TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

BİLİŞİM CİHAZLARINDAKİ SAYISAL DELİLLERİN TESPİTİ VE DEĞERLENDİRİLMESİNDE İŞ AKIŞ MODELLERİ

Mustafa İlker ÖZTÜRK

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

DANIŞMAN
Prof. Dr. İzzet DUYAR

2007 - ANKARA

Ankara Üniversitesi Sağlık Bilimleri Enstitüsü

Fizik İncelemeler ve Kriminalistik Programı

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

Tez Savunma Tarihi : 03.07.2007

Prof. Dr. Tülin SÖYLEMEZOĞLU
A.Ü. Adli Tıp Enstitüsü
Jüri Başkanı

Prof. Dr. İzzet DUYAR
Ankara Üniversitesi

Prof. Dr. İnan GÜLER
Gazi Üniversitesi

Yrd.Doç.Dr. Mehmet DEMİRER
Hacettepe Üniversitesi

Yrd.Doç. Dr. Mustafa DÖNMEZ
Polis Akademisi

ÖNSÖZ

Bilişim teknolojilerinin günlük yaşama biçimlerinde ve yönetim felsefesinde yarattığı büyük değişimden insana dair her husus etkilenmiştir. İnsan olmanın sosyal bir tezahürü olarak suç, bilişim çağında daha da çeşitlenmiş, karmaşıklaşmış ve etkinliğini artırmıştır. Üstelik tehdit kapsamı kolayca ve hızla genişlemiş, sadece bireyler değil kurumlar ve devletler de hedef haline gelmiştir.

Suç artık bilişim teknolojileri ile ilişkilidir. Dolandırıcılıktan hırsızlığa, politik cinayetlerden organize suçlara kadar pek çok önemli suçun bir yerinde cep telefonu, bilgisayar veya internet yer almaktadır. Gelişen ve değişen suç ortamı, adli süreçle ilgili kavramları ve görevleri de değiştirmiştir. Delil sayısallaşmış, bilgisayar suç unsuru olmuş, internetin sanal dünyası bir olay yeri haline gelmiştir.

Toplumsal ivme ve teknolojik gelişim, geleceğin dünyasında bireysel ve kurumsal açıdan en önemli ihtiyaçların güvenlik ve adalet olacağını göstermektedir. Hukuk ve güvenlik hizmetlerindeki kalitenin yükseltilmesi, ancak hukuk sisteminde rol alan tüm kişi ve kurumların teknolojik gelişmelere uyumları ile mümkün olacaktır.

Sayısal delil, sayısal delillerin tespiti ve değerlendirilmesi kavramları adli sürece yeni dâhil olan temel kavramlardır. Bu kavramların ticari kaygılardan arınmış, her şartta uygulanabilir ve genel esaslara kavuşturulmasıyla, kolluk birimlerinin görev etkinliğinin artırılması ve adli sürecin işleyişine olumlu katkılar sağlanacağı değerlendirilmektedir.

Çok değerli fikirleri ile çalışmama yön veren danışmanım Prof. Dr. İzzet DUYAR ve desteğini esirgemeyen hocam Prof. Dr. Tülin SÖYLEMEZOĞLU'na saygı ve minnetlerimi sunarım.

Bu uzun süreci benimle birlikte yaşayan, varlıklarını her zaman yanımda hissettiğim fedakâr eşim Nurgül, yaramaz oğlum Efe ve cefakâr canım Babam'a tüm kalbimle teşekkür ederim. Rüyalarıma giren melek Annem, sen hep kalbimdesin…

İÇİNDEKİLER

KISALTMALAR DİZİNİ

CMK	Ceza Muhakemesi Kanunu
EİK	Elektronik İmza Kanunu
FSEK	Fikir ve Sanat Eserleri Kanunu
HUMK	Hukuk Usulü Muhakemeleri Kanunu
m.	Madde
TCK	Türk Ceza Kanunu
T.C.	Türkiye Cumhuriyeti

ŞEKİLLER DİZİNİ

1. GİRİŞ

İlk çağlarda insanların ateşi bulmasından, tekerleği icat etmesinden, aletler üreterek hayatı kolaylaştırmasından tutun günümüze gelinceye kadar yapılan buluşlar ve gelişmeler aynı mantık içerisinde meydana gelmekte ve evrimsel bir çizgi izlemektedir. Bilgisayar ve İnternet'in ulaştığı günümüzdeki durum, hemen hemen bütün maddi ürünlerin sayısal dönüşüme uğraması yani şimdiye kadar üretilmiş maddi kültür öğelerinin sayısal ortamda birer kopyalarının yaratılmasıdır.

Bilişim ve iletişim teknolojileri, yayılmakta olan yeni uygarlık kültürünü ve bu kültürün getirdiği yeni yaşam biçimini günlük hayata egemen kılmıştır. İnternet olgusunun katalize ettiği bu büyük değişim göz önüne alınarak, sosyal yaşamın en canlı bileşeni olan adli sistemin de bilgi çağının etkileri ve katkılarına göre yeniden değerlendirilmesi, bir gereklilik olarak karşımıza çıkmaktadır.

Duyu organlarının algılama hızını çoktan aşan teknolojik gelişme sürecinde çoğu kez üretilen bilgi, bir öncekini eskitmekte veya işe yaramaz kılmaktadır. Özellikle ticarileşen pozitif ilimlerde eski yöntem, cihaz veya bilginin yerine yenilerinin kullanılması bir moda şeklinde pompalanmaktadır. Ancak olay yeri inceleme, suçla mücadele ve hukukta geleneksel yöntemlerden vazgeçmek mümkün değildir. İnsan kavramını teknolojinin çok daha gerisinde gören bir yaklaşımın kabul görürlüğü cehalet ve suç cesaretinin tezahürüdür.

Teknolojideki gelişmeler yaşamı kolaylaştırdığı, ekonomik ve sosyal hayata önemli katkılar sağladığı gibi pek çok olumsuzluğu da beraberinde getirmiştir. Hızla gelişen bilişim ortamı, hem suç ve suçlu için kaynak olmuş

hem de suç ve suçlulukla mücadelenin en önemli enstrümanlarından birini oluşturmuştur.

Adli ve hukuki süreç içerisinde bilişim teknolojisinin doğrudan veya dolaylı kullanıldığı olaylarda delil tespiti, değerlendirme ve sunumu derinliğine inilerek incelenmesi ve uygulanabilir iş akışlarının ortaya konulması gereken bir kara delik olarak kalmıştır. Adli sistem içinde bilişim cihazları ile ilgili prosedürler kişisel gayretler, standart olmayan süreçler ve hukuka uygunluğu tartışmalı sonuçları içermektedir. Çoğunlukla gözden kaçan, değerlendirilmeyen veya yanlış değerlendirilen deliller ortaya çıkmaktadır.

Kolluk birimleri ve hukuk sistemi açısından sayısal delillerin tespiti ve delillendirilmesi konusunda eğitim, düşünce ve yönetim düzeyinde araştırma/geliştirme çalışmalarının yapılması zorunludur. Şimdinin küçük varsayılan bu zafiyeti, çok yakın bir gelecekte evrensel, toplumsal ve kişisel kurallar, haklar ve çıkarların korunmasında göz ardı edilemeyecek, boş verilemeyecek ve ivedilikle çözüm aranacak bir sorunlar kümesine evrimleşecektir.

Bu çalışma ile bilişim cihazlarındaki sayısal delil incelemesinde bilgi, belge ve işlem standardının oluşturulması, bilişim teknolojisinin suçta kullanımının doğru olarak tasvir edilebilmesi ve bilişim teknolojisinin karar desteği açısından adli sürece sağlayabileceği katkı konularında öneriler sunulmuştur.

Adli bilişim, hukuk ve bilişimin ortaklığını temel alan bir disiplindir. Ancak bu disiplinin pek az uygulayıcısı vardır. Bu çalışma ile hukuk bilgisi sınırlı olan bilişim personeline konunun hukuki yönünde temel bilgiler kazandırmak, bilişim teknolojileri konusunda yeterli bilgisi olmayan hukuk camiasına konunun bilişim yüzü hakkında bilgi vermektir. Nihai hedef, her iki önemli disiplinin icracıları arasında ortak bir dil geliştirebilmektir.

Çalışma kapsamındaki hukuki konular ve bilişim suçları literatür araştırması yöntemi ile incelenmiştir. Literatür araştırmalarında cihaz, marka, model veya inceleme amacına bağımlı olarak yapılan sayısal delil tasnif ve tespit yöntemlerinin standart oluşturmadığı, ticari kaygılar gözettiği ve işlem bütünlüğünü sağlamadığı tespit edilmiştir. Bu temel sorunlara çözüm sağlanması maksadıyla **"Bilişim cihazları/ortamlarındaki sayısal deliller"** bölümü her tür bilişim cihazına uyarlanabilir olma şartını sağlayacak şekilde , **"Sayısal delil tespitinde önerilen iş akışı"** bölümü her tür adli olayda uygulanabilir olma şartını sağlayacak şekilde, **"Sayısal delillerin laboratuvar incelemelerinde önerilen iş akışı"** bölümü her türlü adli bilişim incelemesinin yapılabilir olma şartını sağlayacak şekilde, **"Sayısal delillerin değerlendirilmesi"** bölümü sayısal delillerin hukuki ve teknik açıdan etkin ve hızlı şekilde değerlendirilebilir olma şartını sağlayacak şekilde mesleki tecrübeler ve saha çalışmaları esas alınarak özgün şekilde oluşturulmuştur. Ayrıca bu çalışma donanımlı bir adli bilişim laboratuvarının tesisi için gerekli fiziki ve idari şartları ortaya koymuştur.

Bireylerin ve toplumların hayatında köklü ve evrensel değişimlere yol açan bilişim teknolojilerinin yarattığı yeni felsefe ve düşünce sistematiği, yönetim ve iş yapma yöntemlerine yeni boyutlar kazandırmıştır. Bu bağlamda; sayısal delillerin hukuka uygun bir delil olarak kabul edilebilmeleri, farklı bir mücadeleyi gerektirmektedir. Bu mücadelenin verilebilmesi için sayısal delil kavramının bilinmesi, sayısal delilin adli prosedüre uygun olarak toplanması ve değerlendirilmesi gerekmektedir. Her türlü çalışmanın idari bir takım tedbir ve iş yapma felsefeleri ile desteklenmesi, suçla mücadelede etkinliğin artırılması için zorunludur.

1.2. Bilişim Kavramı

Bilişim, bilginin elektronik ortamda üretilmesi, kaydedilmesi, saklanması, taşınması ve/veya kullanılması ile ilgili cihaz, materyal, işlem ve

yöntemleri kapsamaktadır. Çoğunlukla bilişim ile bilgisayar kelimeleri eş anlamda kullanılıyor olsa da bu aslında küçük bir yanılgıdır. Zira bilgisayar, çok sayıda aritmetiksel ve/veya mantıksal işlemlerden oluşan bir işi önceden verilmiş bir programa göre yapıp sonuçlandıran, bilgileri depolayan elektronik araç, elektronik beyin olarak tarif edilmektedir. Bilişim, bilgisayardan faydalanılarak bilgilerin üretilmesi, depolanması, işlenerek başkalarının hizmetine sunulur hale getirilmesi ve iletilmesi faaliyetini; bilgisayar ise bu faaliyetin gerçekleştirilmesinde en önemli bileşen olan cihazı ifade etmektedir.

İnsanlık, tarihsel süreç içerisinde çeşitli evrelerden geçmiştir. İlk insanların avcılık ve toplayıcılık yaparak yaşamlarını sürdürmelerinin ardından gelen dönemde ağaç, taş gibi çeşitli araçları kullanan insanlar, yaşamlarını daha kolaylaştırmanın arayışı içerisinde olmuşlardır. Daha sonra insan gücünün yerini makine gücünün almasıyla yeni bir döneme geçilmiştir. Bu dönemin de belirgin özelliği, daha yaşanılabilir bir dünya yaratmak ve toplumsal refahı sağlamaktır. Ve nihayet, bütün bu gelişmelerin temelinde yatan bilgi, dünya genelinde gelişimin vazgeçilmez unsuru haline gelmiştir. Bilginin üretiminin artması ile birlikte onun depolanması, iletilmesi ve kullanılmasını sağlayan araçlarda da artış olmuş ve böylece insanlık yeni bir döneme geçiş yapmıştır.

M.Ö. 2000 yılında Çinliler tarafından icat edilen ilk hesaplama aracı sayı boncuğu (abaküs) ile tohumlanan ve 1946 yılında ECKERT ve MAUCLY tarafından ENIAC isimli cihazın geliştirilmesiyle sürgün veren bilişim çağına gelinen sürecin en önemli kilometre taşları; AntiKitira Makinesi (M.Ö. 150–100), algoritma kavramının babası ALHAREZMİ, otomatik olarak çalışan ilk makinenin mucidi EB-ÜL-İZ, Wilhelm SCHICKARD, Fransız mucit Joseph Marie JACQUARD, Fransız fizikçi Blaise PASCAL, Alman matematikçi Wilhelm LEIBNEZ, İngiliz matematikçi Charles BABBAGE, Amerikalı mühendis Herman HOLLERITH olarak sayılabilir. Farklı milletlerden, farklı zaman dilimlerinde, farklı bilimsel disiplinlerdeki binlerce saygıdeğer bilim

insanının en az 4000 yıllık emeğinin ve bilgi üretiminin sonucu bilişim çağı başlamıştır.

Önceleri sadece çok karmaşık bilimsel hesaplamalarda hata ihtimallerinin asgariye indirilmesi amacıyla kullanılan ve tek amacının bu olduğu düşünülen bilgisayar, bilgi ürettikçe daha çok geliştirilmiş, geliştikçe daha çok bilgi üretilmesinin yöntemi olmuştur.

1990'lı yıllarla başlayan yeni toplum yapısında bilgi, bir üretim faktörü niteliğini kazanmış; ekonomik, sosyo-kültürel veya politik karar ve davranışların temel etkeni olmuştur. Bu süreç bilgiyi üreten yegâne güç olan bireyin önemini artırmıştır. Buna paralel olarak bilgi ile nitelenen yeni bir toplumsal yapı ortaya çıkmıştır.

Bugün bilişim ve iletişim teknolojileri, sahip olduğu kapasite nedeniyle hem dönüşmeye ve hem de toplumları dönüştürmenin en etkin ve maliyeti düşük yöntemi gibi görünmektedir. Karşılıklı ilişkiler bütünü olarak görülebilecek toplumların yavaş yavaş bu özelliklerini kaybettikleri ve artık, giderek bir ağ (network) toplumu oldukları yönünde görüşler dillenmektedir.

1.2. Bilişim ve Hukuk

Toplu yaşam, ihtilaf doğuran bir sosyal mekanizmadır. İnsanlar bu ihtilaflarını çözmeden huzur bulamazlar ve yaşamlarını sürdüremezler. Çıkar hırsı ile çatışan insanları teskin eden, birbirleriyle kaynaştıran, yöneticilere nüfuz ve itibar sağlayan biricik tılsım adalettir. Adalet mülkün ve tüm uygar erdemlerin temeli, hukukun idesidir. Hukuk yüzünü adalete çevirmiş toplumsal yaşama düzeni, özgürlük ve barışın ön şartıdır.

Hukuki bir kavram olarak adalet; herkesin kanun önünde eşit sayılması, fırsat eşitliğinin bulunması, herkese kişiliğini geliştirme imkânı

verilmesi, buna engel olan maddi ve manevi sebeplerin ortadan kaldırılması, her türlü imtiyaz ve keyfiliğin önlenmesidir.

Bilişim teknolojisi, sunduğu imkân ve kabiliyetler ile her yaşam alanına nüfuz etmiştir. Alış veriş, bankacılık, eğitim, eğlence, kişisel gelişim, iletişim, basın gibi sosyal hayata ait pek çok unsurun omurgasını oluşturmaktadır. Bilişim teknolojilerinin kullanımının logaritmik olarak artmasıyla birlikte artık sadece teknik bir kavram olmaktan çıkmış sosyal kimliğe de bürünmüştür. Bilişim dünyası, sanal olması nedeniyle kritik edilebilir. Sıfır ve birlerden oluşan dünya bir bilgisayar vasıtasıyla sanaldır. Ancak sosyal bir etkileşimin var olduğu da artık yadsınamaz bir gerçektir.

Bir sosyal ortamda öne çıkan iki unsur vardır: haklar ve sorumluluklar. İşte burada hukuk yerini bulmaktadır. Hukuk, insanların ve kurumların birbirlerine karşı hak ve sorumluluklarını düzenleyen kurallar bütünüdür. Bugün hukuk dünyası, bilişim alanında sanal toplum yaşamını düzenleme, sosyal ihtiyaçları karşılama ve adalet düşüncesini gerçekleştirme amaçlarını tartışmaktadır.

Ekonomide ve teknolojide yaşanan hızlı gelişmeler her zaman hukuk alanında sıkıntılar yaşanmasına neden olmuştur. İnsanoğlunun hayatta kalabilmesi için gereken fizyolojik ihtiyaçlarından evrimleşen ekonomi ve rahat yaşamasını sağlamasını hedefleyen teknolojiyi geriden takip etmek zorunda kalan hukuk, ancak sorunla karşılaşıldığında başvurulan bir kurum olmuştur. Aslında sorun, hukukun sosyal hayatın diğer alanlarının neresinde bulunduğu değil, toplumun yaşama tarzının değişmesi ve gelişmesine karşı gösterdiği duyarlılık seviyesi ve tepki hızındadır. Yani eleştirilmesi gereken husus hukukun toplumsal olguların gerisinde olması değil yeni hukuki durumlara intibak yavaşlığıdır.

Bilişim sistemleri artık kapsam, derinlik ve siyasi etkinliği itibariyle sınırları aşan, kendine has evrensel değerleri ve kültürü olan bir sosyal ortam

yaratmıştır. Bu nedenle milli hukuk sistemlerinin tek başlarına, sanal gerçek ortamları hukuki bir zemine oturtmakta yetersiz kaldıkları bir gerçektir. Uluslararası katılımla asgari müşterek kurallarda anlaşıldığı takdirde, ortaya çıkan sonuç; uygulanabilir, tatmin edici ve evrensel normda bir hukuk olacaktır.

1.3. Bilişim Suçları

Bilişim ile hukukun en çok kesiştiği nokta bilişim suçu kavramıdır. Psikolojik, sosyolojik ve ekonomik anlamda son yılların en önemli araştırma konusu olan bilişim suçları, etkileri ve sonuçları itibariyle mahkeme salonlarının da en sık rastlanan aktörlerinden birini oluşturmaktadır. Sınırları ve gelişim hızı dikkate alındığında adli sürece her gün yeni bir suç türü, suç tekniği ve kavram eklenmektedir. Bu nedenle bilişim suçlarının soruşturulması, klasik suçlara göre daha özel bir eğitim, disiplinlerarası bir uzmanlık ve yeni yöntemler gerektirmektedir.

Bir cep telefonu ile yapılan darp eyleminden bir terör olayına, bankaların internet yolu ile soyulmasından kamu güvenliği ile ilgili bilgilerin çalınmasına kadar çok geniş bir suç yelpazesinde karşımıza çıkan sayısal delil kavramının %100 ilgili olduğu tek suç türü bilişim suçudur. Çünkü fail, mağdur ve yöntem üçlüsünden en az biri kesinlikle bilişim kaynağını kullanmaktadır. Bu bölümde unutulmaması gereken en önemli husus, **her bilişim suçu bir sayısal delil kaynağıdır ancak sayısal delil kaynağı olabilecek tek suç türü değildir.**

Herhangi bir adli olayın bir yerinde bir bilişim cihazının yer alması, yani suç, sanık, mağdur ve/veya tanıkla ilgili her hangi bir bilginin bilişim cihazında saklı olması, bu delilin teknik incelemelerle elde edilmesi anlaşılabilir bir kavramdır. Bu tür delillere yaklaşım, parmak izi incelemesi veya DNA incelemesinden daha farklı anlaşılmamaktadır. Ancak bilişim suçlarında suç

oluşturan eylem, yöntem, sanık, mağdur ve mağduriyet derecesi açılarından kararlara etkili farklı hukuki algılamalar oluşmaktadır. Bu nedenle teknik ayrıntılara boğulmadan bilişim suçlarının tasnif edilmesi ve herkesin anlayabileceği ölçüde açıklanması uygun değerlendirilmiştir.

1.3.1. Bilişim Suçu Kavramı

Sayısal teknolojileri ilgilendiren suçlar; bilgisayar bağlantılı suç, bilgisayarla işlenen suç, bilgisayara karşı işlenen suç, bilgisayar suçu, elektronik suç, siber suç, sanal suç, internet suçu, bilişim sistemi aracılığı ile işlenen suç, bilişim alanında işlenen suç gibi onlarca isimle nitelenmiştir. Suç kapsamını en geniş şekilde kavraması nedeniyle "*bilişim suçu*" terimi son zamanlarda daha çok kabul görmekte ve kullanılmaktadır.

Denetimin olabildiğince zor, suiistimalin ise bir o kadar kolay olduğu bu sanal yaşam biçiminde, İnternet'in vazgeçilmez hale gelmesinde ve yaygınlaşmasında sadece yasal kullanım değil, aynı zamanda onun yasal olmayan yollar için kullanımı da büyük rol oynamıştır.

Bilişim suçu ile ilgili en sık karşılaşılan resmi tarif, Avrupa Birliği Uzmanlar Komisyonu'nun Mayıs 1983 tarihinde Paris Toplantısı'nda yaptığı tanımlamadır. Bu tanımlamaya göre bilişim suçu, bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetkisiz gerçekleştirilen her türlü davranıştır.

Amerikan hukukunda bilişim suçu, bilgisayar verilerinin çalınması, sabote edilmesi veya her hangi bir suç işlenmesi için bilgisayarın kullanılması gibi bilgisayar teknolojisi gerektiren suç çeşidi olarak tanımlanmıştır (Dülger, 2004).

