kullanılmayacağı için elimizdeki medyaları (sabit diskler) silerek (wipe) tekrar kullanılabilir duruma getirebiliriz. Burada silmek yerine "wipe" işleminin yapılmasının sebebi, "wipe" işleminin silme işlemine göre farklı bir algoritmaya sahip olmasıdır. Silme işlemi sadece dosyaların, dosya sistemindeki adres ve uzunluk bilgilerini silmekte iken, wipe işlemi verileri ve verilerin disk üzerinde bulunan tüm değerlerini 0 yapmaktadır. Silme işleminden sonra disk üzerinde herhangi bir dosya olmadığı görülür. Ancak sadece işletim sistemi tarafından dosya isimleri gösterilmemektedir. Oysaki dosyalar yerlerinde durmaktadır. Wipe işlemi sonrasında disk üzerindeki her sektör 0 bilgisiyle işaretlenir. Böylece diske daha sonradan yapılan kopyalama işlemlerine, eski verilerin dâhil olma ihtimali ortadan kalkar. Yani sabit disk adli bilişimde steril hale getirilmiş olur.

Olay yeri incelemesi sırasında elde edilen sabit diskler bir sistemin çalışması için kritik öneme sahip ise diskin kopyasını olay yerinde almak daha uygun olabilir. İmaj alma işlemi için hedef diskin kapasitesi önemlidir. Hedef disk kaynak diskten her halükarda eşit veya büyük olmalıdır. Eğer hedef disk kaynak diskten büyük ise bazı problem ortaya çıkabilir. Mesela kaynak diskimiz 30 GB iken hedef diskimiz 40 GB ise imaj alma işleminden sonra hedef diskin sonu (verilerin bittiği adres) işletim sistemi tarafından tespit edilemeyebilir. Çünkü imaj alma işlemleri dosya içeriği okunmadan, fiziksel seviyede yapılmaktadır. Bu olasılığı engellemek için hedef disk ile kaynak diskin tam olarak eşit kapasitede olması gerekmektedir. Olay yeri inceleme ekipleri, olay yerlerinde ne tür bulgularla karşılaşacaklarını bilemedikleri için her kapasitede diskin eşleniği yanlarında olmayabilir. Bu durumda yapılması gereken, orijinal diskin, uygun bir formatta ve farklı bir medyaya imaj olarak yazdırılmasıdır.

Teorik olarak kaynak diskin kapasitesi büyük ise oluşturulan imajın boyutu daha büyük olur. Genellikle imaj dosyasının kopyalanacağı medya başka bir sabit disk veya CD-ROM, DVD gibi optik ortamlardır. Eğer seçilen ortam CD-ROM veya DVD gibi sınırlı kapasitede medyalar ise kopyalama işlemine başlamadan önce hedef ortamın kapasitesine göre imaj eşit bölümlere ayrılmalıdır ve tam olarak medyalar doldurulmamalıdır. 700 Megabayt (MB) kapasiteli CD-ROM'lar için 700 MB bölümler ayırmak yerine 650 MB'lık bölümler oluşturmak daha güvenli olacaktır.

Oluşturulacak olan imaj genellikle 3 farklı formatta kaydedilebilir: Raw (ham) imaj, gömülü imaj ve Raw + harici dosya bilgisi imajı. Ham imajlar kaynak medyayla aynı bilgileri içerirler. Gömülü imaj ise kaynak medyayla aynı bilgileri ve medya ile ilgili diğer bilgileri (imaj alma zamanı ve süresi, hash değerleri, tarihler) içerirler. Bazı imaj alma sistemleri ise imaj dosyasını ham olarak almakta ve diğer bilgileri farklı bir dosya çıktısı olarak vermektedirler.




Şekil-2.26: İmaj dosyası formatları

Genellikle her imaj alma yazılımının kendine has bir dosya formatı vardır. Bu formatları okumak için yazılımın kendisi kullanılmalıdır. Tüm yazılımların tanıması için ise ham imaj formatı oluşturulmuştur. Ancak bu formatta ekstra bilgi yoktur.

İmaj alma işlemi sırasında kaynak diskten gelen verileri hedef medya içerisinde sıkıştırarak saklayabiliriz. Verileri sıkıştırarak saklamak imaj boyutunun küçülmesini ve böylece yer kazancı sağlar. Ancak sıkıştırma yapılarak imaj almak normal imaj almaktan daha uzun sürer ve imaj oluşturulduğu dosyalara geri çevrilmek istendiğinde de zaman farkı artar.

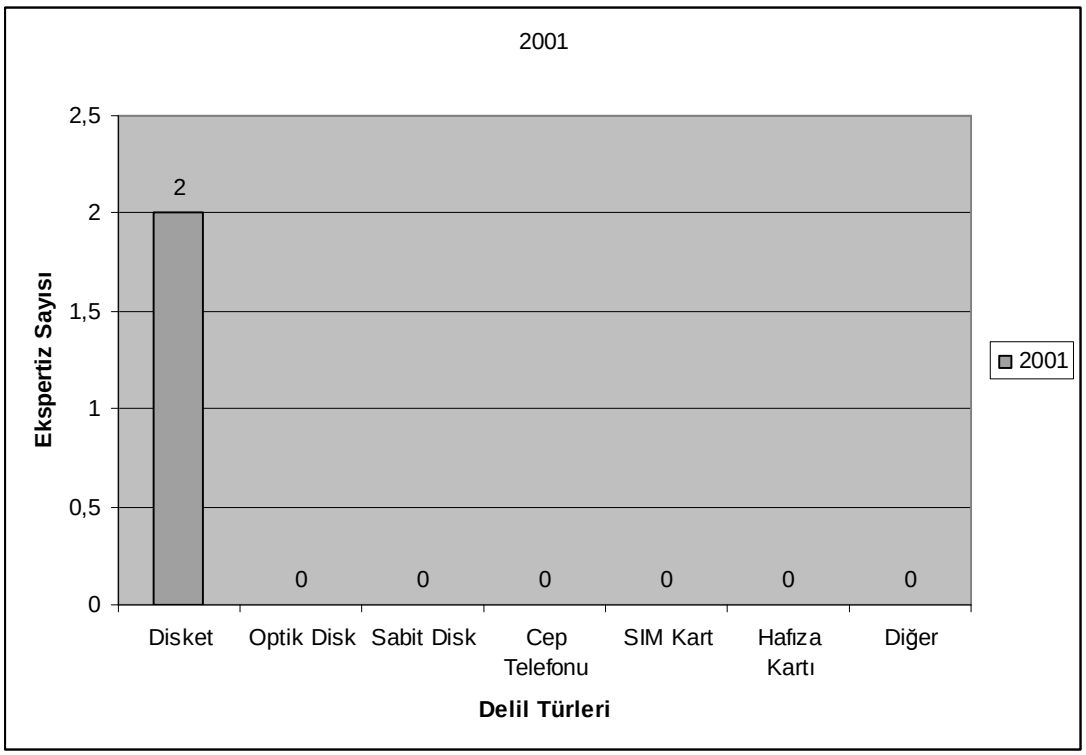
Adli işlemler neticesinde delil üzerinde herhangi bir değiştirilme yapılmamalıdır. Adli bilişim incelemeleri sırasında uygulanan yöntemlerin delili değiştirmediğini ispat etmek için "bütünlük algoritmaları" kullanılır. Bütünlük algoritmaları imaj alma işlemi sırasında uygulanabileceği gibi imaj alma işlemi sonrasında her dosya için tek tek uygulanabilir. Günümüzde sıkça kullanılan bütünlük algoritmaları: CRC, MD5 ve SHA-1'dır. Bu algoritmalar sonucu ortaya çıkan değerler imaj ile birlikte aynı dosya içerisinde saklanabilir veya ayrı bir dosya içerisinde toplanabilir. Algoritmalar sonucu ortaya çıkan değerlerin sonradan tekrar aynı algoritma ile hesaplanması sonucu ortaya çıkan değer ile ilk değerle karşılaştırılması sonucu delil üzerinde değişiklik yapılıp yapılmadığını anlaşılır.

# 3. BULGULAR

Türkiye'de adli bilişim laboratuvarı olarak hizmet vermekte olan ilk ve şuan tek laboratuvar olan Kriminal Polis Laboratuvarları, Data İnceleme bürosuna göre bilişim suçlarının niteliği ve muhteviyatı ile ilgili istatistiki bilgiler aşağıda sunulmuştur. İstatistiki veriler Data İnceleme Bürosuna 2001-2006 yılları arasında gelen ekspertiz işlerini kapsamaktadır.