İtalyan hukukunda bu kavram enformatik suçu, elektronik suç ve bilişim suçluluğu ile ifade edilirken; Fransız hukukunda bilişim suçları ve verileri otomatik işleme tabi tutan sistemlere karşı işlenen suçlar terimleri ile yer bulmuştur (Dülger, 2004).

Ülkemiz hukuk sisteminde bilişim suçları, mülga TCK'na göre tıpkı Fransız hukuk sisteminde olduğu gibi verileri otomatik işleme tabi tutan sistemlere karşı işlenen suçlar ile tarif edilirken; 5271 sayılı yeni TCK'nda Bilişim alanında suçlar başlıklı 10. bölüm, bilişim suçlarına ayrıntılı olarak yer vermiştir (Dülger, 2004).

Bilgi ve İletişim teknolojilerinin evrensel ve ulusal alanda etkisinin ve etkinliğinin artması, suçun bireyselliğinden daha yoğun olarak kurumsal bir kimliğe bürünmesine neden olmuştur. Her ölçekteki organizasyonun bilişim teknolojilerinin iletişim yeteneklerini ve açıklarını kullanma yönünde yasal veya yasadışı olarak yapılandıkları dikkati çekmektedir. Bilişim suçu, bankamatik şifresi kopyalamak gibi nitelikli hırsızlıktan başlayıp toplumdaki güven duygusunu azaltmaya yönelik terörist eylemlere kadar değişik ve etki alanı büyüyebilecek hedeflerle işlenmektedir.

Bilişim suçlarının fail ve mağdur yelpazesi genişlemekte, mağduriyet seviyeleri çeşitlenmektedir. Kişisel tatmin, suç işleme, siyasi çıkar sağlama, ekonomik çıkar sağlama, bilgi toplama, savunma, terörizm veya psikolojik harekât maksadıyla; kişiler, devletler, hükümetler, şirketler, yöneticiler, suç örgütleri, muhalifler, teröristler ve casuslar fail veya mağdur olabilmektedir.

Bilginin ani, hızlı ve çok üretilmesi, iletilmesi ve sonrasında kullanılması, bir takım bireysel veya toplumsal fırsatların yanı sıra tehdit ve riskleri de beraberinde taşımaktadır. Denetimin olabildiğince zor, suiistimalin bir o kadar kolay olduğu sanal yaşam biçiminin vazgeçilmez hale gelmesinde ve yaygınlaşmasında sadece yasal kullanım değil, aynı zamanda yasal olmayan yollar için kullanımı da büyük rol oynamıştır. Ancak altı çizilmesi

gereken konu, bilişim suçu ile mücadelede cephenin her geçen gün biraz daha genişlediğidir.

1.3.2. Bilişim Suçu İşleme Yöntemleri

1.3.2.1. Fiziksel Zarar Verme

Bilişim sistemleri konusu her ne olursa olsun hizmet üretmek maksadıyla kullanılmaktadır. Bilişim suçu söz konusu olduğunda işin somut boyutu genellikle göz ardı edilmektedir.

Ancak sistemin donanım boyutu da veri ve yazılım kadar olmazsa olmaz bileşenini teşkil etmektedir. Hizmetin engellenmesi maksadıyla kasti olarak ve suç teşkil edecek şekilde sistemin fiziksel varlığının tamamına veya bir kısmına yönelecek ızrar eylemi bu kapsamda değerlendirilmelidir.

5271 sayılı TCK 'nun sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunu düzenleyen 244. madde gerekçesinde bu husus "***aracın fizik varlığı ve işlemesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır***" denilerek bilişim sistemlerini fiziki varlığına zarar vererek engellemeyi kastedilmektedir (Dülger, 2004). Suç kastı sadece mağdurun mal varlığına zarar vermek ise 244. madde uygulanmayacak, failin kastının bilişim sisteminin donanım kısmına zarar vermek olduğu durumlarda soruşturma konusu suç tipi söz konusu madde olacaktır.

1.3.2.2. Mantıksal Zarar Verme

Bilişim sistemlerinin işleyişinin fiziksel açıdan engellenmesi çoğu zaman mümkün değildir. Kurumlar fiziksel bilişim yatırımlarını korumada özen

göstermektedirler. Bu nedenle fiziksel olarak erişilmeleri güç olan fiziksel donanım yerine bilişim sisteminin yazılım ve veri bileşenleri, saldırılması daha mümkün ve kolay hedefler olarak seçilmektedir.

Modern yaşama düzeninin ekonomi, sağlık, güvenlik, eğitim gibi temel konuları artık bilişim sistemleri ile düzenlenmekte ve yönetilmektedir. Sağlık ve ekonomi alanlarında olduğu gibi zaman-kritik veya görev-kritik bazı uygulamalarda yaşanabilecek hata, aksaklık ve kesintiler telafi edilemez zararlara neden olabilmektedir. Hayatın akışında bu denli önemli bir yer almış bulunan bilişim sistemlerinin verilerine ve verilerin işleyişlerine zarar vermek toplumsal güvensizlik gibi kimsenin öngöremeyeceği zararların önüne geçmek maksadıyla suç olarak değerlendirilmiştir.

Bu suç kapsamında sadece verilerin silinmesi, değiştirilmesi veya çalınması anlaşılmamalı; verilerin işleniş şekillerini yani programları, verinin yasal sahibi olan kurumun istediğinden farklı olarak değiştirmek, bozmak veya çalmak şeklinde de anlaşılmalıdır. 5271 sayılı TCK 'nun 244. maddesinin 2. fıkrası söz konusu suçu "Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır" şeklinde düzenlemiştir.

1.3.2.3. Elektronik İmza İle İlgili Suçlar

İş yapış yöntemlerinin bilgi teknolojilerine taşınması evrakların elektronik ortamda üretilmesine, işlenmesi ve dağıtılması sonucunu doğurmuştur. Hukuki ve mali sistem, ıslak imza olarak tabir edilen, yassı selüloz yüzey üzerine el yazısı ile imza dışındaki seçeneklerin arayışında olmuştur. Elektronik imza bu ihtiyacın bir sonucu olarak geliştirilmiş bir bilişim teknolojisidir.

Elektronik imza; bilişim sistemi içinde üretilen veri, belge ve dosyaların gönderme ve alma eylemleri arasında geçen süreçte elektronik anlamda değişmediğini garantilemeyi amaçlamıştır. Kâğıt belgelerde yapılan sahtecilik gibi elektronik imza hususunun da suç kastı bir takım yasadışı işlemlere konu edilmesi mümkündür.

5070 sayılı Elektronik İmza Kanunu'nun 16. maddesinde "elektronik imza oluşturma verilerinin izinsiz kullanımı suçu" ile 17. maddesinde "elektronik sertifikalarda sahtekârlık suçu" düzenlenmiştir. Bu suçlar ile korunmak istenen hukuksal değer, devletin korumasında ve denetiminde olan bu tür verilere karşı güven duygusudur.

1.3.2.4. Sosyal Mühendislik Yöntemi

Planlı işlenen suçların çoğunda, elde edeceği kazancı artırmak ve yakalanma riskini en aza indirmek için, fail, önceden yer, zaman ve ortam ile ilgili bilgi toplamak zorunda hissetmiştir. Bu nedenle bilişim sistemleri ile ilgili yasadışı bir operasyon yapmak isteyenler önce bu sistem hakkında detaylı bilgiler toplarlar. Ağın topolojisi, şirket bilgileri, ağ cihazlarının markası/modeli, ağda bağlı bilgisayar sayısı, işletim sistemi, güvenlik yazılımlarının markası/sürümü, uzaktan erişim için telefon numaraları, sorumlu personel bilgileri gibi elde edebileceği her türlü bilgi hedefe ulaşmasına biraz daha yardım eder (Yılmaz, 2005).

Bilgi toplamanın ilk adımı açık kaynak araştırmasıdır. Açık kaynak olarak internet, basılı ve görsel medya, teknoloji dergileri veya şirket broşürlerinde yer alan, şirketlerin bilinmesinde sakınca görmedikleri her türlü bilgi değerlendirilmektedir. Örneğin şirketler müşterilerine güven vermek ve rekabet avantajı sağlamak için çoğu kez bilişim sistemlerinde yaptıkları yatırımları marka ve model belirterek ifşa etmektedir. Bu durumda söz konusu şirket açık bir hedef haline gelmektedir.

Sistem taraması bilgi toplamanın ikinci adımıdır. Bu adımda açık kaynak araştırmasında elde edilen bilgilere göre güvenlik açıkları taranmaktadır. Ne kadar iyi korunursa korunsun her sistemin güvenlik zafiyetleri vardır. Sisteme sızmak isteyen kişiler, elde ettikleri bilgiler ışığında her bir sistem bileşenine göre ayrı ayrı belirledikleri stratejiye göre bir eylem planı oluşturmaktadır.

Gerek bilgisizlik ve eğitimsizlik gerekse dikkatsizlik nedeniyle sistemde yer alan donanım ve işletim sistemlerine ait şifrelerin değiştirilmesi unutulmakta veya çok basit olarak belirlenmektedir. Sosyal mühendislik, bu parolaların çok özel bir çaba göstermeden en uygun tahminlerin yapılması ve hedefe ulaşılması olarak açıklanabilir. Bu konu çok basit görünse de halen çok yaygın olarak kullanılan bir şifre kırma yöntemidir.

1.3.2.5. Virüs Saldırısı

Bilgisayar veya bilişim virüsleri, kendi kendisini çoğaltabilen, kopyalarını başka bilişim sistemlerine ulaştırarak bu sistemlerin isleyişini etkileyebilen yazılımlardır. Bilişim virüsü de bir çeşit yazılımdır. Ancak virüsleri diğer yazılımlardan ayıran nitelik, bulaştıkları sistemde bulunan yazılımlara ve/veya verilere zarar vererek bilişim sisteminin zarar görmesini sağlayacak şekilde tasarlanmalarıdır (Dülger, 2004).

Bilişim virüsleri, bilişim ile ilgili suçlar arasında en sık karşılaşılan ve en fazla zarara neden olan suç işleme araçlarıdır. Hazırlanması ve bulaşması kolay ancak tedbir alınması ve zararın telafi edilmesi çok güçtür. Bulaşma şekillerine, zarar seviyelerine veya hedeflerine göre tasnif edilebilen bilişim virüslerinin oluşturdukları suç unsuru, bilişim sisteminin işleyişini engellemek ve/veya bilgi çalmak olarak değişebilmektedir.

Belgelenen ilk virüs saldırısının 1987 yılında Amerika Birleşik Devletlerinde meydana gelmesinden bugüne kadar binlerce yeni virüs üretilmiş ve dünyaya yayılmıştır. Günümüzde bu husus, artık ticari bir döngü haline gelmiştir. Gün be gün yeni virüsler ortaya çıkmakta olup, akabinde bunların tespiti ve temizlenmesine yönelik ticari çözümler piyasaya sürülmektedir.

1.3.2.6. Truva Atları

Akhalılar tarafından Troyalılara masum bir hediye olarak sunulan büyük tahta attan adını alan bu yöntem, tıpkı adını aldığı gizli stratejinin mantığında çalışır. Kullanıcı yararlı gördüğü için kullandığı bir yazılım, sistem dosyalarına zararlı kod parçacıkları (Truva atı, trojan) eklemektedir. Özellikle internet ortamında dağıtılan ücretsiz programlar bu tür tehlikeleri taşımaktadır.

Truva atı yazılımı, küçük boyutta ve dikkat çekmeyen özellikte olduğundan çoğu kullanıcı tarafından bir tedbir düşünülmez bile. Oysaki Truva atı yazılımları, sistemin tüm güvenlik reflekslerini ortadan kaldıracak şekilde veri ve yazılım bileşenlerine zarar verebilir. Bu durumun doğal neticesi, saldırıya ve bilgi kaybına açık bir bilişim sistemi ve saldırı neticesinde oluşan büyük kayıplardır.

Bilişim dünyasında virüs saldırıları ile beraber en sıklıkla karşılaşılan suç işleme yöntemidir. Sadece bireysel suç faillerinin değil, kurumsal suç faillerinin de en sıklıkla ve kolay kullandıkları yöntemdir. Merak uyandıran ve okunma ihtimali çeşitli şekillerde artırılan bir elektronik posta yolu ile istenen sisteme ulaşılabilmesi, bu yöntemin tercih edilmesinde en önemli nedendir. Üstelik birçok sistemde birden fazla kullanıcının var olması ve her kullanıcının aynı güvenlik hassasiyetini taşımaması nedeniyle birden fazla kullanıcıya

gönderilen aynı tür elektronik postaların en az biri açılarak truva atı aktif hale getirilebilmektedir.

Söz konusu yöntem, teknoloji casusluğu, milli güvenlik ve istihbarat konularında bilgi toplamak için devletlerin bile sıkça başvurdukları bir yöntem olarak dikkat çekmektedir.

Truva atları çok geniş bir yelpazede değerlendirilmektedir. Mantık bombaları, bilişim tavşanları veya bukalemunlar adıyla anılan birçok yöntem Truva atları kapsamındadır.

1.3.2.7. Ağ Solucanları

Ağ solucanları, sistem içinde kullanıcının etkisi olmadan sistem kaynaklarını kullanarak çalışabilen, kendini kopyalayabilen ve sistemin güvenlik açıklarını sürekli tarayıp otomatik olarak sisteme sızmayı deneyen yazılım türüdür.

Bilişim virüsleri veya Truva atları gibi doğrudan sisteme zarar vermek amacını taşımazlar. Ancak sisteme sızmak için açık kapıları tarar, bulur ve haber verirler. Bu sayede sisteme sızmak veya Truva atı yerleştirmek gibi faaliyetlerin gerçekleşmesi için uygun ortamı hazırlarlar.

Ağ solucanları, sistemin dışa açılan iletişim ağı üzerinde bulunan tüm güvenlik tedbirlerinin kendisine verilen talimatlar (yazılım) doğrultusunda aşmaya çalışır. Başarılı olmuş ise sistemde gerçekleştirilecek eylemin sonrasında tüm izlerini silerek tespitini neredeyse imkânsız hale getirir.

1.3.2.8. Şifreleri Kırarak Sisteme Sızma Yöntemi (Hacking)

Bilgi ve iletişim teknolojileri, dünyanın şimdiye kadar şahit olduğu en önemli ilerlemelerden birini temsil etmektedir. Çünkü insanoğluna emsalsiz

miktarda bilgi ve veriye ulaşma ve onları emsalsiz bir hızda yayma imkânı sağlamaktadır. Medeniyetin ilerlemesinde çok önemli bir rol oynayan dilin gelişimi, matbaanın icadı, kütüphanelerin kurulması ve kitle iletişim araçlarının kullanılmaya başlaması gibi patlayıcı bir etki ve potansiyele sahiptir (Whittle, 1997). Yeni teknolojiler, bireyler ve toplumlar için yeni fırsatlar kadar yeni problemler de yaratmaktadır. Bunlar hem olumlu hem de olumsuz etkilere sahiptirler. Genellikle her ikisi de bir aradadır (Mesthane, 1976).

1970'lerde "phreaker" olarak anılan ve telefon sistemlerine girerek bedava telefon görüşmeleri yapan fırsatçılar ile bilişim suçları duyulmaya başlamıştır. Hukuka aykırı olarak bedava telefon görüşmesi yapma eyleminden bugüne gelinen süreçte, iletişim ve bilgisayar teknolojisinde yaşanan gelişmeler, suç tekniklerini ve suç hedeflerini çeşitlendirmiş, suçun etki alanını genişletmiştir.

Amaç, hedef ve kazanımlarına göre tasnif edilmeye çalışılan suç dünyasının aykırı sanal karakterleri bazen cracker, siber terörist, hacktivist, siber pank, siber hırsız veya siber casus olarak anılsa da, nihai ismi bilişim korsanı (hacker) olarak kalmıştır.

Bilişim korsanı, tüm bilgilere giriş özgürlüğü olduğu inancıyla birlikte yüksek seviyede ihtisaslaşmış bilgiye sahip bir kişi olarak tarif edilmiştir.

Bu özgüven ve özelliklerinden dolayı kendi hazırladığı yazılımlarla sistemi tarar. Sistemin açık olan veya az korunan açıklarını ve arka kapılarını (backdoor) bulur. Bilinen veya kendine özel yazılım teknikleri ile şifrelerini kırar ve sistem içinde yasadışı eylemini gerçekleştirir. Virüs yazar ve truva atları hazırlar. İletişim ağlarını yetkisiz olarak dinler (sniffing) veya sistemin güvendiği bir kullanıcı gibi davranarak aldatır (spoofing). Başka bilişim korsanları ile bilgi ve yazılım paylaşır. Ortak hedefler belirler ve ortak eylem

planları hazırlayarak uygular. Kimliklerinin tespit edilememesi için azami tedbirleri alır.

Bilişim korsanlarının en masumları meraklı kullanıcılardır. Bu sanal karakterler, erişilmez olarak bilinen bilgisayar sistemlerine erişmeyi bir başarı olarak görür, eriştikleri sistemde dolaşır, verileri görür ancak değiştirmezler. Ulaşmış olduklarını ispat için ulaştıkları bilgisayar sistemlerine imzalarını atarlar. Bilişim korsanlarının bir kısmı, gerekli tedbirlerin alınmasını sağlamak maksadıyla ulaştıkları sistemin zayıflıklarını sistemin sahibine göstermeyi şiar edinmiştir.

Ancak çoğu bilişim korsanının aynı iyi niyette olduğunu söylemek imkânsızdır. Bilişim sektörü sadece kendi kaynakları itibariyle milyarlarca dolarlık bir sektör haline gelmiştir. Bilişim teknolojilerini kullanarak hizmet üreten sektörlerin parasal zenginlikleri, sisteme sızma (hacking) faaliyetlerini iştah kabartan bir uğraş alanı haline gelmiştir.

Elbette tek sebebi maddi kazanç sağlamak değildir. Teknolojik sırların elde edilmesi, siyasi nedenler, rekabet üstünlüğü sosyal yaşamın her türlü mücadele alanına hizmet edebilmektedir. Bilişim korsanları, günümüzde sanal dünyanın bilgi savaşlarında devletlerin ve kurumların çıkarlarını korumak için aktif olarak kullanılmaktadır.

Bütün bu tespitlerin yanında kullandıkları yazılım, ağ ve teknikler ceza muhakemesi açısından ele alındığında; aynı eylem sürecinde birden fazla suç unsuru oluşturdukları bir gerçektir.

Bugünün küreselleşen ve nasıl olursa olsun kazanmak felsefesinin hâkim olduğu dünya düzeninde, bilişim korsanlığı sadece meraklı kullanıcıların bir hobisi olmaktan çıkmış cazip bir meslek haline getirilmiştir. Bu mesleği benimseyenlerin desturu da zaten bu felsefeye uygundur: “yasadışı ama kimin umurunda”.

1.3.2.9. Salam Yöntemi

Bu teknik genellikle mali sektörde hukuka aykırı yarar sağlama suçları için kullanılan yaygın bir yöntemdir (Dülger, 2004). Teknik, çok fazla kaynaktan (örneğin banka hesabı) kaynak başına fark edilemeyecek kadar küçük miktarlarda gelirin başka bir kaynakta toplanması esasına dayanır. Bu tekniğin kullanımında en sıklıkla uygulanan matematiksel işlem, yuvarlama işleminin failin yararına olacak şekilde ayarlanmasıdır. Bu şekilde yapılan operasyonu hem mağdurların hem de denetçilerin tespit etmesi güçleşmektedir.

Bu teknik; truva atı, sisteme sızma gibi diğer bilişim suçu teknikleri ile birlikte kullanılmakla birlikte daha çok sisteme erişim yetkisi bulunan kurum personeli tarafından yazılımlara yapılan yetkisiz müdahalelerle gerçekleşmektedir.

1.3.2.10. İstem Dışı Alınan (SPAM) Elektronik Postalar

Telefon, faks gibi iletişim vasıtalarına ilave ve alternatif olarak elektronik posta hizmetlerinin yaygın olarak kullanılmaya başlanmasıyla; istem dışı elektronik posta, bilişim hizmetlerini engelleyen büyük bir sorun haline gelmiştir.

Bir gıda firmasının ürünleri için kullandığı bir kısaltma olarak ortaya çıkan SPAM (spiced pork and ham) kavramı, uluslararası Ticaret Örgütünün 1996 yılında yayınlamış olduğu etkileşimli pazarlama iletişimi konusundaki ICC yönergesinde, “ticari amaç taşımayan forum kuraları ile ilgili olmayan ve gönderilmesine açıkça izin verilmeyen reklam” olarak tanımlanmaktadır.

Artan iletişim trafiğinin önemli nedenlerinden birini oluşturan istem dışı elektronik postaların göndereni belli değildir veya sahtedir. Bu tür elektronik

postalar kullanılarak, kullanıcıların burada bahsedilen diğer tekniklere yönlendirilmesi sıklıkla yaşanan bir durumdur. Ayrıca tekniğin uygulanabilmesi için gerekli elektronik posta adresleri içerdikleri kullanıcı sayısına paralel değer bularak yasadışı olarak pazarlanmaktadır.

Ülkemizde bu konu ile ilgili yasal bir düzenleme devam etmektedir. Uluslararası alanda gittikçe önemli bir sorun haline gelen bu uygulamanın engellenmesi için ülke hukuklarında sert tedbirler alınmaya başlamıştır.

1.3.2.11. SSL/SSH Saldırıları

Bankacılık sektörünün maliyetlerinin azaltılması ve müşterilerine daha iyi hizmet vermeleri maksadıyla hayata geçirdikleri internet bankacılığı kavramı güvenlik ihtiyaçlarının daha da artmasına neden olmuştur. İnternetin saldırıya açık olan bir ortam olması nedeniyle ilave güvenlik teknikleriyle verilen hizmetin güvenliği azami seviyeye çıkarılmaya çalışılmaktadır. SSL (Secure Socket Layer) yani güvenli soket katmanı tekniği, bir takım şifreleme algoritmaları ile ağ bağlantısının daha güvenli hale getirilmesini amaçlayan bir teknolojidir (Yılmaz, 2005).

Bağlantının SSL gibi bir teknoloji ile güvenli hale getirilmesi bile saldırı ihtimalini sıfıra indirememiştir. SSL teknolojisi, internet üzerinde bankacılık işlemini yapmak istendiğinde banka bilişim sisteminin kullanıcıya bir elektronik sertifika göndermesi ve her işlemin yetkili bir sertifika otoritesi tarafından onaylanmış bu sertifika ile eşliğinde onaylanarak gerçekleşmesi esasına dayanmaktadır.

İnternet tarayıcısı bu sertifikayı gördüğünde bunu kabul edip etmemeyi kullanıcıya sormaktadır. Bu saldırı tekniği basit olarak fail, kişisel bilgisayarda tespit ettiği bir elektronik imzayı kendi kontrolünde yeniden üreterek banka bilişim sistemine bunu onaylatmakta daha sonra kullanıcıya bu en başta

yapılmış olan onayı tekrarlatmaktadır. Kullanıcıların aslında onayı bir kez yapmış olmalarına dikkat etmeden tekrar onaylamaları tüm denetimi faile geçirmektedir. Bu sayede kullanıcının tüm bankacılık işlemleri failin çıkarına göre gerçekleşmektedir.

SSH (Secure Shell) teknolojisi, SSL teknolojisinin LINUX işletim sistemindeki adıdır. SSH saldırısı da mantık olarak SSL saldırı tekniğinin benzer işlem adımlarına sahiptir.

1.3.2.12. Sistem Kaynaklarını Tüketme Yöntemi

Bilişim sisteminin çalışmasını kasten engellemek maksadıyla yaygın olarak kullanılan bir yöntemdir. Bilişim korsanının amacı sistemi çökertmek veya kullanıcıların bilişim sisteminin kaynaklarına ulaşmasını engellemek olabilmektedir.

DoS (Denail of Services), DDos (Distributed Denial of Services), SYN seli, ping of death, smurf saldırıları bu teknik kapsamında değerlendirilen saldırılardır. Bu tekniklerin ortak amacı bilgisayar ağ iletişimini durdurmaktır.

Bu konu kapsamında değerlendirilebilecek bir diğer özel saldırı türü ise tampon bellek taşması saldırısıdır. Bu saldırı, genellikle çalışan yazılımlarda hata kontrolü konusundaki zafiyetlerin kullanılması esasına dayanır. Normalde bir programın hata ile karşılaştığında durması beklenir. Ancak yazılım firmaları programların her şartta çalıştığını ispat için programı hataya düşse de çalışacak şekilde tasarlarlar. Programın her hataya düştüğünde bellekten yer kaplaması açığını kullanan bilişim korsanı, sistemin çalışmasına engel olana kadar aynı hatanın tekrarlanmasını sağlayarak amacına ulaşır.

1.3.2.13. WEB Saldırıları

WEB saldırıları, kullanıcılar tarafından birebir en sık karşılaşılan ve en popüler yöntemdir. Modern yaşamın sanal tezahürü halinde algılanagelen internetin yaygınlaşmasıyla, bu devasa ağda hizmet veren her bir uç bir site olarak nitelenmiştir. Bu sitelerin sanal dünyaya açılan penceresi ise WEB sayfaları olmuştur.

Günümüzde bilişim korsanlığını iş edinen kişilerin çoğu bir WEB sitesini ele geçirmeyi/çökertmeyi/haklamayı (hacking) bir başarı olarak görmektedir. Bu teknik aslında daha önce bahsedilen tekniklerin birlikte kullanımından ibarettir. Tek farkı hedef bir bilgisayar sitemine girmek değil, bilgisayar sitemi üzerinde hizmet veren web sayfasına (bir tür yazılım) girmektir.

Maddi kazanç sağlamak her saldırı tekniğinin önemli amaçlarından biridir. Ancak bu tekniğin kullanımında tek önemli neden değildir. WEB saldırıları popüler olmak, kişisel ve toplumsal değerleri korumak veya intikam gibi önemli manevi tatmin nedenlerini de içermektedir. Fail tarafından saldırının belgelenmesi ve tanıtıcı bir imzanın bırakılması bu tür saldırılarda sıklıkla görülen bir durumdur.

Sonuçları itibarıyla da kamuoyu bağlamında en dikkat çekici, ulaşılabilir ve yönlendirici etkiye sahip saldırı türleridir.

1.3.2.14. WEB Sayfası Yönlendirme

Web sayfası yönlendirme tekniği, hizmet beklenen site yerine bilişim korsanları tarafından hazırlanan ve gerçeği ile birebir aynı başka bir siteye kullanıcının isteği dışında ve fark ettirilmeden yönlendirilmesi esasına dayanmaktadır.

Bu teknikle şifre ve kişisel bilgilerin sorulduğu siteler için uygulanmakta, daha sonra bilişim korsanları elde ettikleri bilgilere göre gerçek sitelerde yasadışı eylemlerde bulunmaktadır.

İnternet dünyasında izlenme oranı siteye giriş sayısı ile ölçülmektedir. Bu ölçüm sonuçlarına göre siteler reklam verenler tarafından takip edilerek çok izlenen sitelere reklam vermektedirler. Çok masum bir amaçla da olsa, kullanıcıların isteği dışında bazen girilmek istenen site ile beraber başka WEB sayfalarının otomatik olarak açılması sağlanabilmektedir. Linking adı verilen bu otomatik WEB sayfası açma tekniğinin kullanımı her zaman bu kadar masum amaçlara dayanmamaktadır. Sahtecilik amacıyla ve özellikle pornografi içeren sitelerin otomatik açılan WEB sayfaları hukuki sonuçlara yol açabilmektedir. İnternet ortamında pornografiye, özellikle de çocuk pornografisine karşı yürütülen uluslararası mücadelenin yoğun yaşandığı günümüzde; otomatik bağlantı (linking) marifetiyle masum insanların bu sitelerin müdavimi gibi gösterilmesine neden olabilecektir. Bu durumla karşı karşıya kalan kişilerin toplumsal, hukuki, mesleki ve ailevi yönden uğrayacağı zararların telafisi mümkün olmamaktadır.

1.3.2.15. Veritabanı Saldırıları

Sanal ortamda pek çok WEB sayfası gerek kendi kullandığı verileri gerekse kullanıcılarından topladığı verileri tutmak için veritabanları kullanır. Veritabanı saldırısı tekniği, veritabanı kullanan bir sayfada yazılımın güvenlik açıkları nedeniyle veri tabanını kullanılamaz hale getirerek WEB sayfasının hizmetini engelleme esasına göre çalışır.

1.3.2.16. Hukuka Aykırı İçerik

Bilişim ve iletişim sistemleri kullanılarak hukuka aykırı içeriğin başka kullanıcıların erişimine sunulmasını ifade etmektedir. Bölücü, ırkçı, şiddeti teşvik eden, kişilik haklarına tecavüz eden veya çocuk pornografisi ile ilgili içerik bu kapsamda değerlendirilmelidir. Hukukun, basın ve yayın organlarına getirdiği yasaklar ve kısıtlamalara internet ortamı da tabidir.

Bu değerlendirmenin sadece WEB sayfaları için geçerli olduğu görüşü yanlıştır. Bahsi geçen hukuka aykırı içeriğe sahip olan elektronik posta ve bilgisayar oyunları da bu kapsamda değerlendirilmelidir.

Henüz sıklıkla karşılaşılmayan sorunlardan bir tanesi de kişisel verilerin hukuka aykırı kullanımı veya paylaşımında yaşanabilecek sıkıntılardır. Bilişim sistemlerinin her alanda kullanımının artması her konuda veri depolanması ve işlenmesi sonucunu ortaya koymuştur. Kredi kartları ve alışveriş kartları için kayıt altına alınan veya türlü hizmetlerin sağlanması için kişi ve kuruluşlara verilen bilgilerin zaman içinde hukuk dışı faaliyetler için kullanılıp kullanılmadığı ayrı bir sorun teşkil edecektir.

1.3.2.17. Fikri Mülkiyet Haklarını İhlal

5846 sayılı Fikir ve Sanat Eserleri Kanunu, kişilerin emek sarf ederek ortaya çıkardığı düşün ve sanat ürünlerini eser kavramıyla tanımıştır. İlgili kanunda; 07 Haziran 1995 tarih ve 4110 sayılık kanunla yapılan düzenleme ile bilişim yazılımlarının da eser kavramı kapsamında sayılması benimsenmiştir (Dülger, 2004).

Yasanın değişme gerekçesi “bilgisayar program teknolojisi ülkemiz endüstriyel gelişimi için temel öneme sahip bir konu haline gelmektedir. Bir bilgisayar programı gerçekleştirmek için insan gücüne, teknik ve mali yatırıma

ihtiyaç vardır. Buna karşılık ortaya çıkan programın haksız kopyalanması çok kolay ve çok az maliyetle yapılmaktadır. Bu durum bilgisayar programlarının fikri haklarının çok iyi korunmasını gerektirmektedir" olarak gösterilmiştir. (Türkekul, 2004).

Eser kapsamında değerlendirilen yazılım ürünlerinin kopyalanması ve her hangi bir telif/lisans bedeli ödenmeden kullanılması bilişim sektörünün en önemli sorunlarından biridir. Bu konuda yazılım şirketleri yazılımların kopyalanamaması üzerinde ayrıca çalışmaktadır. Ancak sanal dünyanın karanlık karakterleri çoğunlukla bu teknikleri aşan başka yöntemler icat etmektedir.

Fikri mülkiyet haklarının ihlalini oluşturan hukuki ihtilafların, önümüzdeki dönemde artarak devam edeceği gözlenmektedir. Çünkü sınırsız paylaşım anlayışı üzerine inşa edildiği iddia edilen internetin, bu hakların korunmasındaki yeri, rolü ve önemi halen sonuca bağlanmamış bir konudur.

1.4. Delil Kavramı

Sözcük anlamı ile delil, yol gösteren anlamına gelmektedir. Yargılama hukuku açısından delil, uyuşmazlık konusu vakıanın gerçekleşip gerçekleşmediği konusunda mahkeme heyetinde bir kanı oluşturmaya yarayan ispat aracıdır.

Bir hukuki ihtilafı çözmeye veya suç fiilini ispata yarayan ve ikamesi hukuk tarafından yasaklanmamış her şeye (canlı-cansız, yazılı-sözlü) **delil veya ispat vasıtaları** denilmektedir. Ceza yargılamasında gerçeğin bulunmasına yardımcı araçlar olarak deliller oluşturacaktır (Yurtcan, 1996, s.46).

Delil, suç tespitine yarayan her türlü ispat vasıtası, bir hukuki ihtilafı çözmeye yarayan ve ikamesi hukuk tarafından yasaklanmamış her şey (Kaygısız, 2003, s.14), bir hukuki ihtilafı ispata yarayan bilgi ve bulgular (Şafak, 1992, s.94), dava konusu olayın gerçekliğini ortaya koyan araç, kanıt (Bağdatlı, 1995, s.535) uyuşmazlık konusu olayı temsil eden, akla, maddi gerçeği ve hukuka uygun her türlü ispat vasıtası (Toroslu, 2003, s.160) gibi tanımlamalara da tabi tutulmuştur.

Ceza muhakemesinde fiilin fail tarafından işlendiği veya işlenmediği konusunda hukuk düzenince kabul edilen vasıtalarla yargılama makamının tam bir kanaate ulaşmasını temin ameliyesine ispat; ispat ameliyesinde kullanılan hukuk düzeninin kabul ettiği vasıtalara delil denir (Öztürk ve Erdem, 2006).

Ceza uyuşmazlıklarında iki bölüm vardır. Birincisi eylemin kişi tarafından yapıldığının veya yapılmadığının ortaya çıkarılması bölümü, ikincisi de fiilin hukuk kuralları içinde değerlendirildiği (Yurtcan, 2002, s.46) ve maddi gerçeğin kesinlik kazanması halinde hukuki gerçeğin bulunmaya çalışıldığı, fiilin suç olup olmadığının ve suç teşkil ediyorsa hangi suçu teşkil ettiğinin ortaya konulduğu bölümdür. Mahkeme esas hakkında meseleyi doğrudan delillerle temasa geçerek araştırıp, öğrenerek vicdani kanaate ulaşır ve karar verir (Cihan ve Yenisey, 1998).

İspat, fiilin maddi yönünün aydınlatılması için yapıldığından fiilin maddi yönüyle ilgili olguların tek tek aydınlatılması (*yer, zaman, oluş biçimi, nedeni, suç eşyası, hedefi, fail, meydana gelen zararlar*) gereklidir (Yurtcan, 2002, s.46). Hâkim maddi gerçeği bulmaya çalışırken, eylemin maddi yönüyle ilgili tüm olguların deliller vasıtasıyla ispatını arayacaktır.

Maddi gerçeğin re'sen araştırılması ilkesi gereğince mahkeme ulaşabileceği bütün delilleri kullanmak durumundadır. Ancak, demokratik

hukuk devleti ilkesi, maddi gerçeğin araştırılması prensibini sınırlar. Devlet kendisi hukuka aykırılık yaparak, delil toplayamaz (Yenisey, 2006, s.36).

Delil yasakları, delilleri elde etmeyi yasaklayan kurallar ile delilleri değerlendirme sırasında uygulanan yasaklar olmak üzere iki bölümde incelenir.

Delil elde etme yasakları, kanun koyucunun önceden belli tür delillerin elde edilmesini yasaklaması fikrine dayanır. Bazı deliller konuları itibariyle, bazı delillerin elde ediliş yöntemi nedeniyle yasaklanmış olup bazı delil türlerinin ise önceden elde edilmesi yasaklanmıştır. Örneğin, aldatma yasaktır. Şüphelinin özgür iradesini ortadan kaldıracak şekilde bir hataya düşürülerek, mesela mevcut olmayan bir olgunun varmış gibi gösterilmesi veya içinde bulunduğu hukuki durumun gerçeği yansıtmayacak bir şekilde ona anlatılması gibi hallerde aldatma vardır. Bugün geçerli olan hukuki mevzuatımız beden muayenesi bakımından (CMK, m.75) ve telefon dinleme açısından (CMK, m.135) ilave delil yasakları yaratmıştır (Yenisey, 2006).

Delil değerlendirme yasağı, elde edilmiş bulunan belli bir delilin duruşmada ortaya konulmasının ve daha sonra da hüküm verilirken kullanılmasının yasaklanması anlamını taşır. Eğer delil elde edilirken hukuka aykırılıklar yapılmışsa, bu takdirde bu delilin hüküm verilirken kullanılıp kullanılmayacağı, mahkeme tarafından takdiren değerlendirilir. Örneğin, yasak sorgu yöntemleri (CMK, m.148), iletişimin dinlenmesinden sonra kayıtların yok edilmesi mecburiyeti (CMK, m.135) ve beden muayenesinden elde edilen kişisel verilerin sonradan yok edilmesi (CMK, m.75) gibi delil değerlendirme yasaklarında, kanun koyucu, o delilin hiç bir zaman kullanılamayacağını açıkça ifade etmiştir. Buna karşılık, delil elde edilirken yapılan diğer hukuka aykırılıklar açısından, kanunda açık bir düzenleme yer almamaktadır. Bu nedenle, “delil elde etme yasakları konusundaki her ihlalin, elde edilen delilin hüküm verilirken kullanılmasını yasaklamadığına” dikkat edilmelidir. Bu gibi hallerde mahkemenin somut olayda delili kullanıp

kullanmama konusunda takdir yetkisi bulunduğu kabul edilmelidir (Yenisey, 2006).

Olay yerinde tespit edilen deliller, hazırlık soruşturmasında suçun ve suçlunun tespit edilip yakalanmasını, mahkeme aşamasında bu verilere dayanılarak suçun aydınlatılmasını, masumların aklanmasını, suçluların ceza almasını ve hukuki ihtilafın çözümlenmesini sağlamak için önemlidir.

1.4.1. Delil Özellikleri

Günümüz ceza muhakemesinde geçerli olan ispat sistemi, vicdani delil sistemidir (Kunter ve Yenisey, 2003). Temel özelliği, her şeyin delil kabul edilmesi ve delillerin de serbestçe değerlendirilmesi olan vicdani delil sistemi (T.C. Anayasası, m.138); mahkûmiyet için tam bir inanış, başka bir deyişle suçluluk konusunda vicdani kanaat aradığından, esasen şüpheye dayalı cezalandırmayı yasaklamaktadır. Ceza Yargılamasında geçerli olan "Vicdani Delil Sistemi" gereği, hâkim maddi gerçeği ararken, hukuk hâkiminden farklı olarak tarafların ileri sürdüğü delillerle bağlı değildir. Hatta bu ilke gereği kanun bile bazı hususların belli delillerle ispat edilebileceğini öngörmemelidir. Yine vicdani delil sisteminin gereği olarak ceza yargılamasında her şey delil olabilmelidir ve bu şeyin delil olarak değerini hâkim serbestçe takdir edebilmelidir (Kunter ve Yenisey, 2003).

Anayasanın 38/4. ve Avrupa İnsan Hakları Sözleşmesinin 6/2. maddelerinde düzenlenmiş bulunan suçsuzluk ilkesi, suçluluğu hükmen sabit oluncaya kadar kişinin suçsuz sayılması gerektiğini ifade etmektedir. Bu karine uyarınca, suçsuz olduğu varsayılan kişinin suçlu kabul edilmesi için kesin hükümle mahkûm olması, mahkûmiyet için de fiilin ispatlanması, yani şüphenin bertaraf edilmesi gerektiğinden, ceza hâkimi sanığın leh ve aleyhinde ileri sürülen ispat araçlarının bütününün vicdanen incelemesinden

çıkan tam bir inanışla, özgürce ve ispat konusunda bir sınırlama olmaksızın vermelidir.

Suçların tek tek ele alınmasıyla bu suçlarda nelerin delil olarak kabul edilebileceği veya edilmesi gerektiği hakkında hüküm vermek mümkün değildir. Bu nedenle suç fiilini ispata yarayan olguların hukuk önünde delil sayılabilmesi için;

1. Delil olarak kullanılmak istenen vasıtanın olayın bir parçası olmalı ve/veya olayı yansıtmalıdır. Yani İspat için kullanılmak istenen bir vasıta olayı temsil etmelidir (Öztürk ve Erdem, 2006).

2. Bu olayı temsil eden vasıta akla, maddi gerçeğe ve hukuka uygun olmalıdır. Bir ispat aracına delil denilebilmesi için sadece olayı bir şekilde temsil etmesi ve/veya olayı yansıtması yetmemektedir. Akla, maddi gerçeğe ve hukuka uygun olmayan bir ispat aracı teknik anlamda delil olarak kabul edilmemektedir (Öztürk ve Erdem, 2006).

3. Karara gerekçe gösterilecekse müştereklik (tarafların bilmelerini) sağlanmalıdır. Nitekim mahkûmiyet hükmünün gerekçesinde delillerin tartışılması ve değerlendirilmesi gösterilmek durumundadır (CMK, m.230/1/b).

1.5. Olay Yeri İnceleme Kavramı

Doğa güçlerinin etkisiyle veya insan davranışları sonucunda ortaya çıkan, oluşan durum, ilgiyi çeken veya çekebilecek nitelikteki her türlü hadiseye olay denir (www.tdk.gov.tr). Bunlardan, sonuçta kendilerine hukuki bir müeyyide tanınanlara hukuki olay denir.

Olayın işleniş tarzının, mağdur ve suç sanıklarının ilişkisinin saptanabildiği dinamik bölgeye "olay yeri" denir. Olay yeri, olayın başlangıcı, takibi ve sonucunda geçtiği mekânları kapsar. Olayın işleniş tarzını, yöntemini, olayı işleyenlerin hareket tarzını, olaya ait iz ve bulguları içerir. Ayrıca olay yeri suçun işleniş şeklini, suçtan zarar gören mağdurları, suç sanıklarının olay karşısındaki sorumluluk derecelerini net olarak belirler.

Bir ortamı terk eden bir kişinin orada bulunduğuna dair iz bırakması, ya da üstünde o ortamdan bir şeyler alıp götürmemesi mümkün değildir. Olay yeri incelemesi ile elde edeceğimiz en önemli şey maddi delillerdir. Bu tür deliller şüphelinin aleyhine dilsiz birer tanıktır. İnsan tanıklarının varlığı bile onları yok edemez (Edmond Locard).

Olay yeri inceleme, suç delillerinin veya suça konu olabilecek suç eşyasının bulunması, suç-fail-mağdur-alan ilişkisinin belirlenmesi için yasa gereği yapılan arama ve tarama işlemleridir. Bir başka ifadeyle "olay yeri inceleme"; meydana gelen olaylarda incelemeler yaparak iz, eser, emare ve delil gibi suç unsurlarının bulunup bulunmadığını araştırma, varsa bunları bilimsel ve teknik yöntemler kullanarak tespit edip belgeleme, toplama, ambalajlama ve değerlendirmek üzere ilgili birimlere gönderme işlemine denilmektedir.

Olay yeri incelemesindeki temel amaç, maddi hakikate ulaşmada, işlenen suçun aydınlatılmasına veya hukuki ihtilafın çözümlenmesine katkıda bulunacak maddi delillerin bulunması, niteliğinin tespiti ve korunmasıdır. Mevzuat ve uygulamalara bakıldığında; olay yeri inceleme çalışmaları kolluk birimlerinin adli görevleri içerisinde yer almakta olup meydana gelen hukuki bir olayda, olay-fail-mağdur-mekân arasında ilişkiyi sağlayacak araştırma faaliyetini kapsayan hazırlık evresidir.

Olay yeri inceleme çalışmalarını yapan kolluk birimi, suçun işlenmesinden sonraki adli görevle ilgili görevi kapsamında fiile ve faile ilişkin

olarak suçun ve suçluların araştırılması, delillerin toplanıp korunması gibi işlemleri ifa etmektedir.