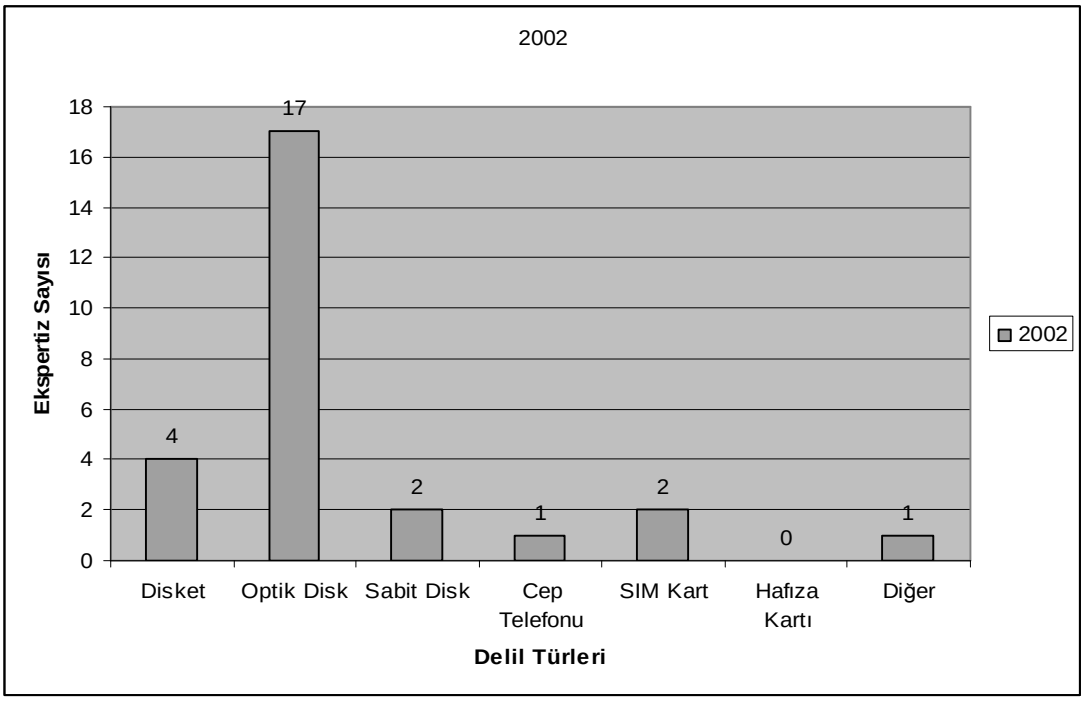
## Yıllara Ait İstatistikler

### 2001



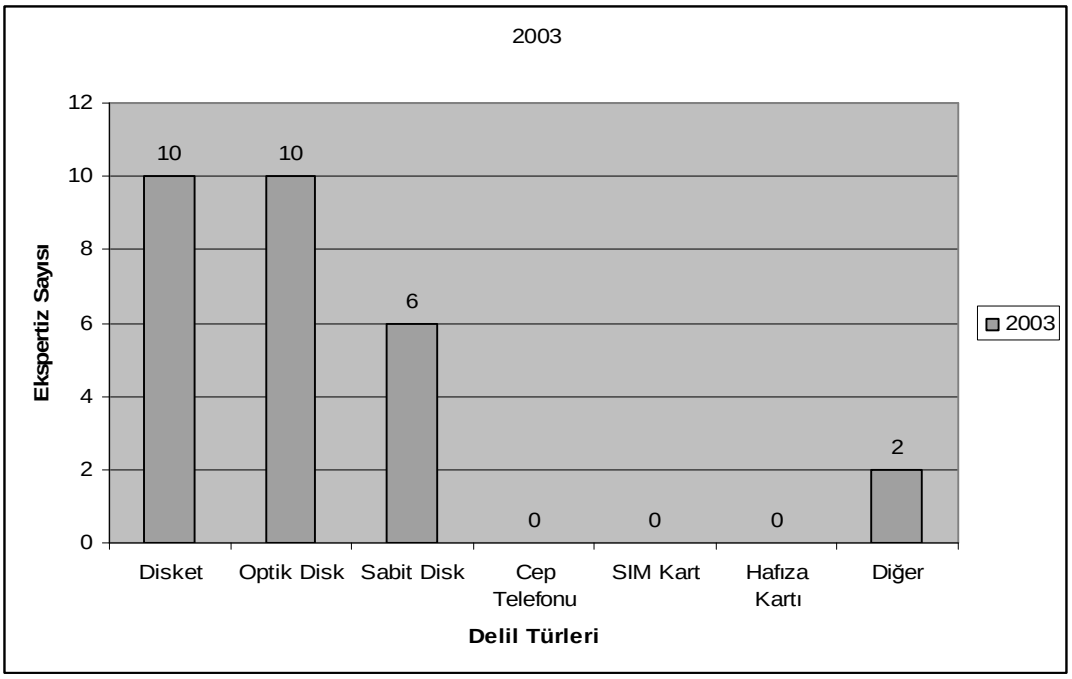

Çizelge-3.3: 2001 Yılına Ait Delil Türleri Grafiği

**2002**



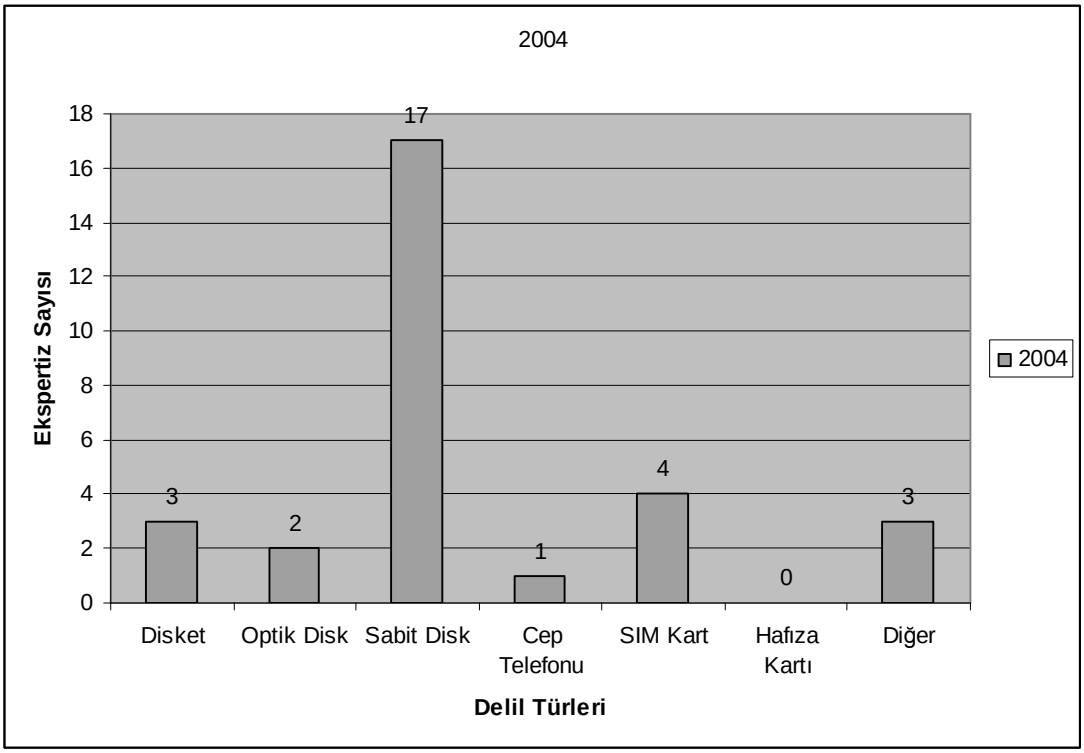

Çizelge-3.4: 2002 Yılına Ait Delil Türleri Grafiği

**2003**



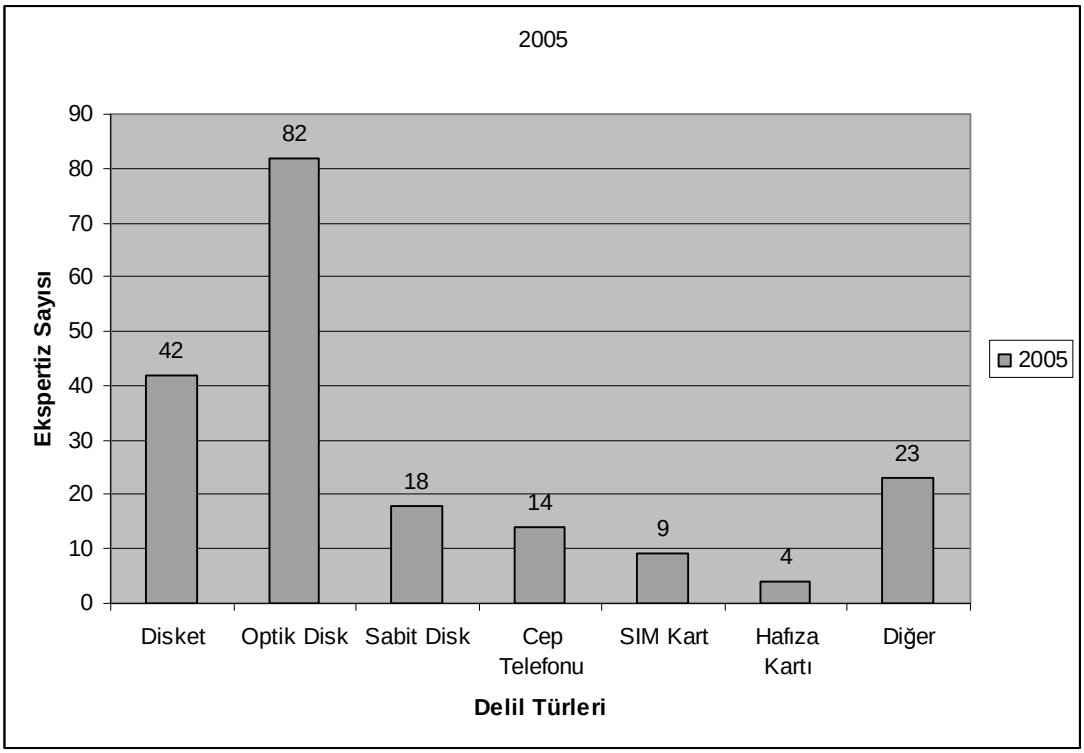

Çizelge-3.5: 2003 Yılına Ait Delil Türleri Grafiği

**2004**



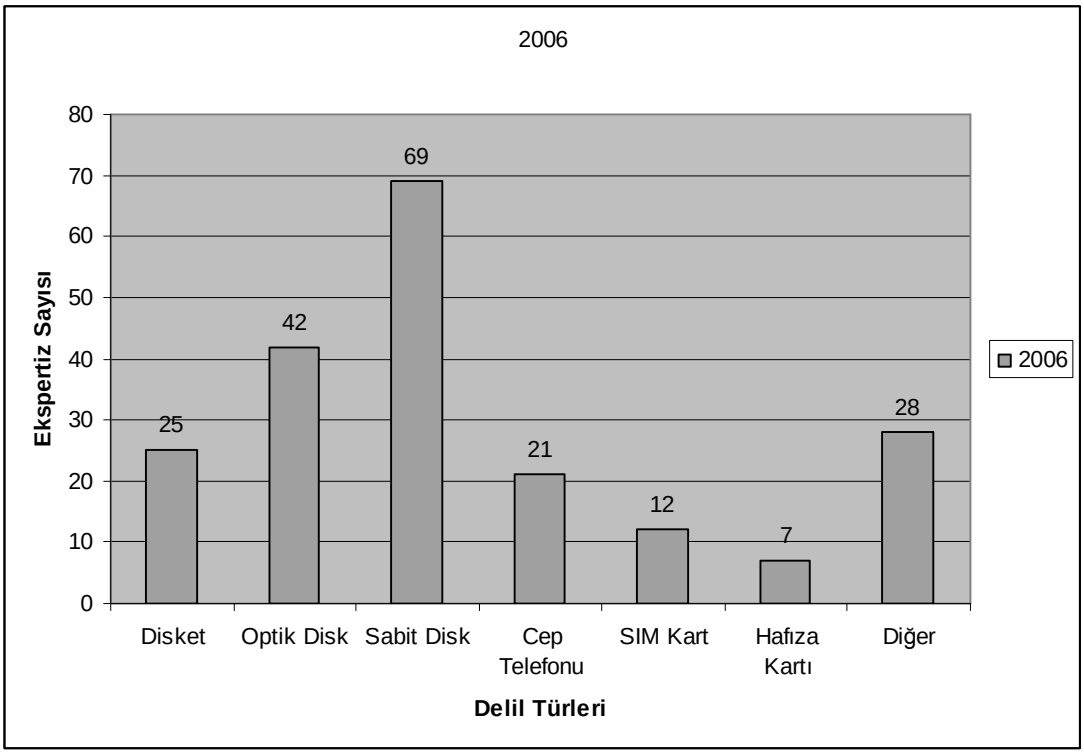

Çizelge-3.6: 2004 Yılına Ait Delil Türleri Grafiği

**2005**



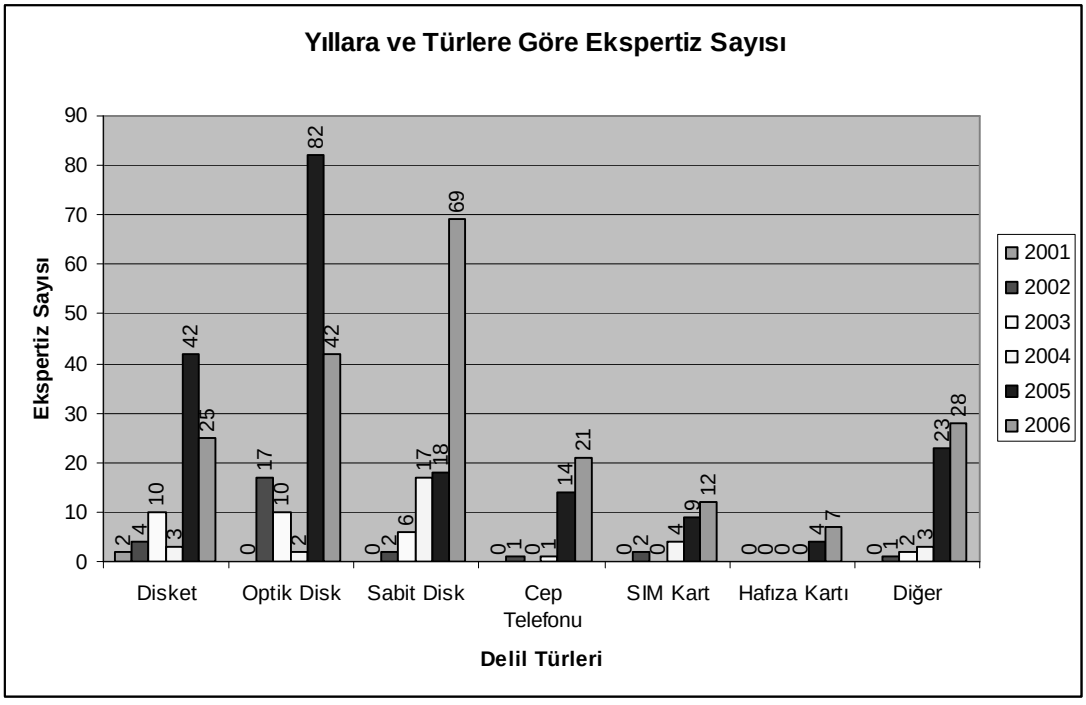

Çizelge-3.7: 2005 Yılına Ait Delil Türleri Grafiği

**2006**



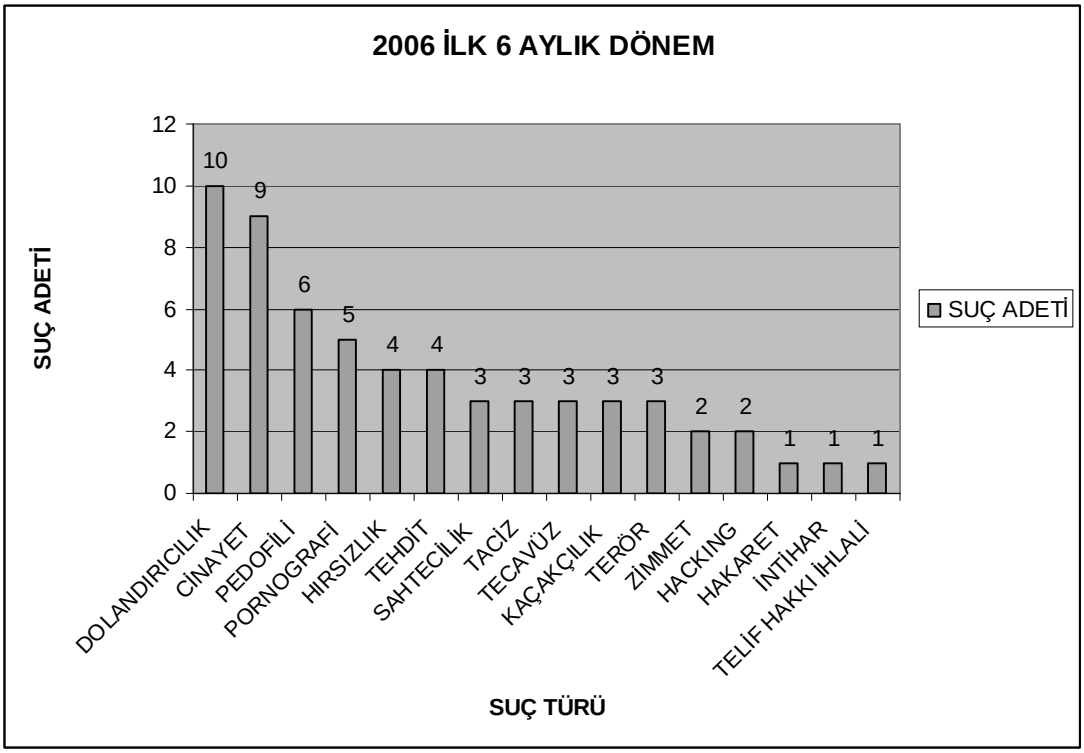

Çizelge-3.8: 2006 Yılına Ait Delil Türleri Grafiği

## 2001 – 2006 Yılları Arasında Delil Türlerine Göre Ekspertiz Sayısı




Çizelge-3.9: 2001 – 2006 Yıllarına ve Delil Türlerine Göre Ekspertiz Sayısı

Bilişim sistemleri kullanılarak işlenen suçlar çok geniş bir yelpazeye dağılmaktadır. Aşağıda Data İnceleme Laboratuvarına 2006 yılının ilk 6 aylık döneminde gelen ekspertiz işlerinin suç türlerine göre dağılımı görülmektedir.




Çizelge-3.10: 2006 İlk Altı Aylık Dönem Bilişim Suçu Türleri

Bilişim sistemleri kullanılarak yapılan dolandırıcılık 10 ekspertiz adediyle birinci suç türü olarak karşımıza çıkmaktadır. Bilişim sistemlerinin gelişmesi ve hayatın her alanında kullanılması İnternet dolandırcılığı, ATM dolandırcılığı gibi dolandırcılık türlerinin ortaya çıkmasına sebep olmuştur. Ülkemizde cep telefonu kullanım oranı yaklaşık olarak %60 civarındadır. Faili meçhul cinayetlerin maktüllerinin üzerinde genellikle cep telefonlarına rastlanmaktadır. Olay yerinden delil toplanması sırasında maktülün üzerinde bulunan cep telefonu delil değeri taşıdığı için laboratuvara gönderilmektedir.

**Örnek Olay Çalışması**

*A.C. isimli müşteki Cumhuriyet Savcılığına başvurarak, B Bankası, Ankara şubesinde kendi adına kayıtlı olan 1234567 no'lu hesabından, 03.09.2003 tarihinde, saat 12:23'de, İnternet üzerinden başka bir hesaba kendisinden habersiz olarak İzmir ili, K Bank, Merkez şubesi, M.N. ve P.R. adlı şahısların banka hesaplarına EFT işlemi yapıldığını bildirmiştir.*