Olay yerindeki sessiz tanıkların bilimsel olarak konuşturulmasının (Kaygısız 2003) sağlanması için teknik ve hukuki olarak çalışan kolluğun, savcının emrinde ve koordineli bir şekilde olay yerlerinde çalışmaları gerekir. Çünkü bir suçla ilgili yargılama süreci içindeki olay yeri inceleme, kolluğun adli görev safhasında yer aldığından, amiri savcıdır.

Ceza Muhakemeleri Kanunu'nda Olay yeri incelenmesi ile ilgili ayrı ve açık bir hükme yer verilmemiş, bu konu Ceza Muhakemeleri Kanunu'ndaki arama ve el koyma ile ilgili düzenlemeler esas alınarak Adli ve Önleme Aramaları Yönetmeliği'nin 9. maddesinde düzenlenmiştir. Bu maddeye göre; suç işlenen konut, işyeri ve kamuya açık olmayan kapalı alanlarda, olay yeri inceleme işlemlerinin yapılabilmesi için hâkim veya gecikmesinde sakınca bulunan hallerde de Cumhuriyet savcısının yazılı emri gerekmektedir. Bu kural suçüstü durumlar ile şüphelinin talebi veya rızasının bulunması halinde bile geçerliliğini korumaktadır. Bu durum özellikle adliyenin bulunduğu merkezden uzak yerleşim birimlerinde işlenen suçlarda hâkim veya Cumhuriyet savcısından yazılı emir alınması için geçecek sürede delillerin yok edilmesi, bozulması veya gizlenmesine imkan vermekte, belki de şüphelinin lehine olabilecek delillerin toplanamaması sonucu şüphelinin haklarının yeterince korunamamasına yol açabilmektedir (TCK, m.160/2).

Olay yeri incelemenin asli maksadı delillerin kaybolmadan veya değiştirilmeden yani karartılmadan önce zaman kaybedilmeksizin toplanmasıdır. Buna karşın delil toplamanın tek yöntemi olay yeri inceleme değildir. Delil elde etme faaliyeti, olayın türü, olay yeri, fail, mağdur veya suçun nedeni gibi etkenlere göre çok farklı şekilde seyredebilir. Olayla ilgili bulunan olay yeri/yerleri ve yakın çevresi ile olayla ilgili kişilerin üst ve eşyalarında delil tespit edilebilir.

1.6. Delil Toplama Kavramı

Hukuk muhakeme hukukunda karar verme yetkisine haiz olan yetkililerin karar verebilmelerini temin için delillerin hazır bulundurulmasına delillerin toplanması denir (Öztürk ve Erdem, 2006).

Ceza Muhakemesi soruşturma evresi ve kovuşturma evresi olmak üzere iki evreye bölünmüştür. Soruşturma evresi savcı tarafından yürütülen bir öğrenme muhakemesidir. Savcı, "***re'sen araştırma ilkesi***" gereğince, suç işlendiği izlenimi veren hal varsa, kendiliğinden gerekli araştırmalara başlamaya mecburdur. "***Suç izlendiği izlenimi veren hal***" ve "***araştırmak için harekete geçme***" birleştiğinde, "***soruşturma evresi***" başlamış olur (Yenisey, 2006).

Soruşturma evresinin başlayabilmesi için, ihbar veya şikâyet üzerine veya kovuşturma makamlarının kendiliğinden, "***bir suç işlendiği izlenimi veren hali***", öğrenmeleri gerekir. İhbar, herkesin savcılık veya polise suç ile ilgili bir bilgi vermesi demektir (CMK, m.158). Savcı, ihbar veya şikâyet dışında kendiliğinden "suç işlendiği izlenimi veren bir hal" bulunduğunu öğrenirse, araştırma ve soruşturmayı böylece de başlatır (CMK, m.160/1) (Yenisey, 2006).

Alman Hukukunda ve mülga CMUK 'nda polise kendiliğinden acele hallerde araştırma yapma yetkisi verilmişken (CMUK, m.156), Yeni Kanun kolluğun suça el koymasını, kişileri yakalamasını ve tedbir uygulamasını kabul etmiş, fakat araştırma yapma yetkisi vermemiştir (CMK, m.161/2) (Yenisey, 2006).

Cumhuriyet Savcısı, maddi gerçeğin araştırılması ve adil bir yargılamanın yapılabilmesi için, şüphelinin lehine ve aleyhine olan delilleri toplayarak, muhafaza altına almakla ve şüphelinin haklarını korumakla

yükümlüdür (CMK, m.160/2). Bu araştırmaları kendisi yapabileceği gibi, emrindeki adli kolluk görevlilerine yaptırabilir (Yenisey, 2006).

Deliller, yeni CMK esaslarına göre sadece soruşturma evresinde toplanacaktır. Yeni sistemde mahkeme delil toplamayacaktır. Sonradan ortaya çıkan bir delil olursa mahkeme bunu savcılık marifetiyle elde edecektir (Öztürk ve Erdem, 2006).

Yeni CMK savcı merkezli bir kanun olduğundan soruşturma evresinde tüm kararları ve emirleri savcılık makamı verecek; kolluk bu karar ve emirleri yerine getirecektir (Öztürk ve Erdem, 2006).

"***Suç işlenmesi***", toplum için bir tehlike yarattığı için, belli fiiller suç haline getirilmiştir. "***Tehlikeyi önlemek***", yani suç işlenmesini önlemek, kolluk kuvveti görevidir. Suçun işlendiği, "***bu izlenimi veren haller***" mevcut olduğu için (CMK, m.160/1), yani başlangıç şüphesi oluşmuşsa, iş artık C. savcısının hâkimiyeti altına girmiştir. Fakat henüz suç işlendiğini gösteren "***somut olgular***" yoksa ve bunların araştırma yapılarak var olup olmadıkları tespit edilecekse, yani "***suç işlendiği tehlikesi***" varsa, bu tehlikeyi önlemek ve bastırmak kolluk kuvveti görevi olduğu için, bu incelemelerin kolluk kuvveti tarafından kendiliğinden yapılması, kolluk kuvveti hukukundan kaynaklanan bir görevdir.

Savcının "***soruşturma evresindeki***" araştırma yükümü ile, mahkemenin "***kovuşturma evresindeki***" araştırma yükümünün kapsamı farklıdır. Cumhuriyet savcısı kamu davasını açıp açmamağa karar vermeğe yetecek kadar araştırma yaparken, mahkeme vicdani kanaate ulaşmak amacı ile, çok daha geniş kapsamlı bir araştırma yapmak mecburiyetindedir (Yenisey, 2006).

Mahkemenin kovuşturma evresinde yaptığı araştırma, delillerin duruşma salonunda ortaya konması yolu ile gerçekleştirilir. Mahkemenin

çözmesi gereken usul hukuku sorunları, esas hakkında vereceği hüküm bakımından önemli olan ve maddi meseleyi oluşturan “olgular” ile “tecrübe kaideleri” mahkeme tarafından re’sen araştırılır.

Medeni yargılama usulünde ise dava malzemesinin taraflarca hazırlanması ilkesi geçerlidir. Deliller dava dilekçesinde veya cevap dilekçesine ek olarak mahkemeye sunulmaktadır. Bunlar dışında mahkemeye delil sunulmak isteniyorsa delillerin dâhil edilmesi hâkimin takdir yetkisine bırakılmıştır. Hâkimin sunulan yeni delillerin yargılamaya dâhil edilmesini uygun bulmaya yönelik karar vermesi durumunda, bu deliller incelemeye konu olabilecektir (HUMK, m.244). Hâkim tarafından re'sen araştırması gereken hususlar bu kapsamın dışında kalmaktadır. Hâkim davanın her safhasında iki tarafın iddiaları hududu dâhilinde olmak üzere kendilerini istimal ve lazım olan delillerin ibraz ve ikamesini emredebilir. (HMUK, m.75)

Ceza Muhakemesi Kanunu’nda delil toplama yöntemleri olay yeri inceleme ile sınırlı değildir. Delil toplama amacıyla da kullanılan koruma tedbirleri, ceza yargılamasını kolaylaştırmak maddi gerçeği ortaya çıkarmak ve yargılama sonunda verilen hükümlerin infaz edilememe olasılığını yok etmeye yönelik, kişilerin hak ve özgürlüklerine yönelik bir kısıtlamalardır. Bu önlemler; yakalama, tutuklama, arama, el koyma, beden muayenesi gibi delil toplama maksadıyla da ifa edilen adli işlemlerdir.

Soruşturma evresinde toplanan delillere göre, karar verme yetkisi bulunan savcı ya iddianame düzenler, ya da takipsizlik (kovuşturmama, kovuşturmaya yer olmadığı) kararı vererek işe son verir. Dava açıldığında, yine toplanan delillere dayanılarak kovuşturmada yetkili bulunan mahkeme heyeti ilgili kararları verirler. Yine toplanan delillere göre bir hüküm ile dava sona erer (Öztürk ve Erdem, 2006).

Konusu maddi gerçeği araştırmak olan ceza yargılamasında önce kolluk sonra da savcı bu görevi yerine getirmekle yükümlüdür. Kolluk delil

toplanmasına ilişkin faaliyeti savcılığın emri üzerine gerçekleştirebileceği gibi, herhangi bir suçla karşılaştıkları ya da suç haberini aldıklarında kendiliğinden de gerçekleşebilir.

Burada hassasiyetle üzerinde durulması gereken husus, savcıların veya kolluk görevlileri sadece sanığın aleyhine olan delilleri değil lehine olan delilleri de araştırıp bulma yükümlülüğünün olduğudur. Delil toplamanın gayesi suçluyu ortaya çıkarmak olduğu kadar masumun hatalı şekilde suçlanmasını önlemektir.

1.7. Bilirkişi Kavramı

Bilirkişi, sahip bulunduğu teknik veya özel bilgisini kullanarak, mahkemeyi maddi mesele ile ilgili bir delil hakkında aydınlatmakla görevlidir. Hâkim veya soruşturma safhasında savcının uygun göreceği kişi veya kurumlar bilirkişi olarak görevlendirilmektedir.

Adlî bilimlerin temel amacı işkence ve kötü muameleyi önleyerek, suçu aydınlatmak ve suçluyu ele geçirmektir. Günümüzde delilden suça ve suçluya gitmek demokrasisi gelişmiş hukuk devletlerinin vazgeçilmezleri arasındadır. Bu kapsamda 5271 sayılı Ceza Muhakemesi Kanunu (CMK) ve Ceza Muhakemesi Kanununa Göre İl Adlî Yargı Adalet Komisyonlarınca Bilirkişi Listelerinin Düzenlenmesi Hakkında Yönetmelik, 1086 sayılı Hukuk Usulü Muhakemeleri Kanunu (HUMK) ile bilirkişilik müessesesini yasal bir zemine oturtmuştur.

Çözümü uzmanlığı, özel veya teknik bilgiyi gerektiren hâllerde bilirkişinin oy ve görüşünün alınmasına re'sen, Cumhuriyet savcısının, katılanın, vekilinin, şüphelinin veya sanığın, müdafiinin veya kanunî temsilcinin istemi üzerine karar verilebilir. Ancak hâkimlik mesleğinin gerektirdiği genel ve hukukî bilgi ile çözülmesi olanaklı konularda bilirkişi

dinlenemez (CMK, m.63/1). Bilirkişi atanması ve gerekçe gösterilerek sayısının birden çok olarak saptanması yetkisi hâkim veya mahkemeye aittir. (CMK, m.63/2). Soruşturma evresinde Cumhuriyet savcısı da bu maddede gösterilen yetkileri kullanabilir (CMK, m.63/3).

Bilirkişiye inceleyeceği şeyler mühür altında verilmeden önce bunların listesi ve sayımı yapılır. Bu hususlar bir tutanakla belirlenir. Bilirkişi, mühürlerin açılmasını ve yeniden konulmasını yine tutanakla belirtmek ve bir liste düzenlemekle yükümlüdür (CMK, m.66/6).

İncelemeleri sona erdiğinde bilirkişi yaptığı işlemleri ve vardığı sonuçları açıklayan bir raporu, kendisinden istenen incelemeleri yaptığını ayrıca belirterek, imzalayıp ilgili mercie verir veya gönderir. Mühür altındaki şeyler de ilgili mercie verilir veya gönderilir ve bu husus bir tutanağa bağlanır (CMK, m.67/1).

Birden çok atanmış bilirkişiler değişik görüşleri yansıtmışlarsa veya bunların ortak sonuçlar üzerinde farklı görüşleri varsa, bu durumu gerekçeleri ile birlikte rapora yazarlar (CMK, m.67/2).

Bilirkişi raporunda, hâkim tarafından yapılması gereken hukukî değerlendirmelerde bulunulamaz (CMK, m.67/3).

Cumhuriyet savcısı, katılan, vekili, şüpheli veya sanık, müdafii veya kanunî temsilci, yargılama konusu olayla ilgili olarak veya bilirkişi raporunun hazırlanmasında değerlendirilmek üzere ya da bilirkişi raporu hakkında, uzmanından bilimsel mütalâa alabilirler (CMK, m.67/6).

Ülkemizde, bilişim teknolojileri ile ilgili bilirkişilik görevlerinin icrasına yönelik, hukuk sistemimizde yetkilendirilmiş bir birim henüz mevcut değildir. Daha çok operasyonel birimlerle birlikte çalışan, ikiz görev olarak da gerektiğinde adli bilişim hizmetlerini yürüten değişik isimlerle kurulmuş

birimler mevcuttur. Standart ve yetkin bir eğitime sahip olunmadan, asli görevlerinin ifasına katkı sağlamak maksadıyla yürütülen ilave bir faaliyet olarak görülmektedir. Bu eksiklikten dolayı bilişim cihazlarındaki potansiyel yasal delillerin elde edilmesi ve değerlendirilmesi konusunda üniversiteler ve bazı ticari kuruluşlara bilirkişi olarak başvurulmaktadır.

1.8. Adli Bilişim Kavramı

Suç mahallinde delillerin bulunup, tespitinin yapılıp, güvenliğinin alınmasından sonra en önemli konu olayın aydınlatılmasına yardımcı olacak şekilde bu delillerin adli incelemesinin yapılmasıdır (Kaygısız ve Yılmaz, 2004).

Olay yeri inceleme görevlileri ve uzmanları, olay yerinin inceleme ve araştırmasının yapılmasını, soruşturma görevlileri ile koordineli çalışmak, delilleri belirlemek, tespit etmek, korumaya almak, ön değerlendirmeleri yapmak ve ilgili yerlere intikalini sağlamakla görevlerini icra ederler. Söz konusu görevliler, hangi olaylarda nelerin delil olabileceğini bilen, bu konuda eğitimleri tamamlanmış ve laboratuvarlardan ne gibi çalışma isteyeceğini bilen kişiler olmalıdır.

Olay yerinde bulunan delilleri, niteliklerine uygun bilim alanlarının verilerine göre laboratuvar ortamında inceleyip bilimsel ve teknik sonuçlar çıkarabilen gerekli teknik ve hukuki bilgiye sahip uzmanlar kriminalistik uzmanları olarak nitelendirilmektedir (Öztürk C., 2006). Bu uzmanlar aynı zamanda gerektiğinde olay yerinde bulunup olay yeri inceleme görevlerini üstlenmek, delillerin ön değerlendirmesini yapmak veya olay yeri inceleme görevlilerine danışmanlık yapmakla görevlidirler (Kaygısız ve Yılmaz, 2004).

Bilişim cihazlarındaki potansiyel yasal delillerin elde edilmesi maksadıyla bilgisayar inceleme ve analiz teknikleri kullanılarak yapılan

kriminalistik uygulaması şeklinde tanımlanan adli bilişim uzmanlık dalı, bilişim cihazlarını incelemek, veriler üzerinde arama yapmak, silinen verileri kurtarmak ve yapılan tüm işlemleri belgelemek görev ve sorumluluğuna sahiptir. Adli bilişim alanı; bilişim uzmanlığı, gelişmiş bir araştırma uzmanlığı ve yeterli hukuki birikimine sahip olmayı gerektiren bir disiplindir (Keser Berber, 2004).

Adli bilişim disiplinin iş akışı en temel anlatımla, "**delili bul, topla, işle, doğrula, yorumla, belgele, kullan**" şeklinde özetlenebilir. Aynı zamanda bu disiplinin görevlerini de anlatan bu özet, adli bilişim konusunda görev yapan tüm personel tarafından bilinmesi gereken en temel kural olmalıdır.

1.9. Sayısal Delil Kavramı

Bilginin fiziksel ortamdan elektronik ortama taşınmasıyla sanal ortamda yapılan işlemler bakımından karşımıza çıkan en önemli sorun ispat sorunu ve bilişim verilerinin delil sayılıp sayılmayacağı hususudur. Bilgi veya bilişim teknolojilerinin kapsam itibarıyla kişilerin ve kurumların mevcudiyetlerini etkileyecek boyutlara ulaşması hukukun bu bilgileri kullanma ihtiyacını zorunlu hale getirmiştir. Bu acil ve yoğun ihtiyaç, sayısal delillerin yeter ve gerek şartlarını vakit kaybedilmeksizin oluşturulmasını zorunlu kılmaktadır.

Sayısal delil kavramının bilişim teknolojilerinin kullanımından ortaya çıkan doğal bir sonuç olduğu yaklaşımı doğrudur. Ancak buna paralel olarak sadece bilişim veya bilgisayar suçları ile ilişkili olduğu eksik bir düşüncedir. Sayısal delil kavramının hukuki olarak taşıdığı anlam herhangi bir maddi delilden farklı değildir. Bu konuda fark yaratan unsur, delilin araştırma, tespit ve delillendirme yöntemlerinin farklı olmasıdır. Yani nitelik olarak değil nicelik olarak bir ayrıma gidilebilir.

Bilişim cihazlarından elde edilen delillerin isimlendirilmesinde bile ulusal veya uluslar arası bir standart mevcut değildir. Yaygın olarak sayısal delil, dijital delil, elektronik delil veya bilişim delili şeklinde isimlendirilmektedir.

Sayısal delil bir bilişim suçu ile ilgili, dijital biçimde kayıt edilen veya aktarılan bilgiler olarak tarif edilmiştir (Shinder 2002). Bu tarifteki en temel eksiklik konunun sadece bilişim suçları açısından ele alınmış olmasıdır.

Bir diğer tarifte ise bir suçun işlendiğini gösteren veya suç ile kurban ya da suç ile faili arasında bir ilişki sağlayan veriler şeklinde özetlenmiştir (Casey, 2004).

En yaygın ve kabul gören tarif ise bir suçun nasıl olduğunu veya suçtaki kritik elemanları adresleyen teorileri destekleyen veya çürüten, bilgisayar sistemleri kullanılarak kayıt edilen veya iletilen verilerin sayısal delil olduğu şeklinde ifade edilen görüştür (Chisum, 1999).

Sayısal deliller için yapılan tüm tariflerin ortak yönü elektronik ortamda kayıt edilmiş veya iletilmiş olması ve hukuki anlamda bir değer taşımasıdır.

Sayısal delil kavramı; bilişim teknolojisi içeren her türlü donanım, bu donanım üzerinde çalışan her türlü yazılım/yazılımlar tarafından kullanılan/üretilen her türlü veri ile bilişim teknolojisi tarafından kullanılan her türlü elektronik sinyali kapsamaktadır.

Sayısal delil kavramını incelerken dikkate alınması gereken diğer önemli bir husus ise bilişim ortamının suçta ve suç mahallinde kullanılma yöntemidir. Bilişim sistemi doğrudan suç işlemek için kullanılabildiği gibi suç izlerini içerebilmekte hatta suçun hedefi olabilmektedir.

Delilin sayısal hale gelmesi olay yeri kavramının da gelişmesine neden olmuştur. Olay yeri artık suçların işlenmiş olduğu yer, bilgisayar sistemleri

veya sayısal bilgi saklama ortamları, bilgisayar ağları ve internetin sanal sonsuzluğudur.

1.9.1. Sayısal Delillerin Hassasiyetleri

Sayısal deliller tıpkı DNA veya parmak izi araştırmalarında elde edilen sonuçlar gibi çoğunlukla ilk anda gözle görülmeyen birtakım özel cihaz ve yöntemlerle elde edilen delillerdir. Sınırları kolayca ve hızlı şekilde değişebilir. Kolayca değişebilir, tahrip edilebilir ve zamana karşı hassas yapıdadır. Bu nedenle bilişim delillerinin elde edilmesi muhtemel ortamlara, öncelikle genel geçerliliğe sahip olay yeri inceleme kurallarına göre müdahale edilmesi gereklidir. Ancak sayısal delillere müdahale edecek olan kişilerin bu amaçla eğitim almaları bir zorunluluktur. Sayısal deliller, normal delillere göre yapı itibariyle bazı hassasiyetleri barındırmaktadır (Keser Berber, 2004).

1. **Sayısal Delilin Bütünlüğü İlkesi:** Sayısal delillerin doğası gereği kolaylıkla kasti veya yanlışlıkla silinmesi, değiştirilmesi veya bozulması mümkündür. Bu nedenle öncelikle sayısal verilerin bütünlüğüne bir zarar gelmemesi önem taşımaktadır.

2. **Sayısal Delilin Doğrulanması İlkesi:** Sayısal delil ele geçtikten sonra adli süreç içinde söz konusu verilerin gerçekten o olaya veya şüpheliye ait olduğunun ispatı gerekmektedir. Fakat delil olarak ele geçirilen verilerin aynısı her hangi bir kişi tarafından da oluşturulabilir. Hatta şüpheli tarafından bu verilerin daha sonra, kolluk kuvveti tarafından oluşturulduğu bile iddia edilebilir. Soruşturma sürecinde sayısal verilerin olay veya şüpheliye ilişkisi teyit edilmelidir.

3. **Sayısal Delilin Doğruluğu İlkesi:** Sayısal delillendirme işlemindeki sayısal delilin kişisel veya kurumsal sahibi, onu ele geçiren kolluk birimi, delilin alındığı elektronik ortam, delilin ele geçirildiği zaman,

delilin içeriği gibi bütün unsurların doğruluğunun daha sonradan inkâr edilemeyecek şekilde belgelenmesi gereklidir.

4. **Sayısal Delilin İnkâr Edilemezliği İlkesi:** Sayısal delillerin ele geçirilmesi esnasında kullanılan teknikler ve kullanılan bilgilerin doğruluğunun gerektiğinde tüm adli süreç boyunca bütününde ispatı gereklidir.

5. **Sayısal Delilin Yeniden Ele Alınabilirliği İlkesi:** Sayısal deliller oluşturulduktan sonra, bu delilleri istendiğinde üçüncü bir şahıs inceleyebilmeli ve yeniden oluşturabilmelidir.

Elde edilen sayısal delilin olay, şüpheli veya diğer bir bilgi ile olan ilişkisini olayın tüm taraflarınca şüpheye mahal bırakmayacak şekilde kurmak hem bilişim teknolojileri hem de adli bilimler konusunda uzman olmayı gerektirmektedir.

Sayısal delillerin orijinal hali ile muhafazası ve yapılan tüm teknik işlemlerin ayrıntılı olarak raporlanması ve kişisel yorumlar yerine teknik bilgi temelli değerlendirmelerin yapılması hukuki açıdan geçerli bir delil sayılmasında etkilidir.

Sayısal deliller, klasik delil toplama yöntemlerine göre de hassasiyetler barındırmaktadır:

1. Klasik suçlarda sanığın, çoğunlukla suçun sonuç doğurduğu alana ya da mağdura fiziksel olarak teması söz konusudur. Bilişim ile ilgili suçlar, mekândan bağımsız olarak işlenebilir. Bu durum, delil toplamayı zorlaştıran önemli bir etkendir.

2. Klasik suçlardaki fiiller ve sonuçları çoğunlukla gözle görülebilir, elle tutulabilir. Bu niteliğinden dolayı da, suçun neticesinden, fiilin

aşamalarına ve başlangıcına gitmek ve sanığa ulaşmak kolaydır. Bilişim ile ilgili suçlarda fiiller ve sonuçları, sayısal yapıya ve elektronik alana dayalıdır. Bu nedenle fiilin aşamalarına, başlangıcına gitmek ve sanığa ulaşmak oldukça zordur.

3. Klasik suçlarda suçüstü söz konusu olabilir. 5271 sayılı Ceza Muhakemesi Kanunu'nun "Yakalama ve yakalanan kişi hakkında yapılacak işlemler" başlıklı 90. maddesine göre, herkes tarafından, suçu işlerken rastlanan ya da suçüstü bir fiilden dolayı izlenen ve kaçma olasılığı olan kişi, geçici olarak yakalanabilir. Bilişim ile ilgili suçlarda bu hükmün uygulanmasına hukuken bir engel yok ise de, yapısı nedeniyle uygulanabilme ihtimali sınırlıdır.

4. Klasik suçlarda deliller, başlangıçtan itibaren çoğunlukla maddi nitelikli, elle tutulabilen, işitilebilen, görülebilen, özellikler taşımaktadır. Bilişim ile ilgili suçlarda bu nitelikler ağırlıklı olarak bulunmamaktadır. Bilişim ile ilgili suçların delillendirmesinde temel sorun, kendisine özgü yapıdaki delilleri, yargılamada kullanılabilecek fiziki yapıya dönüştürebilmektir.

5. Klasik suçlarda delillerin elde edilmesi, saklanması ve ceza yargılaması sürecinde kolaylıkla incelenebilmesi mümkün olabilirken, bilişim ile ilgili suçlarda bu hususta sorunlar yaşanmaktadır.

6. Klasik suçlarda delillerin güvenilirliğini, bir başka ifadeyle şüpheden uzak olmasını sağlamak daha kolayken, bilişim ile ilgili suçlarda elde edilen delillerin şüpheden uzak olmasını sağlamak kolay değildir. Şüpheden arındırılmamış deliller ise, çoğu zaman sonuca etkili olamazlar.

7. Klasik suçlarda genellikle sınırları çizilebilen bir olay yeri mevcut iken bilişim ile ilgili suçlarda olay yeri kavramı teknolojik mutasyona uğrayarak belirsizleşmiştir.

1.9.2. Sayısal Delil Çeşitleri

Sayısal delillerin tasnifinde en yaygın yöntem, suç ile bilişim teknolojisi arasındaki ilişkiye göre yapılan tasniftir:

- Doğrudan bilişim suçu ile ilişkili sayısal deliller,
- Bilişim suçu kapsamına girmeyen suçların araştırmasında kullanılan sayısal deliller.

Sayısal delil araştırma ve tespiti için kullanılan yöntemler sadece mantıksal varlığına erişilebilir (silinmemiş veya hasar görmemiş) verilerle değil, silinmiş olan ancak fiziksel varlığını elektronik ortamda devam ettiren verilerin kurtarılması ve anlamlı hale getirilmesini de kapsamaktadır. Yani araştırma yöntemlerine göre sayısal delillerin tasnif edilmesi durumunda ise aşağıdaki tasnif kullanılabilir:

- Fiziksel ve mantıksal olarak var olan verilerin tespiti ve kıymetlendirilmesi,
- Silinen verilerin kurtarılması ve kıymetlendirilmesi,
- Elektronik izleme faaliyetleri ve kıymetlendirilmesi.

1.9.3. Sayısal Delil Özelinde Hukuki Mevzuat

Esas olarak sorunlar kâğıt yerine elektronik belge, iletişim için elektronik ortam ve işlerin kolaylaşması için bilişim sistemlerinin kullanılmasıyla başlamıştır. Bu yeni ortam ve felsefenin hukuka uygunluğu, güvenilirliği ve kurallarının belirginliği tüm hukuk sistemini etkileyen tartışmanın öncülüğünü yapmıştır.

Sayısal delil; hukuki süreç içinde kimi zaman veri, kimi zaman program, kimi zaman ise bilgisayar olarak karşımıza çıkmaktadır. Ancak isimlendirmede kullanılan bu geniş yelpaze niteliğini yani bilişim sistemi ve onunla ilgili her türlü materyal olduğu gerçeğini değiştirmemektedir.

Bilgisayar ve internet ortamında işlenen suçlar ile bilişim cihaz ve verilerinin delil olarak kullanıldığı suçlara ilişkin olarak soruşturma ve kovuşturma usullerinin yasalarda detaylı bir şekilde düzenlenmesi ve tüm usul işlemlerinin hâkim kararına bağlı kılınarak yargı denetiminde hukuksal güvenceye kavuşturulması amacıyla yasal mevzuata, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde aramaya ilişkin hükümler konulmuştur.

Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin haline getirilmesine hâkim tarafından karar verilir. (CMK, m.134/1)

Bilgisayar kayıtlarının incelenmesi ve bilgisayarlara el koyma Ceza Muhakemesi Kanunu ile düzenlenmiş bir konudur. Bir bilgisayar programında arama, kopyalama ya da el koyma tedbirinin uygulanabilmesi için kesinlikle hâkim kararına ihtiyaç vardır. Bu konuda bilgisayar, genel arama ve el

koyma hükümlerinden ayrılmıştır. Bu konudaki ikinci farklılık ise, soruşturmada başka surette delil elde etme imkânının bulunmaması gerekmektedir. Başka delillerle kanıtlama olanağı varsa bu yönteme başvurulamayacaktır.

Bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılabilmesi için bunları şüphelinin kullanıyor olması da aranan bir başka farklı noktadır. 3. kişilerin üzerlerinin veya eşyalarının aranması ile bunlara el konulması daha sıkı da olsa bazı şartlara tabi kılınarak mümkün kılınmış iken, bilgisayarlarda bu yol tamamen kapatılmış bulunmaktadır.

Ayrıca bu iki şart bulunsa bile, yapılabilecek işlemler kanunda sırayla belirtilmiş durumdadır. Hâkim buralarda, arama yapılmasına, kopya çıkarılmasına, kayıtların çözülerek metin hale getirilmesine karar verecektir. Bu tip verilerin içeriğinin her zaman değiştirilme olasılığının bulunması nedeniyle hem kopyalanıp hem metne dökülmesi daha yerinde olacaktır.

Bilgisayar ve bilgisayar programları ile bilgisayar kütüklerine kullanıcı tarafından şifre konulmuş olabilir ve bu şifrenin çözülmesi zaman alabilir. Hem kullanıcıyı şifreyi çözmeye zorlama hem de şifreyi çözmek ve gerekli kopyaları almak için bu araç ve gereçlere el konulabilir. Amaca ulaşılması halinde el koyma kararı sona erecek yani şifreler kırılıp, kopyalar alındıktan sonra bu araç ve gereçler iade edilecektir. Ancak her halde bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde bir şifre bulunmaması halinde veya çözümü kolay ise bunlara el konulmadan kopyalarının alınıp, yazdırılıp, tutanağa geçirilmesi gerekmektedir.

Yerinde olarak bilgisayar ve kütüklerine el koyma işlemi sırasında sistemdeki bütün verilerin yedeklemesinin yapılacağı düzenlenmiştir. Hatta istemesi durumunda bu yedekten bir kopya çıkarılarak şüpheli veya vekiline verileceği kaleme alınmıştır. Zira yukarıda belirttiğim üzere bu kayıtların değiştirilmesi her zaman mümkündür ve doğruluğu kesin değildir, bu yüzden

en son çare olmak zorundadırlar. Yine de bu husus göz önünde tutularak verilerin güvenilirliğinin arttırılması gerekmektedir.

5271 sayılı Türk Ceza Kanunu'nda bilişim ile ilgili suçlar kapsamında; "***hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçu***" 243. maddede, "***bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçu***" 244. maddede, "***banka veya kredi kartlarının kötüye kullanılması suçu***" 245. maddede, "***kişisel verilerin kaydedilmesi suçu***" 135. maddede, "***kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu***" 136. maddede, "***verilerin yok edilmemesi suçu***" 138. maddede, "***haberleşmenin engellenmesi suçu***" 124. maddede, "***haberleşmenin gizliliğini ihlal suçu***" 132. maddede düzenlenmiştir. Bu suçlara ilave olarak "***nitelikli hırsızlık suçu***" 142. maddenin 2. fıkrasının e bendinde, "***nitelikli dolandırıcılık suçu***" 158. maddenin 1. fıkrasının f bendinde, "***müstehcenlik suçu***" 226. maddesinde ve "***kumar oynanması için yer ve imkân sağlanması suçu***" 228. maddesinde düzenlenmiş olup kanunda hükme bağlanan bu suçlarda çoğunlukla bilişim suçları kapsamında ele alınmaktadır. Bu nedenle söz konusu kanunlara göre müdahil olunan olaylarda elde edilen deliller ağırlıklı olarak elektronik ortamda bulunmaktadır.

Kurumsal ve kişisel olarak bilgisayar ve bilişim cihazlarının yaygınlaşma hızına paralel olarak bu alandaki suçların artacağı endişesi ile bu alandaki eksikliğin giderilmesi maksadıyla Türk Ceza Kanunu bilişim konusunda önemli düzenlemeler yapmıştır. Hükme bağlanan her bir suç, kendisi ile ilgili potansiyel delilleri de hukuk literatürüne kazandırmıştır. Bu düzenlemeler sayısal delillerin varlığını bir tartışma konusu olmaktan çıkarmış nitelik ve nicelik olarak kalitesinin tartışılması ve bir gelenek oluşturulması için imkân yaratmıştır.

4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanununun 4. maddesine göre, bu kanunda düzenlenen suçlar açısından, öngörülen

suçların veya bu suçlara ilişkin delillerin ortaya çıkarılması için, suçları işleyenler ile suçların işleniş biçimlerine benzer tutum ve davranış içinde bulunan kişilere ilişkin yer, kuruluş, çevre ve kurumlardaki her türlü resmi ve özel kayıtlarla bilgisayar verileri incelenebilir.

Devletin ulusal güvenliği bakımından gizli kalması zorunlu olan kayıt ve veriler ise hükmün dışında bırakılmıştır. İncelemenin yapılabilmesi için hâkim kararı gerekmektedir. Bu koruma tedbirinin düzenlenişinde, Alman Ceza Muhakemesi Yasası kaynak alınmıştır. Başkalarına ait bilgisayar verileri, olay ve faile ilişkin oluşturulan anahtara göre taranarak, bu özellikleri taşıyanların bulunması işlemi olarak Almanya'da son zamanlarda düzenlenmiş bir konudur.

Öncelikle belirtmek gerekir ki söz konusu düzenleme sadece organize suçluluk adı da verilen, para kazanmak amacıyla bir araya gelen, uzun süreli örgütlerle mücadele açısından getirilmiş bir düzenlemedir. İkinci önemli özellik ise, 4. madde özel kişi ve kuruluşlarında bilgisayar ve kayıtlarının incelenmesini de düzenlemektedir. Üçüncü özellik ise benzer tutum ve davranışta olanlarında bilgisayar kayıtlarının incelenebilmesidir.

4422 sayılı kanunun doğal olarak, sadece çıkar amaçlı suç örgütleriyle mücadele için öngördüğü bu tedbirin, diğer suç alanlarında uygulanamaması bu konuda bir eksik bulunduğunu göstermektedir. Zira suçların işlenme şekillerinin çeşitlenmesi ve özellikle bilişim suçlarının artması bu konudaki yasal eksiklere hep dikkat çekilmesine yol açmıştır, yani hukuk teknolojik gelişmenin gerisinde kalmıştır.

Özel kişi ve kuruluşlarında bilgisayar ve kayıtlarının incelenmesini de düzenlenmiş olsa da, bu düzenleme özellikle özel kişilere ait kayıtların nasıl inceleneceğini, nereye kadar incelenebileceğini, kişilerin uyma yükümünün ne olduğu ve ilk inceleme ile anlaşılmayan (şifreli) kayıtla karşı neler

yapılabileceği konularında eksik bulunmaktadır. Kişi hak ve özgürlüklerine bu denli müdahaleye açık bir alanın daha sıkı kurallarla belirlenmesi gerekir.

5846 sayılı Fikir ve Sanat Eserleri Kanunu'nda eser sahibinin haklarının korunması açısından düzenlenen suç türlerinin konusuna bilişim yazılımları da dâhil edilmiştir (FSEK, md. 71, md.72, md.73). Bu düzenlemeler ile bilişim yazılımları doğrudan suçun konusunu teşkil etmektedir.

5070 sayılı Elektronik İmza Kanunu'nun 16. maddesinde "***elektronik imza oluşturma verilerinin izinsiz kullanımı suçu***" ile 17. maddesinde "***elektronik sertifikalarda sahtekârlık suçu***" düzenlenmiştir. Bu suçlar ile korunmak istenen hukuksal değer, devletin korumasında ve denetiminde olan bu tür verilere karşı güven duygusudur.

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, kontrolsüz yapılan yayınların denetim altına alınması maksadıyla hazırlanmış olup internet yayıncılığı ile ilgili tüm tarafları bağlayan hükümler yer almıştır.

23 Kasım 2001'de Budapeşte'de, 26'sı üye, 4'ü üye olmayan (ABD, Japonya, Kanada ve Güney Afrika) 30 ülke tarafından imzalanan Avrupa Konseyi Siber Suç Sözleşmesi, ortak bir ceza politikasının oluşturulması ile toplumun siber suçlara karşı korunması, ortak suç tanımlarının getirilmesi, soruşturma yöntemlerinin tanımlanması (veriyi saklama, trafik verisini arama, toplama ve el konulması ile iletişim yetkisi) ve uluslararası işbirliğinin geliştirilmesidir.

Sözleşmenin en önemli boyutu, hala tartışılmayı gerektiren çok sayıda ilkesel yaklaşımın yanı sıra, birçok teknoloji üreticisi ülkenin paylaşımı dolayısıyla kazandığı uluslararası meşruiyet zeminidir. Fakat Avrupa Konseyi Siber Suç Sözleşmesi bilişim suçlarının işlenmesi için bir bilgisayar sisteminin

bulunmasının zorunlu olduğu suçlar olarak öngörmüştür. Sözleşmenin 2. ila 10. maddeleri arasında suç olarak tanımlanan eylemlerde, “İnternet” veya “bilişim ortamı” ya da başka deyişle “siber uzay” kavramları hiç kullanılmamıştır. Böylelikle sözleşme, daha çok bilgisayar verilerine ve bilgisayar sistemine hukuka aykırı maksatlarla yapılan müdahaleleri suç olarak belirlemiştir. Teknolojinin gelişmesine paralel olarak bilişim ortamı ile ilişkili ortaya çıkan ve çıkacak olan suçlardan bahsedilmemesi ve bilişim suçları için bilgisayar sisteminin varlığını gerekli görmesi olması sözleşmenin eksiklerindendir.

Ülke hukuk sistemlerinin birbirinden farklı olmasının yarattığı ispat sorunlarına çözüm bulmaya çalışan uluslararası kuruluşlardan Avrupa Konseyi'nin bu konudaki çalışmaları kayda değerdir. Avrupa Konseyi'nin "Ödeme ve Diğer İlgili İşlemlerde Kullanılan Kişisel Verilerin Korunmasına İlişkin 1 sayılı Tavsiye Kararı" ile "Bilgisayarlarla Kayıt, Belgelerin Çoğaltılmasının Kabulü ve Yazılı İspatın Koşullarına İlişkin Hukukların Uyumlaştırılması hakkında 20 sayılı Tavsiye Kararı" düzenlemeleri bulunmaktadır. 20 sayılı Tavsiye Kararında bilgisayar verilerinin delil olma niteliği konusunda birtakım ilkeler getirilmektedir. Örneğin; doğru ve orijinallerine uygun olan mikrofilm röprodüksiyonları ve bilgisayar kayıtlarının davalarda delil olarak kabul edilmesini sağlayacak düzenlemeler getirilmesi ile usulüne uygun biçimde yapılan mikrofilm röprodüksiyonları ve bilgisayar kayıtlarının, aksi ispat olununcaya kadar doğru ve asıllarına uygun kabul edilmesine yönelik düzenleme yapılması (DPT. Ö.İ.K. Raporu, 1995).

1.10. Delillerin Değerlendirilmesi Kavramı

Ceza muhakemesinde karar verme yetkisine haiz olan yetkililerin, toplanan delillerden sonuç çıkarıp bu sonucu kararlarında kullanmalarına delillerin değerlendirilmesi denir (Öztürk ve Erdem, 2006).

Soruşturmanın amacı suçun kaynağına inmek, olayla irtibatlı tüm delilleri toplamak ve suç sanıklarını ele geçirmektir. Savcının emrinde görev yapan kolluk birimleri ele geçen delilleri, yeni delillere ulaşmak, sanıkları yakalamak ve suçu tüm unsurları ile ispatlamak maksadıyla değerlendirmelere yardımcı olmakla yükümlüdürler.

Ceza muhakemesinde karar verme yetkisine hakim, savcı ve mahkemelerin sahip olduğu gerçeğinden hareketle; bilirkişilerin delilleri değerlendiren değil, teknik anlamda değerlendirme yetkisine sahip olanlara yardımcı personel olduğu unutulmamalıdır (Öztürk C., 2006).

Savcı, soruşturma sonucunda toplanan delillerden çıkardığı sonuca göre dava açma kararı verecektir (Öztürk ve Erdem, 2006). Mevzuatta yapılan yeni düzenlemelerde, savcılarında delilleri değerlendirme mecburiyetleri olduğu vurgulanmaktadır. İddianamede yüklenen suçu oluşturan olaylar, mevcut delillerle ilişkilendirilerek açıklanmadan (CMK, m.170/4) hazırlanan iddianame mahkemece iade edilebilir (CMK, m.174). Savcı delilleri değerlendirmediği takdirde mevzuatın emredici kuralları ile kendisine verilen görevleri yapamaz.

Dava açıldığında toplanan delillerden çıkarılan sonuca göre kovuşturmada yetkili bulunan hâkim veya hâkimler kararlarını verecekler, toplanan delillerden çıkarılan sonuca göre kurulacak hüküm ile sona erecektir (Öztürk ve Erdem, 2006).

Medeni usul hukukunda kişisel çıkarlar ön planda olduğu için taraflar davanın malzemesini ve delilleri mahkeme önüne taşımak zorundadırlar. Tarafların davaya son vermek yetkileri vardır. Tarafların ihtilaf konusu yapmadıkları konuları hâkim kendiliğinden araştıramaz ve bu maksatla delil ikame edemez. Şekli gerçekle yetinilir. Hâkim adeta hakem konumundadır.

Ceza davalarında amaç maddi gerçeğe ulaşmak olduğundan, hâkim, ceza kanununun tatbikinde kendisine arz edilen iddialar ve ikrar ve ispat konusundaki isteklerle de bağlı değildir. Hâkim kanunu uygulamakla yükümlüdür, delilin anlamsız veya anlaşılamaz olduğunu ileri sürerek beraat kararı veremez. Çünkü her kanunun bir anlamı, kanun koyucunun bir iradesi vardır. Hâkim bunu bulmak zorundadır.

Hâkimler görevlerinde bağımsızdırlar; Anayasaya, kanuna ve hukuka uygun olarak vicdani kanaatlerine göre hüküm verirler (T.C. Anayasası, m.138). Hâkim, kararını ancak duruşmaya getirilmiş ve huzurunda tartışılmış delillere dayandırabilir. Bu deliller hâkimin vicdanî kanaatiyle serbestçe takdir edilir (CMK, m.217/1).

1.11. Amaç

Teknolojinin gelişme ve hayatın her alanına nüfuz hızı dikkate alındığında Locard ‘ın "Her temas olay yerinde bir iz bırakır " ilkesi çok yakın bir gelecekte "Her olay yeri bir sanal iz barındırır" şeklinde yorumlanacaktır. Bilgisayar ve internet ortamında işlenen suçlar ile bilişim cihaz ve verilerinin delil olarak kullanıldığı suçların ortaya çıkarılması ve/veya suçun işlenmeden önlenmesi maksadıyla bilişim verilerinin teknik incelemelerle elde edilmesi ve/veya iletişimin dinlenmesi gerekmektedir.