*İzmir Emniyet Müdürlüğü ile irtibata geçilerek M.N. ve P.R. isimli şahısların adresi tespit edilmiş ve Emniyet Müdürlüğüne ifadeleri alınmak üzere davet edilmiştir. Aynı sıralarda K Bankasından, söz konusu hesapları açmak için kullanılan nüfus cüzdanlarının fotokopisi zapt edilmiştir. M.N. ve P.R. adlı şahısları ise yapılan mülakatta, hesapların kendilerine ait olmadığını iddia etmişlerdir.*

*K Bankası güvenlik görevlisinin verdiği ifade ve hesapların açıldığı tarih olan 10.12.2002 tarihinde banka güvenlik kamera kayıtlarının incelenmesi doğrultusunda söz konusu hesapların M.N. ve P.R. isimli şahıslar adına X.Y. adlı şüpheli tarafından açılmış olabileceği müşahede edilmiştir.*

*X.Y. isimli şahsın yürütülen tahkikatında Aydın ilinde ikamet ettiği anlaşılmıştır. Şüpheli şahsın ikametgah adresinde arama kararı çıkartılarak yapılan incelemede bir adet bilgisayara ulaşılmış ve el konularak incelenmek üzere Kriminal Polis Laboratuvarları, Data İnceleme Bürosuna sevk edilmiştir.*

**Örnek Olay Analizi**

A.C. isimli müşteki kendisinden habersiz olarak, İnternet aracılığıyla hesabından EFT (başka banka hesabına para transferi) yapıldığını iddia etmektedir. İlk olarak yapılması gerekli olan işlem, transferin hangi hesaba yapıldığını tespit etmek olmalıdır. Müştekinin verdiği şikayet dilekçesine göre söz konusu banka hesaplarının M.N. ve P.R. adlı şahısların B Bankasında bulunan hesaplar olduğu anlaşılmaktadır. Ancak sahte kimlik kullanılarak açılmış bu hesapların asıl suçlu tarafından hedef saptırmak amacıyla yapıldığı incelemelerden görülmüştür. B Bankası güvenlik görevlisi ve güvenlik kamera kayıtları incelendiği zaman, hesabın açıldığı tarihte başka bir kişi tarafından işlem yapıldığı anlaşılmıştır. Soruşturmalar yürütüldükçe X.Y. isimli şüpheliye ulaşılmıştır ve evinde yapılan aramalar sonucunda İnternet üzerinden işlem yapabilme kabiliyetine sahip olan bilgisayarına el konulmuştur.