İşlenen suçların çok önemli bir kısmında bir adli bilişim bağlantısının tespit edildiği günümüzde bu suçların çözülmesi, faillerin ve zararların tespit edilmesi ve nihayetinde muhakeme sürecinde doğru hükümlerin verilmesi, ancak adli personelin adli bilişim konusunda donanımlı olmaları ile mümkün olacaktır.

Adli bilişimin başlıca uğraşlarından olan sayısal delilin teknik ve hukuki niteliği, sayısal delillerin tespiti ve delillerin sunumu konularında kurumsal,

bölgesel, suç çeşitleri ve kişisel tasarruflara göre değişik standartlar oluşturulmuştur. "***Sayısal delil nedir ?, sayısal delil nasıl tespit edilir ?, sayısal delil nerelerden bulunur ?, olay yeri inceleme esnasında sayısal delil tespiti ve müdahale esasları nelerdir ?, sayısal delil içeren cihazların laboratuvar incelemesinde esaslar nelerdir ?, sayısal delillerin bilgisayar destekli analizi ve değerlendirilmesinde kullanılan teknikler nelerdir?***" sorularına verilen cevaplardaki çeşitlik, bir zenginliği ifade etmemektedir. Cevapların çeşitliliği adli bilişim konusunda uygulama birliğinin olmadığını, yeterli eğitime sahip olunmadığını ve kurumsal yatırım önceliklerinde ilk sıralarda yer bulamadığını göstermektedir.

Bilişim teknolojilerindeki gelişimin adli sürecin her safhasında yarattığı değişim ve karmaşa, bu çalışmanın amaçlarını oluşturmaktadır:

1. Adli bilişimin temel çalışma sahaları olan sayısal delil, sayısal delil tespiti konusunda eğitim ve bilinç eksikliği giderilmesi amaçlanmıştır. Müşterek temel eğitimin hukukçular için ayrı, bilişimciler için ayrı şekilde düzenlenmesinin mümkün ve uygun olmaması nedeniyle söz konusu eğitimin teknik ayrıntılara girilmeden yapılması gereklidir.

2. Uygulayıcılar için bilgi, işlem ve belge standardı sağlanması amaçlanmıştır. Adli bilişim disiplinine taraf olan herkesin ortak bir dil geliştirmesi kabul gören bir standardın sonucu olacaktır.

3. Adli bilişim adına en önemli konulardan biri donanımlı bir adli bilişim laboratuvarının kurulmasıdır. Özel amaçlı bu tür bir laboratuvarın kurulması ve en uygun şartlarda çalışması için gerekli şartların bilinmesi amaçlanmıştır.

4. Sayısal delilin elde edilişi kadar delilin sunumu da muhakeme kalitesinin yükseltilmesinde önemlidir. Bu nedenle veri analizi konusundaki kişisel ve bağımsız çalışmaların yerini sistemli yeni bir yaklaşımın alması amaçlanmıştır.

2. MATERYAL VE METOD

Adli bilişim, bilinen tüm bilişim donanım, yazılım ve yöntemlerinin hukuki kurallar çerçevesinde bütünleşik olarak kullanılabilmesiyle anlam bulan bir disiplindir. Genel ve herkes tarafından kabul gören kuralları oluşturabilecek kadar uzun geçmişe sahip olmayan adli bilişimin az sayıdaki uzmanı, kullandığı bilgi ve yöntemlerin çoğunu eğitim yerine ticari ürünlerden elde etmektedirler. Bu disipline ait yayınlar, ticari kaygılarla işletim sistemi markası, yazılım markası ve belirli bir güvenlik çözümüne özel hazırlanmakta ve güvenilirlik seviyesinin yüksek olduğu düşünülmektedir.

Bu çalışmada materyal olarak bilinen tüm marka ve modeldeki bilişim cihazının teknik özellikleri, yazılımların amaç ve yetenekleri ile kişisel ve kurumsal bilişim ihtiyaç analizleri kullanılmıştır. Buna ilave olarak halihazırda adli bilişim alanında yapılan uygulamalar ve teknik çalışmalar yerinde incelenmiştir. Çoğunlukla konu ile ilgili resmi bir eğitimi almamış olan veya kısmen eğitim alan uygulayıcı personel ile görüşülmüştür. Bilişim teknolojileri kullanılarak işlenen suçların çoğu organize suçlar kapsamında değerlendirilmektedir. Organize suç olaylarının gizlilik içinde soruşturulmasında gösterilen özel hassasiyet ve soruşturmanın gizliliği ilkesi (TCK m.285) nedeniyle bilişim teknolojileri kullanılarak işlenen suçlarla ilgili olay sayısı, işleniş şekli, ele geçen malzeme sayısı, bilişim malzemelerine yapılan adli incelemeler hakkında istatistiksel verilerle desteklemek mümkün olmamıştır. Ancak tez süreci boyunca müdahale edilen olaylar, cihazlar ve elde edilen sonuçlar incelenerek uygulamada karşılaşılan doğru ve yanlışlar biriktirilerek bir kurallar bütünü ortaya çıkarılmıştır.

Literatür araştırması yöntemiyle ve bugüne kadar oluşan ulusal ve uluslararası içtihatlar incelenerek adli bilişim açından hukuki konular açıklanmıştır. Çalışmada yer alan teknik konular ile ilgili ulusal ve uluslararası

kaynaklar incelenmiş, ortak sonuçlar üretilmesinde bu çalışmalardan da faydalanılmıştır. Çalışmanın özgünlüğünü sağlayan tasnif ve kuralların hazırlanmasında bilişim materyallerinin teknik özellikleri, yetenekleri ve suça etkileri müşterek olarak değerlendirilmiş, ortak bir sayısal delil tasnifinin ortaya çıkarılması ve bilişim cihazlarına müdahale kurallarının oluşturulması maksadıyla da yazılım geliştirme tecrübesi, adli bilişim uygulamacısı olarak kazanılan saha tecrübesi ile bilgisayar destekli istihbarat analiz yöneticiliği tecrübesi yoğunluklu olarak kullanılmıştır.

3. BULGULAR

Bilişim teçhizatı (yazılım, donanım, bilişim ağ ortamı) kullanım amacına göre pek çok veriyi kullanır, pek çok veriyi üretir ve pek çok veriyi de depolar. Verinin tek başına da çok kıymetli olması, ticari anlamda fazlasıyla değer kazanmasına yol açmıştır. Bu nedenle verinin bir şekilde içinde yer aldığı her türlü süreç pazarlama değeri olan bir alan haline gelmiştir. Bugünün küresel bilişim pazarında; **silinen ve bozulan verileri kurtarma, güvenlik ihlallerinin tespiti, mali ve idari denetim, veri analizi, kurumsal bilişim güvenliği, GSM telefon yardım kitleri** ve **ağ trafiğinde akan verilerin dinlenmesi** ile ilgili çözümler en çok talep gören ve yatırım yapılan bilişim sahalarıdır. Bu konular aynı zamanda adli bilişimin başlıca çalışma sahalarını ve yöntemlerini oluşturmaktadır.

Sayısal delillerin tasnifi ve tespiti konusunda yapılan literatür araştırmasında görülmüştür ki **tespit ve tasnifler çoğunlukla tek bir cihaz türü** (kişisel bilgisayar, cep telefonu, el bilgisayarı vb.), **tek bir işletim sistemi** (Microsoft WINDOWS NT, Microsoft WINDOWS XP, UNIX, LINUX vb.) **veya tek bir amaca** (veri kurtarma, bilgisayar ağı adli bilişimi, bilgisayar destekli veri analizi, şifre kırma vb.) **yönelik oluşturulmuştur**. Yayınları hazırlayan uzmanların en iyi bildiği ancak bilişim açısından eksik bir cihaz/marka/amaç hakkında, üstelik ticari kaygılar gözetilerek hazırlanan bu tür yayınların göz ardı ettiği en önemli gerçek, bilişim yelpazesinin geçmiş-gelecek ve cihaz/marka/amaç ölçeğinde inanılmaz büyüklükte olduğudur. Yani 10 yıl önce piyasaya sürülen Pentium-II işlemcili bir kişisel bilgisayar da, daha az yaygın bir işletim sistemi de (MS-DOS, DOS, Mac-OS, OS400, irix, solaris) veya bir uzman sistem de (tıbbi cihazlar, üretim robotları, vb.) adli bilişim kapsamında incelenebilir. Karşılaşılması muhtemel bu tür istisnaların üstesinden gelebilmek maksadıyla markası, modeli veya

türü ne olursa olsun her türlü cihaza uyarlanabilecek bir sayısal delil tasnifi ihtiyacı ortaya çıkmıştır.

Bu çalışma ile tasniflenen bilişim cihaz/ortamlarındaki sayısal delililer, cihaz veya yazılımın marka, model ve türü ile cihazın kullanım amacından bağımsızdır. Bu sayede olayın türü, elde edilen bilişim materyalinin muhteviyatı ve uzman yetkinliğinin adli bilişim uygulamasının başarısına etkisi delil toplama açısından sabitlenmektedir. Aranacak sayısal delililer, bilişim cihazı/ortamına göre aşağıda oluşturulan listelerden seçilerek özelleştirilebilir hale getirilmiştir. Sürekli aynı tür cihazları benzer tekniklerle incelemeyi alışkanlık haline getiren uzmanların, yeni bir materyal ile karşılaştıkları zaman otomatik olarak yaptıkları (veya yazılımlara yaptırdıkları) işlemleri atlamamaları ve araştırması unutulan bir verinin kalmaması sağlanacaktır.

Olay yeri ve laboratuvar incelemelerinde faydalı ve etkili olacağı değerlendirilen bu tasnif yöntemi sayesinde bilişim cihaz/ortamlarındaki sayısal delililer ile ilgili genel bir kuralın ortaya konulması hedeflenmiştir. Adli inceleme esnasında değişkenlik gösteren her türlü parametreye (olay türü, cihaz türü, marka ve model, vb.) rağmen **her olaya özel incelemelerin** yapılabilmesi için bu genel kuralın başvuru ve referans kaynağı olarak kullanılması, iş yapma yöntemlerinin disiplin altına alınması ve ortak bir bilimsel lisanın geliştirilmesinde en temel faydayı sağlayacaktır.

Sayısal delililer, çoğunlukla elektronik yapıdadır. Bu yapı, dış dünyaya ancak görsel veya işitsel olarak yansıtılabilir. Ancak, sayısal delillerin elde edilmesi kolay değildir. Çoğunlukla, incelenen bilişim materyalinden başka bilişim materyali kullanılarak delil elde edilmeye çalışılmaktadır. Bu nedenle delil elde etmede kullanılacak ürünlerin kapsamı ve yetenekleri kadar delil elde edilmektedir. Bu döngünün sorgulanabilmesi için bilişim cihazlarında suça ait iz ve eserlerinin bulunabileceği yerler iyi bilinmeli ve tüm olasılıklar üzerinde titizlikle durulmalıdır. Bilişim cihazlarındaki delillerin tespiti için en

önemli gerek şart, bu cihazların iyi tanınması ve delil olabilecek verilerin bilinmesidir.

3.1. Olay Yerindeki Sayısal Deliller Konusunda Önerilen Tasnif

3.1.1. Bilişim Cihazları/Ortamlarında Sayısal Deliller

3.1.1.1. Bilgisayar/Bilgisayar Sisteminde Sayısal Deliller

En basit tarifiyle bilgisayar; çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyindir (www.tdk.gov.tr).

Bilgisayar, kullanıcısından aldığı verilerle mantıksal ve aritmetiksel işlemleri yapan; yaptığı işlemlerin sonucunu saklayabilen; sakladığı bilgilere istenildiğinde ulaşılabilen elektronik bir makinedir. Bu işlemleri yaparken girilen verilerle insanların amaçları doğrultusunda ve programının yetenekleri ölçüsünde işlemekte, istendiğinde depolamakta ve görsel ve/veya işitsel biçimde raporlamaktadır.

Bilgisayar, bilişim dünyasının en temel aktörüdür. Genellikle veri hacmi insan gücü ile yönetilemeyecek kadar büyük olan organizasyonlarda kapasiteleri yüksek, görevleri uzmanlaştırılmış, birden fazla bilgisayar aynı anda kullanılmaktadır. Birden fazla bilgisayarı kullanan veya birden fazla bilgisayara hizmet eden yapılar bilgisayar sistemi olarak tanımlanmaktadır.

Kullanım niteliği, hizmet çapı, ürettiği maddi veya manevi değer gibi parametreler, çoğunlukla bilgi teknolojileri konusunda niceliği belirlemek için kullanılmaktadır. Bu nedenle ölçülebilen değerleri ne olursa olsun kişisel bilgisayar, diz üstü bilgisayar, avuç içi bilgisayar, her ölçekteki sunucu tip

bilgisayarlar bilgisayar ve bilgisayar sistemi sınıflandırması altında değerlendirilmelidir.

Bilgisayar, temel olarak üç ana bileşene sahiptir: donanım, işletim sistemi ve yazılım. Donanım fiziksel teçhizat ve aksamı temsil etmektedir. İşletim sistemi, bilgisayarın temel aritmetik ve mantıksal görevleri nasıl yapacağını bilgisayara öğreten, donanım ve yazılım arasındaki işlemlerin yönetilmesini sağlayan yazılımlardır. Yazılım ise kullanıcıların kendi amaçları (iş, eğlence, araştırma, suç, vb.) doğrultusunda veri operasyonlarını yapıp donanım ile etkileşime geçmelerini sağlamaktadır.

Bundan sonraki alt başlıklar her bir bileşenden elde edilebilecek sayısal delilleri içermektedir. Bu delillerin nasıl elde edileceği ayrı bir çalışma ve uzmanlık konusudur. Bu tekniklerden güvenlik endişeleri nedeniyle bahsedilmeyecektir.

3.1.1.1.1. Bilgisayar Donanımında Sayısal Deliller

- Bilgisayarın marka/model/seri numarası/üreticisi
- Bilgisayarın mevcut durumu (çalışır halde, arızalı, vb.)
- Anakart teknik özellikleri
- Merkezi işlem birimi (CPU) teknik özellikleri
- Çevre birimleri bağlantı (port) teknik özellikleri
- Ağ bağlantı teknik özellikleri
- Yedekleme birimleri teknik özellikleri
- Ses ve grafik teknik özellikleri
- EPROM (Erasable and Programmable Read Only Memory) teknik özellikleri ve şifreleri
- EPROM ‘dan elde edilen veriler
- Ağ üzerinde uzaktan erişim özellikleri
- Eylemin donanıma etkileri

3.1.1.1.2. İşletim Sisteminde Sayısal Deliller

- İşletim sisteminin markası ve üreticisi
- İşletim sisteminin mevcut durumu (çalışır halde, hatalı, vb.)
- İşletim sisteminin sürümü
- İşletim sisteminin lisanslama özellikleri
- Yüklü bulunan yamalar
- İşletim sisteminin dosya sistemi türü (FAT, NTFS, vb.) ve disk bölümlemeleri
- İşletim sisteminin yapılandırma ayar dosyaları (config, registry vb.)
- İşletim sisteminin dosya sisteminde tutulan geçici, kalıcı veya silinen tüm kütüphane/dosya/kayıt/verilerin içerikleri ve kimlikleri (metadata)
- İşletim sisteminin dosya sisteminde tutulan geçici, kalıcı veya silinen tüm kütüphane/dosya/kayıt/verilerin dosya türlerine göre tasnifi, bu tür dosyaların kullanım amaçları ve bu tür dosyaları kullanan yazılımlar
- İşletim sisteminde tanımlı olan harici donanım birimleri
- İşletim sisteminde tanımlı bulunan kullanıcı kimlikleri
- İşletim sisteminde tanımlı kullanıcıların geri dönüşüm kutularında bulunan dosyalar
- İşletim sisteminde tanımlı yetkilendirme politikası
- İşletim sisteminde tanımlı erişim politikası ve açık olan portlar
- İşletim sisteminde tanımlı güvenlik politikası ve şifreler
- İşletim sisteminde kullanılan güvenlik teknikleri
- İşletim sisteminin ürettiği geçici, kalıcı veya silinen dosyalar
- İşletim sisteminde tutulan geçici, kalıcı ve silinen günlük ve tarihçeler
- İşletim sisteminde gömülü olarak kullanılan programların (internet tarayıcı, kelime/resim işleme programları, vb) ürettiği geçici, kalıcı veya silinen dosyalar/kayıtlar (çerezler dahil)
- İşletim sisteminde gömülü olarak kullanılan programların (internet tarayıcı, kelime/resim işleme programları, vb) geçici, kalıcı veya silinen günlük ve tarihçeleri

- Kullanıcı tarafından çalıştırılan işletim sistemi seçenekleri (virüs kontrolü, ateş duvarı, vb.)
- Görev yöneticisi vasıtasıyla tespit edilebilen uygulamalar ve işlemler
- İşletim sistemi açılış ve kapanış politikası
- İşletim sistemi açılırken ve kapanırken çalışan yazılım/yazılımlar
- Eylemin işletim sistemine etkileri

3.1.1.1.3. Bilgisayar Yazılımında Sayısal Deliller

- Yazılım/yazılımların markası ve üreticisi
- Yazılım/yazılımların sürümü
- Yazılım/yazılımların amacı
- Yazılım/yazılımların mevcut durumu (çalışır halde, hatalı, vb.)
- Yazılım/yazılımların kurulumu için gerekli ön şartlar
- Yazılım/yazılımların kurulum bilgileri ve yapılandırma ayar dosyaları
- Yazılım/yazılımların teknik özellikleri
- Ticari olmayan kurumsal veya kişisel amaçla hazırlanmış olan Yazılım/yazılımların kaynak kodları
- Yazılım/yazılımların lisanslama özellikleri
- Yazılım/yazılımlarda tanımlı bulunan kullanıcı kimlikleri
- Yazılım/yazılımların yetkilendirme politikası
- Yazılım/yazılımların erişim politikası
- Yazılım/yazılımların güvenlik politikası ve şifreler
- Yazılım/yazılımların kullandığı güvenlik teknikleri
- Yazılım/yazılımlar tarafından kullanılan geçici, kalıcı ve silinen veriler
- Verilerin tutulduğu veritabanı marka/model/sürümü
- Verilerin tutulduğu veritabanı özellikleri
- Verilerin tutulduğu veritabanı lisanslama özellikleri
- Verilerin tutulduğu veritabanı yetkilendirme politikası
- Verilerin tutulduğu veritabanı erişim politikası

- Verilerin tutulduğu veritabanı güvenlik politikası ve şifreleri
- Verilerin tutulduğu veritabanı tarafından tutulan günlük ve tarihçeler
- Yazılım/yazılımların kullandığı kalıcı ve geçici dosyalar
- Yazılım/yazılımların ürettiği kalıcı ve geçici dosyalar
- Yazılım/yazılımların kayıt altına aldığı günlük ve tarihçeler (son yapılan işlemler, sık kullanılan belgeler gibi)
- Yazılım/yazılımların açılış ve kapanış politikası
- Bir yazılım marifetiyle ağ üzerindeki başka bilgisayar ve/veya cihazın her türlü veri trafiği dinlenerek elde edilen veriler.
- Eylemin yazılım/yazılımlara etkileri

3.1.1.2. Çevre Birimlerinde Sayısal Deliller

Bilişim sistemi kapsamında veri girişi ve çıkışı amacıyla kullanılan cihazlardır. Yazıcı, tarayıcı, çizici, kesintisiz güç kaynağı, web kamerası, mikrofon, klavye, barkot okuyucuları, küresel konum belirleme (GPS) cihazları bu kapsamda değerlendirilmelidir.

Çevre birimlerinden elde edilebilecek sayısal delil muhtevası aşağıdaki başlıklardan oluşabilir:

- Çevre biriminin türü (yazıcı, tarayıcı, vb.)
- Çevre biriminin kullanım amacı
- Çevre biriminin marka/modeli/seri numarası/üreticisi
- Çevre biriminin mevcut durumu (çalışır halde, arızalı, vb.)
- Çevre biriminin çalışabilmesi için gerekli ön şartlar
- Çevre biriminin kurulum bilgileri ve yapılandırma ayar dosyaları
- Çevre biriminin teknik özellikleri
- Çevre biriminin güvenlik özellikleri ve şifreler
- Çevre biriminin geçici/kalıcı hafıza birimlerinde tutulan veriler
- Çevre biriminin ağ bağlantı özellikleri

- Çevre biriminin paylaşım/erişim özellikleri
- Çevre biriminin ürettiği günlük ve tarihçeler
- Eylemin çevre birimine etkileri

3.1.1.3. Yedekleme ve Bellek Birimlerinde Sayısal Deliller

Bilişim sistemi kapsamında verinin saklanması ve/veya taşınması maksadıyla kullanılan bileşendir. Sabit disk, taşınabilir disk, disket, CD, DVD, bellek çubukları, bellek kartları, harici sürücüler bu kapsamda değerlendirilir.

Yedekleme birimlerinden elde edilebilecek sayısal delil muhtevası aşağıdaki başlıklardan oluşabilir:

- Yedekleme biriminin türü (Disket, CD, Disk, taşınabilir disk, taşınabilir çubuk bellek, bellek kartı, vb)
- Yedekleme biriminin kullanım amacı
- Yedekleme biriminin marka/modeli/seri numarası/üreticisi
- Yedekleme biriminin mevcut durumu (çalışır halde, arızalı, vb.)
- Yedekleme biriminin dosya kayıt sistemi (NTFS; FAT, vb.) ve bölümlemeleri
- Yedekleme biriminin çalışabilmesi için gerekli ön şartlar
- Yedekleme biriminin teknik özellikleri
- Yedekleme biriminin güvenlik özellikleri ve şifreler
- Yedekleme biriminde tutulan geçici, kalıcı veya silinen tüm kütüphane/dosya/kayıt/verilerin içerikleri ve kimlikleri (metadata)
- Yedekleme biriminin ağ bağlantı özellikleri
- Yedekleme biriminin paylaşım/erişim özellikleri
- Yedekleme biriminin ürettiği günlük ve tarihçeler
- Eylemin yedekleme ve bellek birimine etkileri

3.1.1.4. Ağ İletişim Cihazlarında Sayısal Deliller

Bilişim sistemi içinde bir bilgisayar ağının oluşturulması, işletilmesi ve/veya yönetilmesi maksadıyla kullanılan cihazlardır. Modem, yönlendirici, anahtarlama cihazı, HUB, konektörler bu kapsamda değerlendirilmelidir.