İnternet üzerinden dolandırıcılığa benzeyen bu olayın delili olabilecek sadece bir adet bilgisayar kasası mühürlenerek Data İnceleme bürosuna ulaştırılmıştır.

Bilgisayar kasaları içerisinde bulunan sabit disk, işlemci, hafıza, anakart, BIOS gibi elektronik bileşenlerden sadece sabit disk içerisinde bulunan bilgiler adli amaçlı olarak kullanılabilir. Çünkü elektrik enerjisinin kesilmesi durumunda sadece manyetik olarak dizayn edilmiş olan sabit disk içerisindeki dijital veriler muhafaza olunur.

Şüpheli bilgisayar kasasının mühürü sökülerek içerisindeki sabit diski çıkarılır. Sabit diskin yapılan ilk görsel incelemesinde fiziksel olarak herhangi bir bozukluğunun olmadığı müşahede edilmiştir.

Adli bilişim inceleme prosedürlerine göre dijital delillerin kontamine olmaması adına yapılması gereken ilk işlem, delilin birebir (bit-by-bit) imajının alınması olmalıdır.

Uygun adli bilişim yazılım ve donanımları kullanılarak diskin imajı alınarak, asıl delil üzerinde daha başka bir işlem yapılmaz.

Şüpheli diskin adli bilişim donanımı olarak “Ultrakit” cihazı, yazılım olarak ise “Encase” kullanılarak birebir imajı alınır. Ultrakit cihazı yazma-koruma görevi görerek orijinal delilin değiştirilmemesini garanti eder. Encase yazılımı ise diskin tüm sektörlerini tarayarak birebir kopya alınmasını sağlar.

Şüpheli diskin teknik özellikleri adli bilişim uzmanı tarafından;

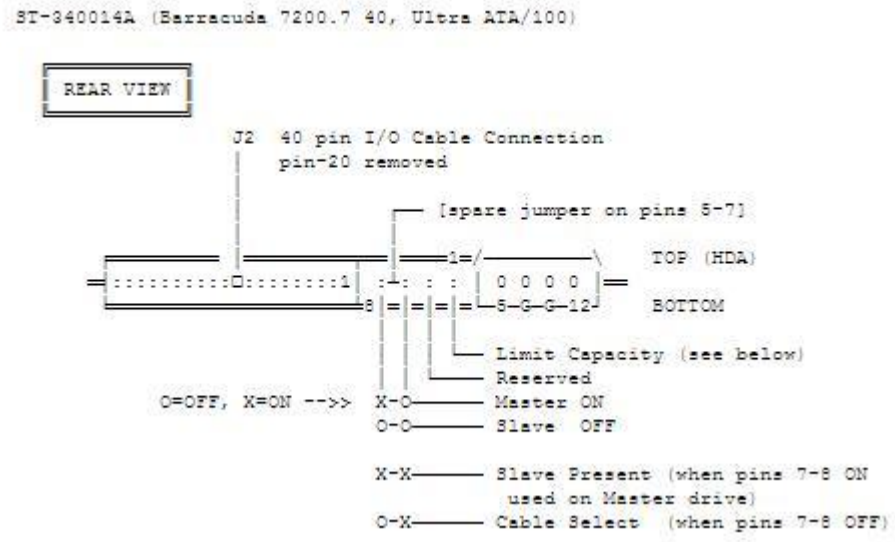
| **PARAMETRE** | **DEĞER** |
|---|---|
| **MARKA** | Seagate |
| **MODEL** | ST340014A |
| **SERİ NO** | XF703134 |
| **KAPASİTE** | 40 Gigabayt |
| **HIZ** | 7200 RPM |

| | |
|---|---|
| **SİLİNDİR** | 1023 |
| **KAFA** | 256 |
| **SEKTÖR** | 63 |
| **BAĞLANTI ARABİRİMİ** | IDE (Ultra ATA/100) |
| **ERİŞİM ZAMANI** | 8.5 milisaniye |
| **FAKTÖR** | 3,5” |

Çizelge-3.1: Seagate ST340014A Model Sabit Disk Spefikasyonları

olarak not edilmiştir.

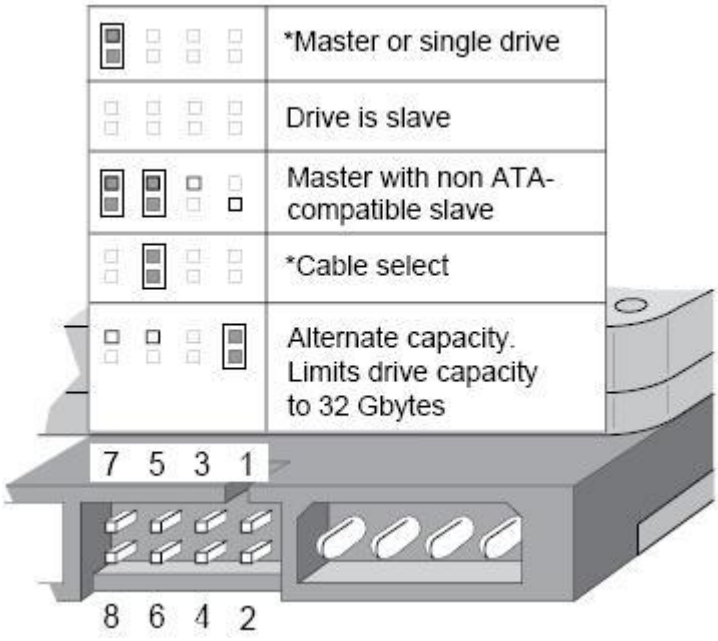
Sabit diskin İnternetten alına spefikasyonunda ise aşağıdaki bilgilere ulaşılmıştır.




Şekil-3.1: Seagate ST340014A Model Sabit Disk Bağlantı Şeması

Sabit disk incelemelerinde mutlaka disk “MASTER” konumunda iken imaj alınmalıdır. Çünkü bu konum “SLAVE” konumuna göre oldukça fazla zaman

tasarrufu sağlar. Örnekte 7. ve 8. pinlerin jumper ile birleştirilmesi sonucu "MASTER" konumuna geçilir.




Şekil-3.2: Seagate ST340014A Model Master / Slave Ayarı

Adli bilişim incelemeleri için İnternet vazgeçilmez bir unsurdur. İncelenecek olan delillerin İnternet üzerinde araştırılması adli bilişim uzmanına büyük kolaylıklar sağlar. Dijital delillerin yapısı, teknik özellikleri ve bağlantı cetvelleri uzmanın işini oldukça kolaylaştırır.

Şüpheli diskin imajının alınması sonucunda toplam 19,387,736,064 bayt (yaklaşık 18 GB) imaj dosyası açığa çıkmıştır. Bu imaj dosyası sabit disk üzerinde bulunan aktif, silinmiş dosyalardan ve imaj formatına ait diğer bilgilerden oluşmaktadır. Yani;

Aktif Dosyalar + Silinmiş Dosyalar + İmaj Bilgileri = İmaj

40 Gigabayt olduğu bilinen bir diskin yaklaşık olarak %50'si doludur. Tüm diskin imajının alınması, diskin hızı, bağlantı arabirimlerinin türü ve Encase yazılımına bağlı olarak 2 saat, 36 dakika, 8 saniye sürmüştür.

Adli bilişim sürecine göre imajı alınan disk muhafaza altına alınmış olunmaktadır. Artık uzmanın orijinal delil ile herhangi bir işi kalmamıştır. Sıradaki adım olayın müzekkeresi ile ilgili anahtar kelimelerin tespit edilip arama yapılmasıdır. Doğru anahtar kelimelerin seçilmesi uzmanın yetenek düzeyiyle ilgilidir. Anahtar kelimelerin belirlenmesinde olayın kovuşturulmasını yürüten savcının da katkısı olabilir. Müzekkerinin tekrar okunması suretiyle aşağıdaki anahtar kelimeler belirlenmiştir.

| **Anahtar Kelime** | **Seçilme Sebebi** |
|---|---|
| **A.C. [a.c.]** | Müştekinin adı |
| **1234567** | Banka hesap numarası |
| **B Bank [b bank]** | Müşteki hesabının bulunduğu banka ismi |
| **K Bank [k bank]** | Paraların transfer edildiği banka ismi |
| **M.N. [m.n.]** | İsmi kullanılan 1. şahıs |
| **P.R. [p.r.]** | İsmi kullanılan 2. şahıs |

Çizelge-3.2: Şüpheli Delil Üzerinde Aratılan Anahtar Kelimeler

Encase gelişmiş bir arama fonksiyonuna sahiptir. Yukarıdaki anahtar kelimeler ile bir anahtar listesi oluşturulup arama motoru çalıştırılır. Anahtar kelime araştırması adli bilişim incelemelerinin en önemli noktalarından biridir. Bu aşamada tüm deliller ortaya çıkabilir.

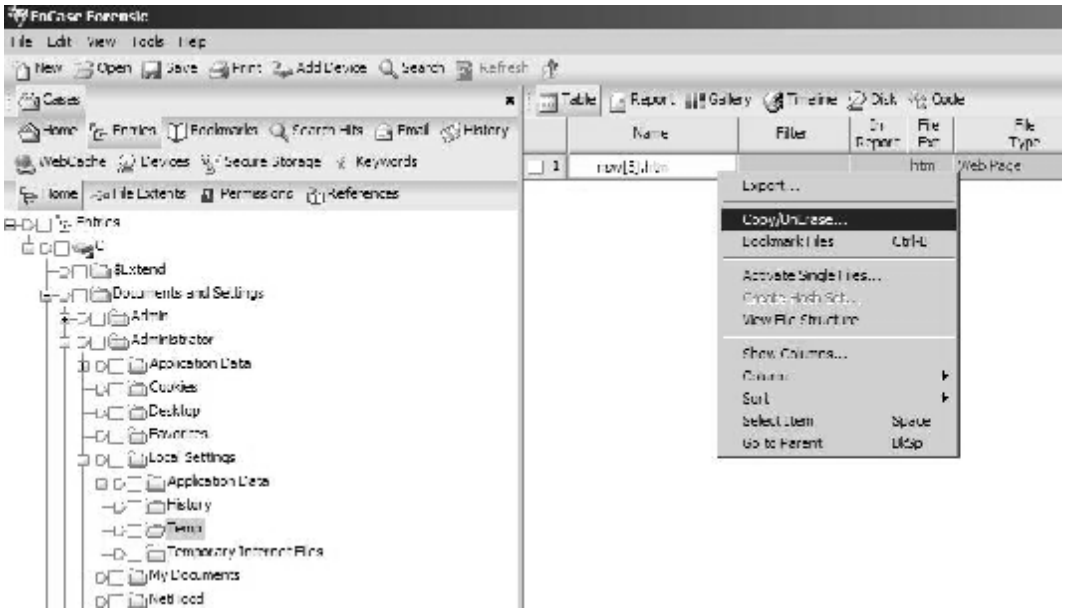
19,387,736,064 bayt boyutundaki veri içerisinde 6 adet anahtar kelimenin araştırılması imaj dosyasının kaydedildiği ortamın hızına göre 4 saat, 11 dakika, 34 saniye sürmüştür.

Arama işlemi bitince sonuçların incelenmesi safhasına geçilir. Yapılan incelemelerden sonra;

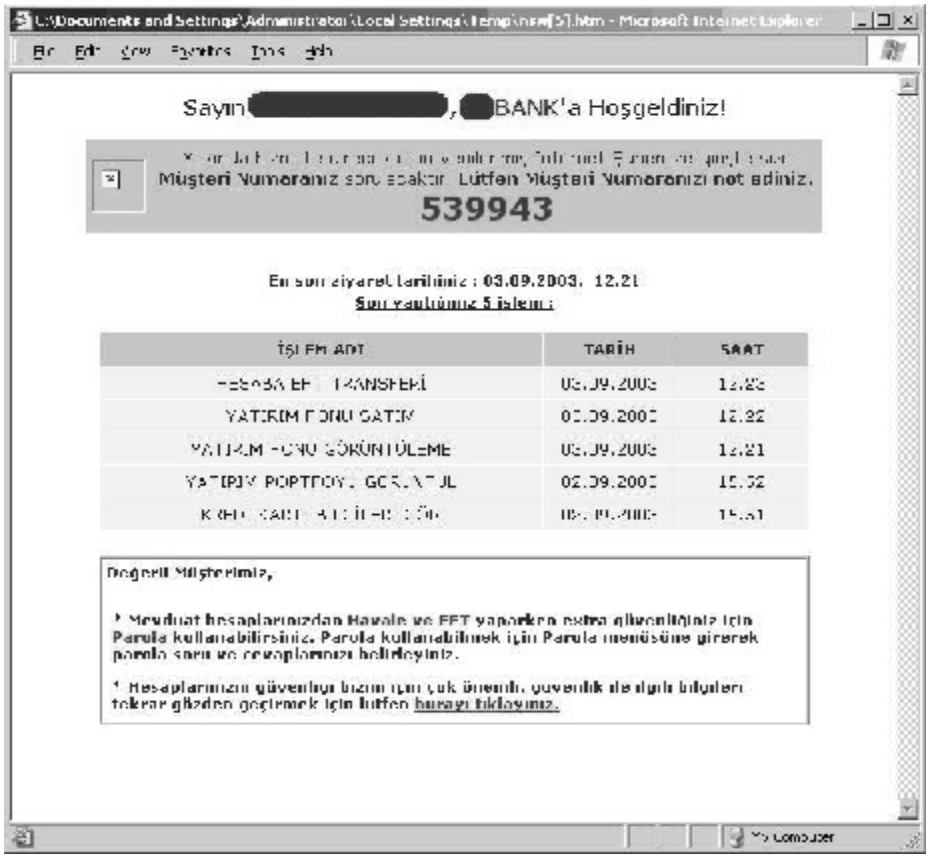
İpucu 1) Şüpheli sabit diskin

C:\Document and Settings\Administrator\Local Settings\Temp\nsw[5].htm

yolunda bulunan “nsw[5].htm” dosyasında anahtar kelimelerden “A.C.” kelimesine ulaşılmıştır. “nsw[5].htm” dosyası sabit diskin pasif alanında bulunmaktadır. Encase yazılımının veri kurtarma özelliği kullanılarak söz konusu dosya kurtarılmış ve aşağıdaki İnternet Web sayfasının olduğu görülmüştür.




Şekil-3.3: Ulaşılan Silinmiş Dosyanın Encase ile Kurtarılması




Şekil-3.4: Ulaşılan Dosyanın İçeriği

İpucu 2) Şüpheli sabit diskin

C:\Windows\Ntuser.dat dosyası içerisinde bulunan

\Registry\Default\Software\Microsoft\Internet Explorer\Explorer Bars\ {C4EE31F3-4768-11D2-BE5C-00A0C9A83DA1}\FilesNamedMRU\000

kayıt girdisinin değerinin “A.C.” olduğu anlaşılmıştır. Söz konusu kayıt girdisi (registry) tetkik konusu sabit disk üzerinde “A.C.” kelimesinin daha önce kullanıcı tarafından arattırılmış olduğu anlamına gelmektedir.

İpucu 1 ve İpucu 2 maddelerinden anlaşılmaktadır ki şüheli X.Y., müşteki A.C. şahsının adını bilmektedir. A.C. şahsının şikayetçi olduğunu düşünerek,

A.C. hesabından M.N. ve P.R. şahıslarının hesaplarına yapılan para transferinin kayıtlarının X.Y.'nin bilgisayarında neden bulunduğu sorusu şüpeheliye yöneltilebilir. Bu sorunun cevabı aynı zamanda olayın da çözümüdür.

Ulaşılan bilgiler ışığında yukarıdaki örnek olay ait ekspertiz raporu aşağıdaki gibi düzenlenmiştir.

*Ankara Kriminal Polis Laboratuvarı*

ANKARA

**Uzmanlık Numarası :** DATA-2003 / 000

**Ekspertizi Veren Yer :** Ankara Emniyet Müdürlüğü
**(Yazı gün ve sayısı) :** 05/09/2003 B.05.1.EGM.x.xx.xx.xx

**Ekspertiz :** Sabit Disk Tetkiki

**Ekspere Verilen Eşya :** Tetkik konusu,
Seagate marka, ST340014A model, XF703134 seri no'lu, 40 GB kapasiteli, 1 (bir) adet sabit disk.

**R A P O R**

Sorulan hususlar doğrultusunda gerekli incelemeler yapılmış, müşahede ve tespitlerimiz ile hasıl olan kanaatimiz aşağıda belirtilmiştir.

Tetkik konusu bulguların doğruluğu kontrol edilerek fiziksel incelemeye alınmış ve müzekkerede belirtilen tetkik konusu sabit disk olduğu anlaşılmıştır.

Fiziki inceleme ve tespit işlemlerini müteakiben imaj kopya alma işleminin yapılması amacıyla; X.Y.'den alındığı belirtilen, XF703134 seri no'lu sabit disk yazma-koruma sistemi vasıtasıyla adli delil inceleme istasyonuna bağlanmıştır. Söz konusu diskin Encase versiyon 5.03 ile imajı alınmıştır.

İlk aşamada bulgular üzerinde ön inceleme yapılmış ve aşağıdaki sonuçlar elde edilmiştir.