Ağ iletişim cihazlarından elde edilebilecek sayısal delil muhtevası aşağıdaki başlıklardan oluşabilir:

- Ağ iletişim cihazının türü (Modem, router, hub, switch, vb.)
- Ağ iletişim cihazının ağ üzerindeki görevi
- Ağ iletişim cihazının marka/modeli/seri numarası/üreticisi
- Ağ iletişim cihazının mevcut durumu (çalışır halde, arızalı, vb.)
- Ağ iletişim cihazının çalışabilmesi için gerekli ön şartlar
- Ağ iletişim cihazının teknik özellikleri
- Ağ iletişim cihazının güvenlik özellikleri ve şifreler
- Ağ iletişim cihazında tutulan geçici, kalıcı veya silinen veriler
- Ağ iletişim cihazının ağ bağlantı özellikleri
- Ağ iletişim cihazının paylaşım/erişim özellikleri
- Ağ iletişim cihazının ürettiği günlük ve tarihçeler (log)
- Teknik dinleme sonucu bilişim ağı üzerinden akan sayısal verinin elde edilmesi ve çözümlenmesi ile elde edilen veriler
- Eylemin ağ iletişim cihazlarına etkileri

3.1.1.5. Entegre Cihazlarda Sayısal Deliller

Kullanım amaçları çok çeşitli olsa da içeriğinde bilişim teknolojisi barındıran cihazlar bu kapsamda değerlendirilmelidir. Cep telefonu, çağrı cihazı, sayısal kamera ve fotoğraf makinesi, özel amaçlı kameralar (ısıya hassas, kızıl ötesi, vb.), fotokopi makinesi, ATM cihazı, elektronik ajanda, faks makinesi, elektronik veri bankası, akıllı kart, POS makinesi bu kapsamda

değerlendirilmelidir. Son zamanlarda günlük kullanıma sunulan elektronik veya mekanik ürünlerin pek çoğunda bilişim çözümleri ile bütünleşme sağlanmıştır. Bu nedenle bu kapsama alınabilecek pek çok ürün daha bu listede sayılabilir.

Entegre cihazlardan elde edilebilecek sayısal delil muhtevası aşağıdaki başlıklardan oluşabilir:

- Entegre cihazın türü (Cep telefonu, fotokopi makinesi, ATM cihazı, vb.)
- Entegre cihazın kullanım amacı
- Entegre cihazın marka/modeli/seri numarası/üreticisi
- Entegre cihazın mevcut durumu (çalışır halde, arızalı, vb.)
- Entegre cihazın çalışabilmesi için gerekli ön şartlar
- Entegre cihazın teknik özellikleri
- Entegre cihazın güvenlik özellikleri ve şifreleri
- Entegre cihazın veri depolama yetenekleri ve şifreleri
- Entegre cihazda tutulan geçici, kalıcı veya silinen veriler (son yapılan işlemler, arama kayıtları gibi)
- Entegre cihazın ağ bağlantı özellikleri
- Entegre cihazın bağlı olduğu ağ üzerinde gönderdiği ve/veya aldığı her türlü veri
- Entegre cihazın paylaşım/erişim özellikleri
- Entegre cihazın ürettiği günlük ve tarihçeler (en son yapılan işlemler, son yapılan aramalar, gelen çağrılar, vb.)
- Entegre cihazın açılış ve kapanış politikaları
- Eylemin entegre cihaza etkileri

3.1.1.6. İnternet Ortamında Sayısal Deliller

İnternet, insanoğlunun şimdiye kadar yapılandırdığı en büyük iletişim sistemidir. İnternet, birçok bilgisayar sisteminin birbirine bağlı olduğu, dünya

çapında yaygın olan ve sürekli büyüyen bir iletişim ağıdır. Bu ağın belirli bir yöneticisi yoktur. İnternet kullanıcıları birbirleri ile haberleşmek için ortak bir anlaşma dili kullanırlar. Bu ortak anlaşma diline TCP/IP protokolü denir. Bu protokol sayesinde donanım ve yazılımdan bağımsız olarak bilgisayarlar arası iletişim mümkün olur. Bu anlaşma dilinde her bilgisayarın bir adresi vardır. Tıpkı her evin bir adresi, her telefonun bir numarası olduğu gibi bu adresler numaralarla ifade edilir ve bilgisayarın IP adresi şeklinde ifade edilir. Bu adreslere bilgiler en kestirme yoldan ulaşır.

İnternetin en temel işlevi, haberleşme ve iletişimdir. İnternet, insanların her geçen gün gittikçe artan "***üretilen bilgiyi saklama/paylaşma ve ona kolayca ulaşma***" istekleri sonrasında ortaya çıkmış bir teknolojidir. Bu teknoloji yardımıyla pek çok alandaki bilgilere insanlar kolay, ucuz ve hızlı bir şekilde erişebilmektedir. İyimser bir bakış açısıyla internet bu haliyle bir bilgi denizi veya devasa bir kütüphaneye benzetilebilir.

İnternetin cazibesi kullanıcıların fikirlerini ifadede tamamen özgür olmalarıdır, İnternet "*büyük bir alışveriş merkezi haline gelen dünyadan ve bu dünyanın tüketim kültüründen kaçanların oluşturdukları ve özgür ifadenin serbest bir şekilde dolaşabildiği bir cennettir; burada kanunlar ve zorunluluklar yoktur, herkes istediğini yapabilir ve söyleyebilir*" (McClellan, 1994).

"*İnternet bir özgürlükler cennetidir. Özgürleşme ifadede başlar ve giderek zamana ve mekâna, vücut ve görüntü gibi fiziki bütün özelliklere ve hatta kimliğe kadar uzanır. Kullanıcılar dünyanın neresinde olurlarsa olsunlar internete girdikleri anda zaman ve mekân anlamını yitirir. İnsanın görüntüsü ve vücudu ile ilgili özellikler de bu sanal dünyada ağırlıklarını kaybetmektedir. İnternet üzerinden haberleşenler istedikleri kişiliği, rolü, cinsiyeti ve varlık biçimini denemek şansına sahiptirler"* (Stallabrass, 1995).

Bu anlamda İnternet sadece ifade özgürlüğü değil sonsuz özgürlük vaat etmektedir. Oysa demokrasi kültürünün en önemli girdilerinden birisi özgürlüğe konulan sınırlamalarla yaşamasını bilen ve bu sınırlar çerçevesinde toplumsal varoluşunu şekillendiren insanların varlığıdır.

Birçok insan için sonsuzlukla anlam bulan İnternet ortamından elde edilebilecek sayısal delil muhtevası aşağıdaki başlıklardan oluşabilir:

- İnternete bağlantı şekli (kurumsal ağ, ADSL, kablosuz, vb.)
- İnternet bağlantısı için kullanılan şifreler
- Üzerinden bağlantı sağlanan internet servis sağlayıcısı bilgileri
- Tespit edilebilen son bağlantı yaptığı site adresleri
- Söz konusu sitelerin türleri (haber, eğlence, forum, vb.)
- Bağlanılan sitelerin özellikleri (üyelik sistemi, başka bir adrese yönlendirmeli, bağlantı sonrası bir program yüklemeli, vb.)
- Söz konusu sitelerin tespit edilen sayısal kimlikleri (IP adresi, etki alanı (domain), sahibi, hizmetin verildiği ülke, vb.)
- Bağlantı için kullanılan internet tarayıcısının marka ve sürümü
- Kullanılan internet tarayıcısının aktif olan özellikleri
- İnternete bağlantı sonucu oluşan tüm geçici ve kalıcı kayıtlar
- İnternet ortamında iletişim ve sohbet için kullanılan yazılım/yazılımlar (MSN Messenger, ICQ, vb.)
- İletişim veya sohbet yazılımlarının ürettiği geçici veya kalıcı kayıtlar
- Kullanılan elektronik posta hizmet programları (Outlook, Outlook Express, Thunderbird, vb.)
- Elektronik posta hizmet programlarının kullandığı ve ürettiği kalıcı, geçici ve silinen kayıtlar
- Gelen ve giden elektronik posta sahipleri ve alıcıları
- İnternet ortamında kullandığı takma isim/isimler (nickname)
- Şifre ile girilen sitelerde kullanılmakta olan “Beni hatırla” seçeneğinin işaretlenmiş olması ihtimali göz önünde bulundurularak bu tür sitelerde kullanılan şifre dosya/kayıtları

- Forum, sohbet (chat) veya arkadaşlık gibi internet siteleri sıklıkla olmak üzere kullanıcının girdiği veriler ve kullanımla ilgili günlük ve tarihçeler
- Kullanımı yaygınlaşmaya başlanan IP tabanlı telefon sistemlerinin tuttuğu kayıtlar
- Web kamerası tarafından kaydedilen görüntüler
- İnternet bağlantılarının denetlenmesi maksadıyla kullanılan içerik filtreleme yazılımları, ateş duvarı yazılımları veya saldırı önleme yazılımları tarafından tutulan kayıtlar ve günlük ve tarihçeler
- İnternet servis sağlayıcıları tarafından internet bağlantıları ile ilgili tuttuğu veriler
- Ağ kaynaklarını kullanan yazılım/yazılımlar ve kullandıkları portlar
- Teknik dinleme sonucu internet üzerinden akan sayısal verinin elde edilmesi ve çözümlenmesi ile elde edilen veriler
- İnternet kaynakları kullanılarak gerçekleşen eylemin etkileri

3.2. Sayısal Delil Tespitinde Önerilen İş Akışı

3.2.1. Olay Yerindeki Bilişim Cihazlarına İlk Müdahale

3.2.1.1. Genel Kurallar

1. Sayısal delillerin toplanması hususunda adli sürecin tüm görevlileri hukuki mevzuata uygun genel adli usul, ilke ve kurallara uymaktan ve uyulmasını sağlamaktan sorumlu ve yükümlüdür.

2. Bilişim delillerinin yapısı gereği çok kolaylıkla karartılabilir olmasından dolayı tüm faaliyetlerde hızlı olunması çok önemlidir. Bu nedenle adli bilişim ile doğrudan ilgili ihbar ve şikâyetlerin üzerinde titizlikle durulmalıdır.

3. Şüpheli dâhil olmak üzere hiç kimsenin olay mahallinde bulunmasına, her hangi bir şeye dokunmasına ve hiçbir işi tamamlamasına izin verilmemelidir. Olay yerindeki telefon ve veri iletişimi kontrol altına alınmalıdır. Olay yerinde bilişim cihazına müdahale yetkilisi uzman personel dışında hiç kimsenin bilişim sisteminde çalışmasına izin verilmemelidir.

4. Bilişim cihazlarına el konulurken ve/veya sayısal delillerle çalışılırken yapılan her işlem ayrıntılı olarak belgelenmeli ve bu belgeler korunmalıdır. Olay yerinin genel görünüşü bilgisayar sistem ve donanımlarının genel görünümü videoya çekilmeli ve fotoğrafları çekilmelidir. Ayrıca sistemin tüm bağlantıları, irtibatları, görüntüleri, ekranları, üzerindeki yazılar ve seri numaraları detaylı ve incelenebilecek şekilde görüntüye alınmalıdır. Bu amaçlar için kasete çekim yapan video ve film üzerine çekim yapan fotoğraf makinelerinin kullanılmasına özen gösterilmelidir. El konulan cihaz/sistem/malzemenin gerekli şekilde muhafaza altına alınıp etiketlenmesinin ardından son hali ile tekrar kamera ve fotoğraf kayıtları alınmalıdır.

5. İnceleme öncesi bir planlama yapılmalıdır. Suçun türü, ele geçmesi muhtemel bilişim cihazları ve verilerin niteliği, ele geçmesi muhtemel başka deliller (parmak izi, DNA, vb.) ve tehdit değerlendirmelerinin esas alındığı planlamaya göre uygun niteliklere haiz uzman personelin görevlendirmesi sağlanmalıdır. Her uzmanın her sistem veya cihaz hakkında bilgi sahibi olamayacağı unutulmamalıdır. Hazırlanan planda personel sayısı, niteliği, görevi, soruşturma sorumlusu, kullanılacak malzeme (araç, gereç, ambalaj malzemesi, iz tespit cihazları gibi) açıkça belirtilmelidir (Öztürk ve Erdem, 2006).

6. Olay yerine gelen diğer kolluk birimlerinin yapacakları herhangi bir hata nedeniyle meydana gelecek değişiklikler elektronik teçhizat veya ortamların delil olma özelliğini ortadan kaldırır. Bu nedenle olaya ilk müdahaleyi yapacak kolluk personelinin eğitimli olmasına dikkat edilmeli ve müdahale öncesi müdahale edilecek olay ve cihaz ile ilgili azami düzeyde bilgilendirilmelidir. Cihazın, suçun ve/veya soruşturmanın niteliğine göre uzman personelin müdahalesini beklemek en iyi hal tarzı olacaktır.

7. Bilişim teknolojileri ile ilgili adli uygulamalara asla yalnız gidilmemelidir. Olay yeri incelemesi esnasında mutlaka konunun uzmanı bir kişi daha olmalıdır.

8. Bilişim teknolojileri ile ilgili bir olay yerine müdahale öncesinde hedef, yöntem, zanlı, olayın meydana geldiği mekân bilgileri gözlem yolu ile incelenmelidir.

9. Olay yerinde bulunan diğer bilişim malzemelerinin kapalı olanları açılmamalı, açık olanlar ise cihazın türüne göre kontrol edilerek gücü kesilmek suretiyle kapatılmalıdır.

10. Bilişim teknolojileri ile ilgili bir olay yeri müdahalesi öncesinde muhtemel olay yerine uzaktan erişim ile delillerin karartılması ihtimaline karşı elektromanyetik koruma sağlayacak donanım ve yazılımlar bulundurulmalıdır.

11. Cihazın kasasının açık olması durumunda eksik olan parçalar tespit edilmeli (sabit diskin sökülmesi gibi), olay yeri bu eksik parçaya göre gerekirse yeniden incelenmelidir.

12. Olay yerinde o anda sistem üzerinde takılı bulunmayan tüm bilişim materyali (disket, cd, teyp, kartuş, taşınabilir disk/bellek, bellek kartı, kulanım kılavuzu, sistemle ilgi belgeler, vb.) toplanmalıdır.

13. Cihaza bağlı tüm çevre birimleri ayrıntılı olarak kontrol edilmelidir. Bu cihazların içerisinde başka ilave cihazın (taşınabilir bellek gibi) bulunup bulunmadığı tespit edilmelidir.

14. Olay yerinden toplanan bilişim malzemeleri hasar görmüş (imha edilmeye çalışılan bir disk, disket, CD, vb.) ve bu nedenle yedekleme amaçlı bileşenlerin bilgi yazan manyetik yüzeyleri görünür hale gelmiş olabilir. Bu nedenle bu tür malzemeyi toplarken mutlaka elektrostatik korumalı kıyafet (eldiven gibi) ve muhafaza kullanılmalıdır.

15. Cihazın çevresindeki notlar, karalamalar veya basılı kâğıtlar toplanmalıdır. Kullanılan şifrelerin toplanan bu kâğıtlar üzerinde olması ihtimali dikkate alınmalıdır.

16. Olay yeri inceleme işlemlerinde veri kopyalamak için kullanılacak olan malzemenin daha önce kullanılmamış olmasına dikkat edilmeli, özellikle bir kez yazılabilen manyetik ortam tercih edilmelidir.

17. Yapılan inceleme, denetim ve belgelemelerin ardından el konulacak bilişim malzemeleri, tüm kabloları ve fişleri daha sonra tekrar takabilmek üzere etiketlenerek yerlerinden sökülmeli, delil torbalarına yerleştirilmeli ve mühürlenmelidir. El konulan malzemenin kendi enerji bileşeni varsa (şarjlı pil, pil vb.) kesinlikle sökülerek muhafaza altına alınmalıdır.

18. İnceleme maksadıyla el konulan bilişim malzemesinin elektrostatik etkiler, ısı, nem, toz gibi olumsuz etkenlerden koruyacak şekilde

muhafazası için tedbirler alınmalıdır. El konulacak malzemenin büyüklüğüne ve hassasiyetine uygun nakliye tedbirleri uygulanmalıdır.

3.2.1.2. Açık Olan Bilişim Cihazına İlk Müdahale

1. Bilişim ortamının topolojisi (bilgisayar ağı, kablosuz ağ, kızılötesi, bluetooth, internet bağlantısı vb.) öncelikle tespit edilmeli, uzaktaki bir cihazda delil bulma ihtimaline göre inceleme genişletilmeli ve/veya derinleştirilmelidir. Soruşturmanın niteliğine göre uzaktan erişimle delillerin kaybolmasını ve karartılmasını engellemek için alınması gereken koruma tedbirleri planlama aşamasında belirlenmeli ve tereddütsüz uygulanmalıdır (gerektiğinde ağ kablosunu çekmek, modemi kapatmak vb.).

2. Cihaz üzerinde tutulan verilerin bit dizgisi şeklinde birebir kopyası (klonlama) alınmalı, alınan kopyalardan biri şüpheli/şüphelilerin hukuki temsilcisine tutanak ile teslim edilmek üzere olay yeri sorumlusuna iletilmelidir.

3. Tespit edilen anormalliklere karşı (sabit diskin işlemde olduğunu gösterecek şekilde ışığın aniden yanıp sönmesi, ethernet portu lambasının uzaktan bir erişimin olduğunu gösterecek şekilde yanması gibi) yapılacak işlemler önceden belirlenmelidir.

4. Öncelikle cihazın açık olup olmadığı kesinlikle tespit edilmelidir. Bazı durumlarda *uyku* modunda veya *hazırda bekle* modunda bekleyen cihazlar kapalı sanılarak gücü kesilmekte, bu nedenle delil kayıplarına neden olunmaktadır.

5. Açık bulunan cihazın ekranda parola soran penceresi olup olmadığı kontrol edilmelidir. Cihazı çalıştırmak için parola soruluyorsa bilinen,

öğrenilen ve doğruluğundan emin olunan parola girilerek sistem açılmalıdır. İlk müdahale ortamında uzman personelin bulunması durumunda parola kırılması gibi gerekli işlemler yapılabilir. Ancak bu işlemin uzun zaman alacak olması veya işe yaramaması durumunda cihazın **gücü kesilerek** kapatılmalıdır.

6. Cihaza girildiği takdirde sistem saati, o anda çalışan tüm işler, en son yapılan işlemler ile uzaktaki cihaza ve/veya uzaktaki cihazdan bir erişimin varlığı kontrol edilmeli ve ivedilikle kayıt altına alınmalıdır. Uzaktaki bir cihaza bağlı ise bu cihaza fiziksel olarak ulaşılmalı, mümkün değilse veriler ivedilikle kopyalanmalıdır.

7. Cihazın herhangi bir harici yedekleme birimine erişiminin olup olmadığı kontrol edilmelidir. Erişim o anda aktif ise ve erişilen yedekleme birimine el konulma ihtimali yoksa ivedilikle söz konusu cihaz verilerinin kopyası alınmalıdır.

8. Toplanabilecek tüm delillerin cihazın açık olan ilk halinde toplanmasına özen gösterilmelidir. Cihaz açık iken **olay yerindeki sayısal deliller konusunda önerilen tasnif** bölümünde listelenen verilerden planlamaya uygun olanlar toplanmalıdır. Cihazın kapatılması durumunda bazı delillerin kaybolması ihtimali göz önünde bulundurulmalıdır.

9. Açık olan çevre birimlerinin kapatılmadan önce ön belleklerinde ve iş kuyruklarında bir dosyanın olup olmadığı tespit edilmeli ve imkân dâhilinde bunların çıktıları alınmalıdır.

10. Soruşturmanın ileri aşamalarında kullanılmak üzere açık olan yazılım veya internet sayfalarının varsa şifreleri değiştirilmelidir. Buna ilave olarak sistemde kurulu olan bir şifreleme veya koruma yazılımı var ve

aktif ise bu şifreler de değiştirilmelidir. Şifre değiştirme imkânı yoksa bu yazılımlar ile şifrelenen dosyaların ivedilikle kopyası alınmalıdır.

11. Cihaz o anda bir iletişim ağına bağlı ise (internet dâhil) web kamera ile iletişim ve sohbet programlarının çalışıp çalışmadığı kontrol edilmeli, çalışıyor ise görüşülen şahıslar tespit edilmeye çalışılmalıdır.

12. Ağa bağlı olan bir cihazın o anda her hangi bir dosya indirmesi (download) veya yüklemesi (upload) yapıp yapmadığı tespit edilmelidir. Bu işlemleri yapmak maksadıyla yüklü bulunan yazılımların indirdiği veya yüklediği dosyalara ayrıca dikkat edilmelidir.

13. Yapılan inceleme, denetim ve belgelemelerin ardından cihaz kesinlikle normal kapatma yöntemleri kullanılarak kapatılmamalıdır. Normal kapatılması halinde cihazın çalışırken tuttuğu tüm geçici dosyalar, geçici kayıtlar, kısa yollar, link dosyaları, swap dosyaları, hazırda beklet dosyaları, internet önbellek ve geçmiş dosyaları gibi delil niteliği taşıyan bilgiler kaybolacaktır. Söz konusu bilgilerin kaybolmasını önlemek maksadıyla doğrudan güç irtibatı kesilerek cihaz kapatılmalıdır.

3.2.1.3. Kapalı Olan Bilgisayara İlk Müdahale

1. Öncelikle bilgisayarın kapalı olduğundan emin olunmalıdır.