1- X.Y.'den el konulan seri numarası XF703134 olan sabit disk üzerinde yürütülen incelemelerde; üzerinde çift işletim sistemi (dual boot) bulunduğu anlaşılmıştır. Ayrıca diskin iki bölüme (partition) ayrıldığı ve her bölüme bir işletim sisteminin yüklenmiş olduğu görülmüştür. Yapılan ön incelemede disk üzerinde bulunan işletim sistemlerine ilişkin olarak tespit edilen bilgiler aşağıdaki tablolarda gösterilmiştir.

| **1. İşletim Sistemine Ait Bilgiler** | | |
|---|---|---|
| İşletim Sistemi | Microsoft Windows XP | |
| Ürün Seri Numarası | 55274-649-3885121-XXX | |
| Kayıtlı Sahip | X.Y. | |
| Kayıtlı Kurum | (Bilgi girilmemiş) | |
| Etki Alanı | WORKGROUP | |
| Bilgisayar İsmi | Bilgisayar | |
| Bilgisayarın en son kapatılma tarih ve zamanı | 05.09.2003 03:45:15 | |
| Bilgisayara Bağlı Yazıcılar | HP OfficeJet R60 | |
| Bilgisayara Bağlı Network Kartları | HP NetServer 10/100TX PCI LAN | |
| IP Adresi | 85.137.90.24 | |
| **Kullanıcı Bilgileri** | | |
| **UID** | **Kullanıcı İsmi** | **Profile dizini** |
| 500 | Administrator * | |
| 501 | Guest * | |
| 1000 | HelpAssistant * | |
| 1003 | X.Y. | C:\Documents and Settings\X.Y. |

* Sistem tarafından oluşturulmuş kullanıcı isimleri

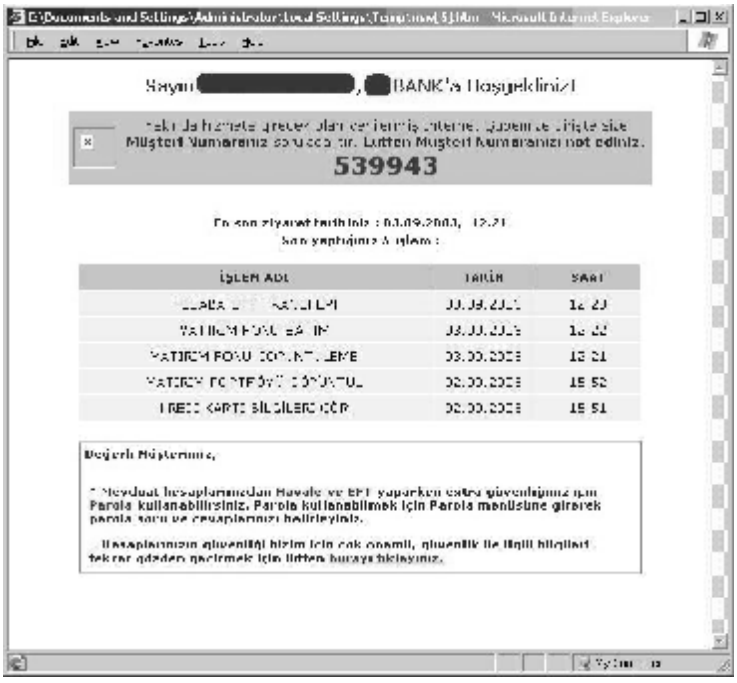
| **2. İşletim Sistemine Ait Bilgiler** | |
|---|---|
| İşletim Sistemi | Microsoft Windows ME |
| Bilgisayar İsmi | X.Y. |
| Bilgisayara Bağlı Yazıcılar | 1. HP OfficeJet R Serisi<br>2. Panasonic KX-P1150 |
| Kullanıcı İsmi | X.Y. |

Ön inceleme işleminden sonra fezleke okunarak soruşturma ile ilgili anahtar kelimeler çıkarılmıştır. Çıkarılan anahtar kelimeler sınıflandırılarak delil inceleme programına girilmiştir. Girilen anahtar kelimeler aşağıdadır:

| Kategori | Tipi | Anahtar Kelimeler | Tanımlama |
|---|---|---|---|
| **Kullanıcı ismi** | | A.C. | |
| | | [a.c.] | |
| **Hesap No** | | 1234567 | |
| **Banka** | Grep | a?bank | abank, |
| | Grep | a?kredi | abank, |
| | Grep | b?bank | bbank, |
| **Yer** | | van | |
| | Grep | [İi]zm[iİ]r | izmir, İzmir, İZMİR |
| | Grep | ankara | ankara |
| **İsimler** | Grep | M.N. | |
| | Grep | P.R. | |

Girilen tüm anahtar kelimeler, imajı sabit disk içerisinde aratılmıştır. Arama sonucunda bulunan veriler incelenmiş ve aşağıdaki sonuçlar çıkartılmıştır.

1- A.C. ve [a.c.] anahtar kelimelerinin X.Y.'nin sabit diskinin X.Y. kullanıcısına ait *geçici internet dosyaları*[35] *arasında* geçtiği görülmüştür. Bulunan söz konusu dosya incelendiğinde Abank'ın internet sitesinde A.C.'ya ait alana 03.09.2002 tarihinde X.Y. kullanıcısı tarafından kullanıcı adı ve şifresi kullanılarak girildiği anlaşılmıştır. Tespit edilen dosyanın ekran görüntüsü aşağıdadır.




[35] Bilgisayardan İnternette herhangi bir sayfaya girildiğinde o sayfanın bir kopyasını tutan ve daha sonra aynı web sayfasına bağlanılmak istendiğinde kolay bağlantı yapılması için önceki bağlantıya ait olan dosyaların kullanılabilmesini sağlamak amacıyla İnternette bağlanılan web sayfalarına ait bilgilerin tutulduğu "C:\Documents and Settings*kullanıcı ismi*\Local Settings\Temporary Internet Files" dizinidir. Bu dizindeki dosyalar daha önce o bilgisayar ve o kullanıcı tarafından internetteki o sayfaya bağlanılmış olduğunu gösterir.

2- X.Y.'nin sabit diskinde C:\Windows\Ntuser.dat dosyası içerisinde bulunan \Registry\Default\Software\Microsoft\Internet Explorer\Explorer Bars\ {C4EE31F3-4768-11D2-BE5C-00A0C9A83DA1}\FilesNamedMRU\000 içerisindeki registry[36] bilgisinde "A.C." kelimelerinin bulunduğu tespit edilmiştir. Söz konusu registry kaydı, tetkik konusu bilgisayar üzerinde bu kelimelerin daha önce kullanıcı tarafından arattırılmış olduğu anlamına gelmektedir.

Bu bilgiler haricinde anahtar kelimelerle eşleşen olay ile ilgili herhangi bir bilgiye rastlanmamıştır.

Arama işlemi sonuçlarının incelenmesinin ardından, Abank'taki A.C.'nın hesabına nasıl girilmiş olduğunun araştırılması amacıyla bütün bulgular üzerinde detaylı inceleme yapılmıştır. İnceleme esnasında X.Y.'nin evinde bulunan bilgisayarda bir çok şifre kırma, şifre çalma vb. amaç için kullanılan "trojan" olarak tabir edilen programlar bulunduğu ve bu programlarla elde edilmiş bir çok kullanıcı ismi ve şifre ile çok sayıda kişinin bilgisayarından alınmış klavye kayıtlarına rastlanmıştır.

**SONUÇ:**

X.Y.'nin evinde bulunan XF703134 seri numaralı sabit diskindeki X.Y. adlı kullanıcı tarafından A.C.'nin Abank'taki hesabına 03.09.2002 tarihinde kullanıcı hesabı ve şifre girilerek bağlanılmış olduğu tespit edilmiştir.

Bununla birlikte "A.C." isminin, tetkik konusu bilgisayar içerisinde bilgisayarın kullanıcısı tarafından arama işlemine tabi tutulduğu anlaşılmıştır.

[36] Registry; Windows işletim sistemlerinde sisteme ait tüm bilgilerin tutulduğu bir veri bankasıdır.

# 4. TARTIŞMA

Bu çalışma bilişim suçlarının, Türkiye'deki boyutu üzerinde yapılmıştır. Bir suçun aydınlatılmasında iki temel safha olan "olay yeri incelemesi" ve "laboratuvar incelemesi"nin, bilişim suçlarının vuku bulduğu vakalarda nasıl yürütülmesi gerektiği üzerinde durulmuştur. Konu hakkında yurt dışı kaynaklı birçok yayının olması sebebiyle öncelikle yurt dışı literatür taraması yöntemine başvurularak durum tespiti yapılmıştır. Söz konusu literatür taraması İnternet üzerinden ve konuyla ilgili çıkan süreli yayınlar üzerinden gerçekleştirilmiştir. Yapılan incelemelerde, A.B.D., İngiltere ve Almanya gibi gelişmiş ülkelerde konu hakkında müeyyideler getiren bir çok kanunun olduğu anlaşılmıştır. Ülkemiz kanunları ile karşılaştırıldığında ise ülkemiz ceza yasalarının ve olay yeri inceleme yönetmeliğinin yetersiz kaldığı görülmüştür. Söz konusu kanun maddeleri çalışma içerisinde belirtilerek yetersiz olduğu düşünülen yerler gösterilmiştir.

Çalışmada ayrıca bilişim suçlarının vuku bulduğu olay yerlerinde delil toplamak ile görevli olay yeri inceleme uzmanlarının genellikle karşılaştığı durumlar ve olay yeri incelemesinde sık yapılan yanlışlar SASEM'de (Suç Araştırma ve Soruşturması Eğitim Merkezi) yapılan birebir mülakatlar ile tespit edilmiştir. Yapılan mülakatlarda saha personelinin, bilişim delillerini toplamakta ve paketlemekte eksik olan yönlerinin olduğu anlaşılmıştır. Bu bağlamda bilişim suçlarının vuku bulduğu olay yerlerinde söz konusu delillerin nasıl toplanması ve paketlenmesi gerektiği konusu üzerinde durulmuştur.

Laboratuvar incelemeleri, Adli Bilimler'in vazgeçilmez bir unsurudur. Tezde ayrıca, ülkemizde, 2002 yılında kurulmasına başlanılan, fakat günümüzde henüz resmi olarak ekspertiz işi kabul etmeyen Kriminal Data İncelemeler Bürosunun çalışma yöntemlerinden bahsedilmiştir. Almanya Federal Kriminal Dairesi (BKA), Data İncelemeler Bürosu baz alınarak yapılan karşılaştırmalarda, ülkemiz laboratuvarının teçhizat ve personel yönlerinden yetersiz olduğu müşahede edilmiştir. Avrupa Birliği, Twinning (Eşleştirme) projesi kapmasında iki ülke laboratuvarlarının akredite edilmesi konusunda yapılan çalışmalar incelenmiştir. Yapılan incelemeler neticesinde, elektronik ve dijital delillere laboratuvarda uygulanması gereken adli prosedürler çıkarılarak, açıklanmaya çalışılmıştır.

Suç işleme içgüdüsü insanın doğasında vardır. Suçlu insanlar, tarih boyunca amaçlarına ulaşabilmek için yasal olmayan türlü yollara başvurmuşlardır. Suç işlemek amacıyla kullanılan her türlü alet ve yöntem, arkasında mutlaka bir iz bırakmıştır. (Locard prensibi: Her temas iz bırakır.) Suçluların arkalarında bıraktıkları izleri araştırmak, Adli Bilimler'in çalışma alanına girer. Tarih boyunca suç işlemek amacıyla kullanılan alet ve yöntemler arttıkça, Adli Bilimler'in çalışma alanı da genişlemektedir.

Yaşadığımız çağa adını veren bilişim teknolojileri hayatımıza her an biraz daha nüfuz etmeye devam etmektedir. Normal bir insanın hayatını oldukça kolaylaştıran teknolojik gelişmeler, bir suçlunun suç işlemesini de kolaylaştırmaktadır. Suç oluşumunu engellemek için teknolojiyi yasaklamak, normal insanların haklarını ellerinden almamak adına, haksızlıktır. Bilişim teknolojileri kullanılarak işlenen suçların sayısının gün geçtikçe arttığı aşikardır. Bu nedenle, bilişim suçlarının işlenmeden önce önlenmesi ve

işlendikten sonra faillerinin bulunması, bir hukuk devletinin sorumluluğu altında olmalıdır.

Ülkemiz bir hukuk devletidir ve konusu suç olan eylemler kesinlikle cezalandırılmalıdır. Bilişim suçları, hukuk literatürü için yeni bir kavramdır. Ancak söz konusu suçların, bilişim teknolojisinin hayatımıza girme hızı yönüyle, ileride oluşacak suç oranları arasında daha fazla öneme sahip olacağı açıktır.

Modern hukuk sistemlerinde, bir suçu açığa çıkarmak için delillendirme konusu büyük öneme sahiptir. Adaletin sağlanması amacıyla hukuki meselelerde hata yapılmaması önem arz etmektedir. Bilişim suçlarında ceza kanaatine kavuşmak amacıyla, diğer Adli Bilimler disiplinlerinde olduğu gibi maddi delillere göre hareket etme ihtiyacı ortaya çıkmıştır. Adli Bilişim ile uğraşanlar, bu ihtiyacı karşılama amacında olmalıdırlar.

Adli Bilişim, ülkemizde olduğu gibi dünya ülkelerinde de yeni bir bilim dalı olması sebebiyle, disiplini oluşturan kuram, yöntem ve standartların belirlenmesi gerekmektedir. Hiçbir sözlü kural yazılı kurallar kadar geçerli olamaz.

Adaletin yerini bulmasında önemli bir görev yargı birimleri kadar kolluk kuvvetlerine de düşmektedir. Adalet sisteminin ön gücü sayılan kolluk kuvvetleri, suçun işlenilmeden önce önlenmesinin yanında, işlenildikten sonra faillerinin bulunması konusunda da çalışmak zorundadırlar. Bu görevlerin hassasiyeti yapılan işin ehemmiyetini artırmaktadır.

Ülkemizde, kolluk kuvvetlerimizin çalışma alanına giren olay yeri incelemesi, her suçun açığa kavuşturulması açısından önemli hassasiyetlere sahiptir. Olay yeri incelemesi yürütülürken yapılabilecek en ufak bir hata geri dönülemez sonuçlara neden olabilir. Bilişim suçlarının ardında bırakılan iz ve delillere, bu konuda yeterince bilgisi olmayan kişiler tarafından müdahale edilirse, delillerin karartılması, hatta yok edilmesi son derece olasıdır.

Bilişim suçlarının işlenilmesinin ardından olay yerinde bulunabilecek elektronik deliller, olay yeri inceleme ekiplerinin karşılaştığı yeni delil türleridir. Elektronik deliller, diğer delil türlerine benzer, ortak özelliklerinin yanında, farklı bir takım özelliklere de sahiptirler. Elektronik delillerin sahip oldukları farklı özelliklerin, olay yeri inceleme ekipleri tarafından bilinmesi ve bu doğrultuda araştırmaların yürütülmesi hayati öneme sahiptir. Bu noktada olay yeri inceleme ekiplerinin bilişim suçları vakalarında delil toplanması konusunda eğitilmeleri önem arz etmektedir. Her an gelişen teknoloji sonucu ortaya çıkan değişimleri anlamanın tek yolu eğitimden geçmektedir. Ülkemiz olay yeri inceleme uzmanlarının yetiştirildiği merkez olan Kriminal Polis Laboratuvarları Dairesi Başkanlığı, Suç Araştırma ve Soruşturması Eğitim Merkezi'ne (SASEM) bu konuda önemli görevler düşmektedir. Adli Bilişim'in ülkemizde temellerinin doğru olarak atılabilmesi ve ileride yetiştirilecek uzmanların işlerini doğru yapmaları için eğitime önem verilmelidir. Konusunda zaten uzman olan olay yeri inceleme ekipleri için ise düzenlenecek hizmet içi eğitimler ile Adli Bilişim konusunun doğru olarak anlaşılması sağlanmalıdır.

Ülkemizde, kanunlar ile olay yerlerinden delil toplama ve inceleme görevi Emniyet Genel Müdürlüğü, Kriminal Polis Laboratuvarları Dairesi Başkanlığı'na verilmiştir. Bilişim suçlarında olay yeri inceleme ekipleri tarafından elde edilen ve laboratuvara gönderilen delillerin incelemeleri ise KPL'nin Data İncelemeler Bürosu tarafından yürütülmektedir. Adli Bilişim laboratuvar incelemeleri olarak tanımlayabileceğimiz bu tür incelemeler yüksek bilişim bilgisini gerektirmektedir. Çünkü incelenen deliller yüksek teknoloji ürünleridir ve sayısal alandaki bilgilerin tam olarak uygulamalı kullanılmasını gerektirmektedir. Bu nedenle Data İncelemeler Bürosu'nda görevli uzmanlar ileri sayısal muhakeme yeteneğine sahip ve fen bilimlerine ilgi duyan kişiler olması tercih edilmelidir.

Data incelemeler laboratuvarında, elektronik delillere uygulanan prosedürler kayıt altına alınmalıdır. Eğer uygulanan prosedürler kayıt altına alınmaz ise delillerin mahkemelerde maddi geçerliliğinin bozulması riski ortaya çıkabilir. Ayrıca tutulan bu kayıtlar, elektronik delillerin laboratuvara nasıl ulaştırılması gerektiği konusunda da bilgi verir. Olay yerlerinde karşılaşılan elektrikli veya elektronik her bulgu, delil olarak ele alınmamalıdır. Olay yerinde bulunan bir elektronik kantardan bilgi elde etmek data incelemeler laboratuvarı için mümkün görünmemektedir. Bu nedenle laboratuvara gönderilen deliller konusunda daha dikkatli olunmalıdır.

Suç Araştırma ve Soruşturması Eğitim Merkezi'nde olay yeri inceleme ekiplerine verilecek eğitimlerin müfredatı, konu hakkında yeterli bilgi ve tecrübeye sahip olan Data İncelemeler Bürosu uzmanları tarafından düzenlenebilir ve konu hakkında gerekli belge ve dokümanlar bu büronun uzmanları tarafından hazırlanabilir.

Adli Bilişim disiplinine has araştırma yöntemleri bilişim teknolojilerindeki gelişmelerin gidişatına göre şekillenmektedir. Bilişim teknolojisinde gerçekleşen değişimler ve yenilikler disiplini doğrudan etkilemektedir. Bu nedenle konunun muhatabı olan kimselerin kati surette bilişim teknolojisini alenen takip etmeleri gerekmektedir. Teknolojideki son gelişmeleri anlık takip etmenin en kolay yolu İnternet'tir. Dünya çapında bir ağ olması sebebiyle, İnternet, her an, herkes tarafından kullanıma açıktır.

Tezde, geleneksel delil türlerine ek olarak, olay yerlerinde yeni ortaya çıkmaya başlayan elektronik delillerden bahsedilmiştir. Elektronik delillerin, diğer delillerle ortak ve farklı özellikleri vardır. Bu nedenle bu tür delillere müdahale edilirken uygulanması gereken yöntemler açıklanmıştır. Yöntemler açıklanırken, Emniyet Genel Müdürlüğü, Olay Yeri İnceleme uzmanlarının delillere yaklaşım tarzları ve çalışma şartları göz önünde bulundurulmuştur.

Adli Bilişim laboratuvar çalışmaları, olay yerinde el konulan elektronik delillerin, laboratuvara ulaştırılarak, dijital delile dönüştürülmesi çalışmalarını ve dijital deliller üzerinde inceleme yapma safhasını kapsamaktadır. Konu esas itibarıyla tezin özünü oluşturmaktadır. Adli bilimlerin ortak paydası olan laboratuvar incelemeleri, Adli Bilişim disiplinin de çekirdeğini oluşturmaktadır. Bilişim teknolojisinin ürünü olan birçok araç ve yöntem, Adli Bilişim'in de çalışma şartlarını kolaylaştırmaktadır.

Tezin dördüncü bölümünde bahsedilen laboratuvar çalışmalarında, diğer dünya ülkelerinin data inceleme laboratuvarlarında sık kullanılan dd yazılımdan bahsedilmiş ve nasıl kullanıldığı açıklanmıştır. Olay yeri inceleme

ekipleri tarafından da oldukça fazla kullanılan bir yazılım olan dd, elektronik delillerden dijital delil elde etmeyi gösteren güzel bir örnek olmuştur. Ancak yazılım fazla sayıda özelliğe sahiptir. dd'nin tüm özelliklerini göstermek yerine, olay yeri inceleme ekipleri tarafından sıklıkla kullanılabilecek özelliklerinden bahsedilmiştir.

Adli dijital imaj oluşturma işlemimin diğer bir ayağı yazılımsal ve donanımsal yazma koruması kullanmaktır. Tezde yazılımsal yazma korumalarında bahsedilmiş ve kullanılmasının sakıncaları açıklanmıştır. Donanımsal yazma korumalarının ise çalışma sisteminden bahsedilmiştir ve piyasada sık kullanılan donanımsal yazma korumaları ile ilgili İnternet siteleri konusunda bilgi verilmiştir.

# 5. SONUÇ VE ÖNERİLER

“Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi” adlı bu tez, iki ana konuyu araştırmayı hedeflemiştir: Bilişim suçlarında elde edilen delillerin olay yerinde toplanması ve dijital delillerin data incelemeler laboratuvarında incelenmesi. Diğer dünya ülkelerinde olduğu gibi ülkemizde de yeni araştırılmaya başlanılan bir konu olan “Adli Bilişim” disiplini, Disiplinlerarası Adli Bilimler çatısı altında, diğer adli bilimler disiplinleri gibi araştırılmaya uygun görünmektedir. Kendisine ait metodoloji ve kavramların oluşturulmasıyla beraber, adalet sistemi içindeki yerini alması kaçınılmazdır. Adaletin tam olarak sağlanması amacıyla tüm bilim dallarının seferber edilmesi gerektiği açıktır. Bu nedenle Adli Bilişim’in de bir an evvel belirli kurallar dahilince çalışma yöntem, araç ve gereçlerinin ortaya konulması gerekliliği yapılan çalışmadan anlaşılmaktadır.

Adli Bilişim, kuram ve uygulamaları dünyada yeni oluşturulmaya başlanmış bir bilimdir ve konu hakkında yapılan her çalışma bu alanı aydınlatmaya yöneliktir. Bu nedenle ülkemizde konu hakkında yapılan akademik ve laboratuvar çalışmaları çeşitlendirilerek ve derinleştirilerek sürdürülmelidir.

Adli bilişim alanında yapılan laboratuvar çalışmaları, klasik suç türleri olan dolandırıcılık, sahtecilik ve zimmet gibi suçların daha fazla bilişim sistemleri kullanılarak işlendiğini göstermiştir. İstatistiki verilere bakıldığı zaman, dolandırıcılık, cinayet ve pedofili gibi suçlarda bilişim sistemleri kullanıldığı görülmektedir. Pedofili suçu son yıllarda ülkemiz hukuk literatürüne girmeye başlamıştır. Gün geçtikçe pedofili konusunun önemi toplum tarafından anlaşılmaktadır. Pedofili suçunu engellemek için gerekli tedbirler alınmalı ve bu konuda hakkında yapılan akademik çalışmalar arttırılmalıdır.

# ÖZET

## Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi

Bu araştırmanın genel amacı; bilişim suçlarının vuku bulduğu olay yerlerinden elde edilen delillerin toplanması, elde edilen delillerin data inceleme labouratuvarına sevki ve laboratuvarda incelenmesi konusunda bir yaklaşım yolu göstermek ve saha personeli tarafından sık yapılan yanlış davranışları düzeltmektir.

Bilişim suçları, suç türleri arasına yeni katılmış olan bir kavramdır. İşlenmesinde yüksek teknoloji ürünleri olan bilişim sistemlerinin kullanılıyor olması, bu tür suçların önlenmesini ve faillerinin bulunmasını zorlaştırmaktadır. Ancak teknolojik aletlerin hayatımıza her gün bir adım daha girmesi, bu konu hakkında yapılması gereken çalışmaların gerekliliğini ispatlamaktadır.

Araştırmada, öncelikle suç kavramı genel olarak ilk bölümde tanımlanmış, konunun uzmanı olan yerli ve yabancı kriminolog ve sosyologların tanımlarına yer verilmiştir. Birinci bölümde ayrıca, bilişim suçlarının tanımı ve tanımlamayı yaparken dikkat edilmesi gereken hususlar anlatılmıştır.

Bilişim suçunun vuku bulduğu yer olan olay yerinde, olay yeri inceleme uzmanın delillere müdahale etme konusunda dikkat etmesi gereken noktalar ikinci bölümde anlatılmaya çalışılmıştır.

Elektronik delillerden, dijital deliller elde edilmesi ve dijital delillerin nihai olarak incelendiği yer olan data inceleme laboratuvarında, delillerin bütünlüğünün bozulmaması ve karartılmaması için alınması gereken önlemler ve inceleme yürütülmesi teknikleri üçüncü bölümde anlatılmaya çalışılmıştır. Ayrıca bu bölümde, yürütülen incelemenin sonuçlarının gerekli mercilere iletilmesi amacıyla Adli Bilişim ekspertiz raporu yazma konusu açıklanmıştır.

**Anahtar Sözcükler:** Adli bilişim, bilişim suçu, dijital delil, olay yeri, hukuk.

# SUMMARY

## Evidence Collection and Examination in IT Crimes

The main aim of this thesis is, to show an approach in collecting the evidence from the crime scenes where IT crimes occur, transferring these evidence to the data examination laboratory and examining in data laboratory and correcting the faults that are done by field personnel.

IT crimes is a new phenomenon that is added to crime literature. Usage of high technology product IT systems in performing these crimes, makes it difficult to prevent these crimes and to find the criminal. However much more appearance of technological devices to our life day by day; prove the necessity of investigations that have to be done in this disciplinary.

In this thesis, firstly crime concept is defined generally in first part, some definitions of native and foreign criminologists and sociologists whose are experts is this disciplinary are also included. Beside this, in first part also the definition of IT crimes and the details which you should pay attention while making this definition is also explained.

The points which a crime scene investigator should pay attention while handling the evidence in the crime scene where an IT crime occurred, are also explained in second part.

Precautions for preventing the loss of integrity of the evidence and examination techniques that are performed in data laboratory where electronic evidence convert to digital evidence and this digital evidence finally examine, are explained in third part. Also in this part, the concept of writing a computer forensics expertise report for sending the results of a performed examination to a related court is explained.

**Key Words:** Computer forensics, computer crime, digital evidence, crime scene, law.

# KAYNAKLAR

ACPO (Association of Chief Police Officers), Computer Crime Group (1999). Good Practice Guide For Computer Based Evidence. London: National Hi-Tech Crime Unit.

ANDERSON, A., MOHAY, G. (2003). Computer and Intrusion Forensics. Boston: Artech House.

ASHCROFT, J. (2001). Electronic Crime Scene Investigation: A Guide for First Responders. Washington: U.S. Department of Justice, National Institute of Justice.

ATASOY, S. (2006). Olay Yeri: İnternet, Erişim: [http://hurarsiv.hurriyet.com.tr/goster/haber.aspx?id=4334930&tarih=2006-04-30]. Erişim Tarihi: 08.06.2006.

BAYER, M., KAYGISIZ, M. (2002). Olay Yeri İnceleme, Ankara: Emniyet Genel Müdürlüğü.

BAYRAM, L. (2005). Deliller ve Bilirkişilik Müessesi, Polis Dergisi, Sayı 28.

BERBER, L. K., (2004). Adli Bilişim, Ankara, Yetkin Yayınları.

BROWN, C. (2001). Procedural Aspects of Obtaining Computer Evidence with Highlights from the DoJ Search & Seizure Manual. California: Technology Pathways.

BROWN, J. (1989). Erişim:[http://groups.google.com/group/ comp.risks/browse_frm/month/1989-08].Erişim Tarihi: 07.02.2006.

CARRIER, B. (2005). File System Forensic Analysis. New Jersey: Addison Wesley.

CASEY, E. (2002). Handbook of Computer Crime Investigation. California: Academic Press.

CURTIS, P. A. (2000) Cyber Crime: The Next Challenge: An Overview of the Challenges Faced by Law Enforcement While Investigating Computer Crimes in the Year 2000 and Beyond. Arkansas: Arkansas Systems.

DÖNMEZER, S. (1994). Kriminoloji. İstanbul: Beta Basım.

GREENFIELD, R. S., MARCELLA, A. J. (2002). A Field Manual For Collecting Examining And Preserving Evidence Of Computer Crimes. Florida: Auerbach Publications.

HAILEY, S. (2003). What is Computer Forensics? Erişim:

[http://www.cybersecurityinstitute.biz/forensics.htm,Erişim Tarihi: 21.03.2006.

HATCHER, M., MCDANNELL, J., OSTFELD, S. (1999). American Criminal Law Review. Washington: Georgetown University Law Center Publications.

HILBERT, E. J., MORFF, L., WHELAN, D. (2004). The Cyber Challenge, Cybercrime and the Challenges Ahead. California: Federal Bureau of Investigation.

HTCI, (High Tech Crime Institute) (2004). High Tech Crime Investigator International Course Workbook & Lab. Manual. Florida: HTCI Publications.

KARAGÜLMEZ, A. (2005). Bilişim Suçlarında Delil Toplamayı Etkileyen Başlıca Konular. 2. Polis Bilişim Sempozyumu, 14-15 Nisan 2005. Ankara: Emniyet Genel Müdürlüğü.

KAYGISIZ, M. (2003). Adli Bilimler. Ankara: Seçkin Yayıncılık.

MAHER, M. (2004).Writing a Computer Forensic Technical Report. SANS Institute.

ÖZCAN, M. (2004). Siber Terörizm ve Ulusal Güvenliğe Tehdit Boyutu, İnternet ve Hukuk, ATAMER, Y. İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

ÖZGENÇ, İ. (2005). Yeni Türk Ceza Kanununun Genel Hükümleri ve Yansımaları Paneli. Ankara: Yargıtay Yayın İşleri Müdürlüğü.

POLAT, O. (2004). Kriminoloji ve Kriminalistik Üzerine Notlar. Ankara: Seçkin Yayıncılık.

POTACZALA, M. (2001). Computer Forensics. Florida: University of Central Florida Publications.

SCHWEITZER, D. (2003). Incident Response Computer Forensics Toolkit. Indianapolis: Wiley Publishing.

STEPHENSON, P. (2000). Investigating Computer-Related Crime. Florida: CRC Press.

UNDERWOOD, J. (2006). Erişim: [http://www-staff.it.uts.edu.au/~jim]. Erişim Tarihi: 12.01.2006.

UZUNAY, Y. (2005) Dijital Delil Araştırma Süreci, 2. Polis Bilişim Sempozyumu. Ankara.

VACCA, J. R. (2002). Computer Forensics. Boston: Charles River Media.

WHITCOMB, C. M. (2002). An Historical Perspective of Digital Evidence: A Forensic Scientist's View. New York: Utica College Publications.