2. Olay yerinde kolluk birimleri dâhil olmak üzere hiç kimsenin bilgisayar sistemini çalıştırmasına izin verilmemelidir.

3. Cihaz üzerindeki sabit ve/veya taşınabilir disk/bellekler uzman personel tarafından sökülerek, söz konusu bileşenlerin bit dizgisi şeklinde birebir kopyası (klonlama) alınmalı, alınan kopyalardan biri

şüpheli/şüphelilerin hukuki temsilcisine tutanak ile teslim edilmek üzere olay yeri sorumlusuna iletilmelidir.

3.2.2. Sayısal Delil İçeren Bilişim Ürünlerinin Muhafazası

Polisin Adli Görevleri Yönetmeliğinde delillerin toplanması, muhafazası ve ilgili yerlere gönderilmesi ile ilgili hususlar düzenlenmiştir. Bu yönetmelik, kolluk birimlerinin kanunlarda suç sayılan fiil ve hareketlerin ortaya çıkmasıyla başlayan adli görevlerin yerine getirilmesi, suç ve sanıklarıyla ilgili delillerin tespiti, toplanması ve muhafazası, ambalajlanması, ilgili yerlere gönderilmesi ve bu konulara ilişkin diğer hususları kapsamaktadır (Öztürk ve Erdem, 2006).

Toplanan delillerin yapılacak olan duruşmada kullanılabilir durumda korumak için yapılan işleme delilin muhafazası denilmektedir (Öztürk ve Erdem, 2006). Olay mahallinde bulunmasından mahkemeye delil olarak sunulmasına kadar geçen süre içerisinde korunması sağlanamayan delil, ne kadar bilgilendirme potansiyeline sahip olursa olsun geçersiz sayılabilir.

Soruşturma veya inceleme tamamlanıncaya kadar deliller muhafaza edilir. Deliller, soruşturmayı yürüten makamlarla götürülünceye kadar özel ortamlarda, kilitli yerlerde ve mühürlü olarak muhafaza edilmelidir (Öztürk C., 2006). Delillerin muhafazasında gösterilen özen, delillerin yargı önünde geçerlilik şartını sağlayacaktır.

Olay yerinde etiketlenmesi gereken (Salmaner, 1988) deliller, sarsılmayacak ve niteliklerine uygun şekilde ayrı ayrı ambalajlanmalıdır. Deliller olay yerinden muhafaza altına alınacağı mekâna, nitelik ve niceliklerine uygun yöntemlerle nakledilmelidir. Delilin ambalajlama ve nakil işlemleri ayrıntılı olarak belgelenmelidir.

Deliller nicelik ve nitelikleri dikkate alınarak muhafaza tedbirleri geliştirilmeli; her türlü fiziksel, kimyasal ve elektrostatik etkenlere karşı koruma sağlayacak ortamlar belirlenmelidir. Delilin çalınması veya kasti zarar verilmesinin engellenmesi maksadıyla üzerinde çalışılmayan cihazların kapalı olarak tutulması gibi ilave güvenlik tedbirleri geliştirilmelidir. Muhakemenin uzaması ihtimali göz önünde bulundurularak delilin uzun süre muhafaza için teknik ve teknolojik imkânlardan faydalanılmalıdır (Öztürk ve Erdem, 2006).

3.3. Sayısal Delillerin Laboratuvar İncelemelerinde Önerilen İş Akışı

3.3.1. Adli Bilişim Laboratuvarının Önerilen Teknik Özellikleri

Sağlıklı, hızlı ve düşük maliyetle sayısal delil elde edilebilmesi için her şeyden önce incelemenin yapılacağı laboratuvar ortamının, aşağıda belirtilen idari hususlarla desteklenen fiziki şartları sağlanmalıdır:

1. Delillerin fiziki güvenliğinin sağlanması maksadıyla laboratuvarın fiziki güvenlik tedbirleri (kilit sistemi, gözetleme sistemi, yangın ihbar ve önleme sistemi, vb) alınmalıdır **(*fiziki*)**.

2. Delillerin saklandığı mekân ile incelemelerin yapıldığı mekân fiziksel olarak aynı yerde olmalıdır **(*fiziki*)**.

3. Aynı anda birden fazla incelemenin yapılabilmesine imkân veren mekân genişlikleri ve oda düzenlemeleri sağlanmalıdır **(*fiziki*)**.

4. Adli incelemelerin kesintiye uğramaması ve delil kaybına engel olunabilmesi için laboratuvarın elektrik tesisatında elektriksel dalgalanmalara engel olacak çözümler kullanılmalıdır (kesintisiz güç kaynağı, jeneratör gibi) **(*fiziki*)**.

5. İncelenecek cihazların elektrostatik ve elektromanyetik açıdan güvenliğinin sağlanması maksadıyla laboratuvar gerekli yalıtıma sahip olmalıdır **(*fiziki*)**.

6. Bilişim cihazlarının toza karşı hassasiyeti nedeniyle muhafaza edildiği mekânlarda toz yalıtımı sağlanmalıdır **(*fiziki*)**.

7. Ortamın en uygun ısı ve nem düzeyinde (18 ^{o}C – 21^{o}C ısı, %20 - %50 nispi nem) tutulmasını sağlayacak iklimlendirme tertibatı kurulmalıdır **(*fiziki*)**.

8. Bilişim malzemesinin sökülüp takılabilmesi ve inceleme yapılabilmesi için gerekli her türlü teçhizat (alet, ölçüm cihazı, donanım, yazılım) bulundurulmalıdır **(*fiziki*)**.

9. Laboratuvara giriş ve çıkışlar denetim altına alınmalı, denetimsiz ve izinsiz her hangi bir bilişim malzemesinin giriş ve çıkışına engel olunmalıdır **(*fiziki ve idari*)**.

10. Yürütülen tüm adli incelemelerin kayıt altına alınabilmesi amacıyla laboratuvarın 24 saat esasına göre yüksek çözünürlükte kamera kaydı alınmalı ve bu kayıtlar yapılan işlemlerin ibrazı için saklanmalıdır **(*fiziki*)**.

11. Laboratuvar kapsamında uzmanlaşma sağlanmalı, gelen materyal uzmanlık alanlarına göre ilgili birim/personel tarafından incelenmelidir. Daha üst uzmanlık gerektiren vakalarda (kriptografi, mali suçlar, görüntü işleme, vb.) güvenilir irtibat noktaları (uzman personel) önceden tespit edilmeli ve koordinasyondan çekinilmemelidir **(*idari ve fiziki*)**.

12. Teknik incelemelerde bir iç denetim mekanizması oluşturulmalı, incelemelerin başka bir uzman tarafından denetlenmesi sağlanmalıdır **(*idari*)**.

13. İncelenecek cihazda başka disiplinleri ilgilendiren bir izle karşılaşılması durumunda (kan, parmak izi, mermi kovanı, vb.) öncelikli ve kontrollü olarak bu izlerin değerlendirilebilmesi maksadıyla gerekli koordinasyonların yapılabilmesi için gerekli donanım ve bilince ulaşılmalıdır **(*idari*)**.

14. Hangi vasıta ile elde edilmiş olursa olsun, incelemeye alınacak olan bilişim malzemelerinin laboratuvara girmesinden inceleme sonrası iadesi arasında geçen süreçte belgeleme son derece önemlidir. Delilin teslim alınması ve ambalajlarının çıkarılması işlemlerinde delilin tüm nitel ve nicel özelliklerinin belirlenmesi ve tutanak altına alınması maksadıyla kamera kaydı dışında ilave teknik ve/veya idari tedbirler (incelemelerde ses kaydı yapılması, kontrol listesi doldurulması, vb.) alınmalıdır **(*idari ve fiziki*)**.

15. Laboratuvar personelinin dinlenme ve toplantı gereksinimlerinin karşılanması maksadıyla gerekli mekân düzenlemeleri yapılmalı, incelemeler esnasında özellikle sıvı malzemelerin (su, çay, kahve, vb) tüketimi konusunda hassasiyet bilinci artırılmalıdır **(*idari ve fiziki*)**.

16. Adli bilişim incelemelerinde olayın hikâyesi önem taşımaktadır. Bu nedenle inceleme maksadıyla gelen teçhizatın ne amaçla geldiğinin bilinmesi maksadıyla tutulacak kayıt ve tutanaklarda bilmesi gereken prensibine göre olayın hikâyesinin yer alması sağlanmalıdır **(*idari*)**.

17. Adli bilişim laboratuvarında yürütülen tüm faaliyetlerin takibinin yapılması ve personel, olay ve incelenen teçhizata ilişkin istatistiksel değerlendirmelerinin yapılabilmesi için bir **laboratuvar yönetim**

sistemi (yazılım) oluşturulmalıdır. Delilin geldiği andan raporun gönderildiği ana kadar tüm sürecin takip edilebileceği çok amaçlı bu tür bir sistem sayesinde yeni katılan personelin eğitim süreci kısalacak ve kalitesi artacaktır **(*idari ve fiziki*)**.

3.3.2. Adli Bilişim Laboratuvar İncelemesinde Önerilen İş Akışı

Adli bilişim çalışması öncesi ayrıntılı bir çalışma planı çıkarılmalıdır. Olay türü, inceleme sorumlusu, delil üzerinde çalışacak uzman personel sayısı ve niteliği, incelenecek malzemenin fiziksel özellikleri, incelenecek veri türleri, incelenecek işletim sistemi, tahmini inceleme süresi gibi konular planlamada esas alınmalıdır. Adli bilişim incelemesinin omurgasını teşkil edecek olan planlama statik ve standart bir süreç değildir. Her olay ve delil kendi koşullarında incelenmelidir. Bu nedenle her planlama, ortak parametreleri barındırsa da farklılıklar gösterecektir.

Her olay ve delil türüne göre farklılaşan adli bilişim incelemesinin, sayısal delilde **bütünlük, doğruluk, doğrulanma, inkâr edilemezlik ve yeniden ele alınabilirlik ilkeleri** ile aşağıdaki kurallara uygunluğu adli sürecin tüm tarafları açısından delilin geçerliliğini güçlendirecektir:

1. Araştırma esnasında soruşturma veya kovuşturma ile ilgisi olmayan ancak başka bir suçun işlendiği şüphesini uyandırabilecek bir delil elde edilirse bu delil koruma altına alınmalı ve durum ivedilikle savcı bilgilendirilmelidir.

2. Adli bilim uygulaması kapsamında kullanılacak tüm cihaz ve yazılımların marka, model ve lisans durumları kayıt altına alınmalıdır.

3. Adli bilişim uygulaması esnasında kullanılan yazılımlar, teknikler ve işlem adımları ayrıntılı olarak kayıt altına alınmalı ve adli bilişim

uzmanı tarafından olaya özel hazırlanan yazılım varsa bu yazılımlara ait kaynak kodlar belgelenmelidir.

4. Bilişim sisteminin fiziksel varlığı olan donanım incelemeleri tamamlanmalıdır. Mevcutsa olay yerinden alınan fotoğraf ve görüntüler ile karşılaştırmalı inceleme yapılmalıdır.

5. Bilişim sistemindeki donanım uyuşmazlıkları ve eksiklikleri tespit edilerek kayıt altına alınmalıdır.

6. Sistemdeki veri depolama aygıtlarında bulunan tüm bilgiler, üzerinde çalışılması ve silinen verilerin kurtarılabilmesi için *bit dizgisine* göre yedeklenmelidir (klonlama). Olayın hassasiyet derecesine göre çift (gerekirse daha fazla) yedekli olarak incelemelere başlanmalıdır. Veri üzerine yapılacak incelemeler asıl kaynağından değil, kesinlikle yedekleme üzerinde yapılmalıdır.

7. Yapılacak adli bilişim uygulamasında inkâr edilemezliğin sağlanması yani ilk olay verisinin orijinal hali ile kullanıldığına dair teknik ispatın yapılabilmesi maksadıyla alınan yedeklemelerde özet (hash) fonksiyonları ve zaman damgaları (time stamping) kullanılmalıdır.

8. Şifre ve kullanıcı adı gerektiren veri çözümlemeleri (işletim sistemine giriş, yazılımlara giriş, şifre ile korunan dosyalara giriş vb.) için şifrelerin kırılması için bilinen şifreler denenmeli ve/veya şifre kırma yazılımları kullanılmalıdır. Şifrenin kırılamaması durumunda ayrıntıl olarak raporlanmalıdır.

9. Donanım incelemesinin tamamlanması ve yedeklemenin alınmasını müteakip bu çalışmanın **olay yerindeki sayısal deliller konusunda önerilen tasnif** bölümünde listelenen bilgilerden mevcut olanlar tespit edilmeli ve tasnif edilerek kayıt altına alınmalıdır.

10. Veri depolama maksadıyla kullanılan cihazlardan silinen veya hasar gören cihazlardaki (kırılan, yanan disk, CD vb.) veriler, veri kurtarma konusunda uzmanlaşmış yazılımlar ve donanımlar kullanılarak kurtarılmalıdır.

11. Sistem üzerinde bulunan dosya türlerinin orijinal veya sonradan türünün değiştirilmiş olma durumları (örneğin asıl resim dosyası olarak üretilmiş bir dosyanın uzantısının değiştirilerek fark edilmemesinin sağlanmasına karşı) denetlenmelidir.

12. Elde edilen verilerde uyumsuzluk kontrolü yapılmalıdır (olması ya da olmaması gereken bir verinin tespiti).

13. Elde edilen ve kurtarılan verilerin birbirleri ile olan ilişkileri tespit edilmeli ve anlamlandırılmalıdır.

14. Uzmanlık gerektiren konular (kriptografi, resim içindeki yazılı mesajların tespiti, mali verilerin denetimi vb.) tespit edilmeli, ilgili disiplinlerdeki uzmanlarla koordineli çalışılmalıdır.

15. Soruşturma veya kovuşturma ile ilgisi olmayan hususlar göz ardı edilerek hedef küçültülmelidir (çocuk pornografisi ile ilgili bir araştırmada, çoklu ortam (resim, video, ses, vb.) dosyalarına ve internet kayıtlarına yoğunlaşılması).

16. Elde edilen, veri, bilgi, dosyalar soruşturma kapsamında kullanılması öngörülen analiz tekniklerine uygun hale getirilmelidir (Telefon kayıtları ve GSM baz istasyonları verilerinin uyumunun sağlanması, zaman çizelgesi uygulanacak verilerin hazırlanması vb.).

17. Olay ve veri türüne göre daha önceden belirlenen anahtar kelimelere göre içerik araştırması yapılmalıdır (kredi kartı sahteciliği ve dolandırıcılığı ile ilgili yapılan bir incelemede elde edilen dosyaların içeriğinde VISA, MASTERCARD, AMERICAN EXPRESS, CVV vb. kelimelerin aranması).

18. Sunuma esas olmak üzere elde edilen veri, bilgi ve dosyaların teknik açıdan ne anlam taşıdığı, hangi uygulamaların nedeni ve/veya sonucu oluştuğu, hangi editörler ile gösterileceği açıklanmalıdır.

19. Elde edilen tüm bilgilerin kâğıt ortamında veya talep edilirse sayısal ortamda dökümü alınarak rapora eklenmelidir. Bilirkişi görüşlerini bir rapor halinde sunmak mecburiyetindedir (CMK, m. 67). Rapor eklerinde elde edilen tüm bilgiler ve elde ediş teknikleri ile eylemin işleniş biçimi teknik açıdan ayrıntılı olarak sunulmalıdır.

3.4. Sayısal Delillerin Değerlendirilmesinde Önerilen İş Akışı

Sayısal deliller; elde edilmesi zor, içerdiği bilgi bakımından çok etkili ve üzerinde tartışmaların eksik olmayacağı bir değerdir. Sayısal deliller üzerinde süregelen tartışmaların asgariye indirilmesi için:

1. **Sayısal delil, hukuki geçerliliğine göre değerlendirilmelidir:** Sayısal delilin öncelikle hukukun temel gerekleri olan akla, maddi gerçeğe ve hukuka uygunluğu denetlenmelidir. İkinci olarak olayla ilişkili olup olmadığı tespit edilmelidir. Son olarak da yargılamadan önce müşterekliğinin sağlanmasına özen gösterilmelidir.

2. **Sayısal delil, teknolojik geçerliliğine göre değerlendirilmelidir:** Sayısal delilin bütünlük, doğrulanma, doğruluk, inkâr edilemezlik ve yeniden ele alınabilirlik ilkelerine göre uygunluğu denetlenmelidir.

Soruşturma evresinde toplanan, tasnif edilen ve yorumlamaya hazır hale getirilen deliller, bir kararın tekâmül etmesi için değerlendirmeye alınmaktadır. Özellikle bilişim cihazlarından elde edilen veri tipi delillerin pek çoğu tek başına bir anlam ifade etmemektedir.

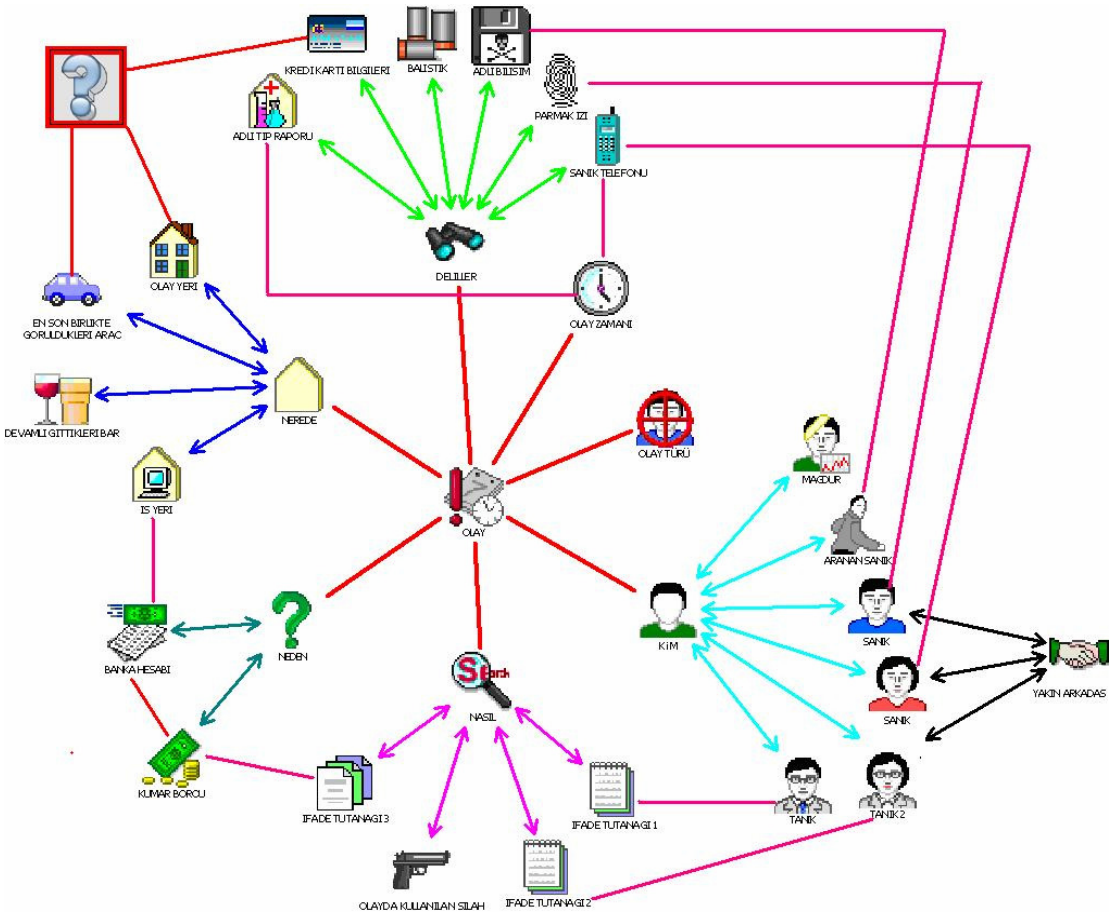
Çok, çeşitli ve standart olmayan deliller arasında ilişkilerin ortaya çıkarılması, değerlendirilmesi ve analizine çok zaman harcanmaktadır. Üstelik sadece insani yetenekler ölçüsünde yapılan analizler hataya açık olma riskini taşımaktadır. Bu tür analizlerde kaynak yetersizliği (zaman ve personel) nedeniyle çeşitliliğe gidilememektedir. Sonuçta delil toplama ve inceleme konusundaki üstün başarı, değerlendirme konusundaki muhtemel zafiyeti engellememektedir.

Suç ve suçluluğun logaritmik olarak artması, buna karşın hukuk sistemi ile ilgili kurum kaynaklarının bu artışa yetişememesi nedeniyle her olayın çözümlenmesi için ayrılan kaliteli zaman ve zinde personel sayısı da azalmaktadır. Bilgisayar destekli değerlendirme ve analiz teknikleri, soruşturma evresinde mevcut olan sorunların asgariye indirilmesi için kullanılabilecek en etkin, hızlı ve düşük maliyetli çözümdür. Olay yerinde toplanan deliller, finans kayıtları, telefon görüşmeleri, arşiv kayıtları, nüfus bilgileri, tanık/mağdur/şüpheli ifadeleri gibi birbirinden farklı karakterdeki delilden; birden fazla yöntemle ve soruşturmacının yeteneği ölçüsünde, etkili sonuçlara ulaşmak mümkündür:

1. **İçerik analizi:** Tespit edilen veriler içinden belirlenen anahtar kelimelere göre içeriğin taranması, eşleştirme ve “serbest metin” analiz tekniklerini ifade etmektedir. İçeriğin taranması için kullanılacak anahtar kelimeler, alay türüne ve soruşturmacı veya uzman personelin yaratıcılığı ile sınırlıdır. Bir terör soruşturması kapsamında incelenen bir bilişim cihazında içeriğinde “**bomba, silah, eylem, Ankara, PKK**,”

kelimelerini içeren dosyaların aranması bu tekniğin konusunu teşkil etmektedir.

2. **Görsel analiz:** İnsanların resim, video, çizelge gibi görsel materyalleri görsel olarak yorumlama ve anlama melekelerinin, aynı içerikteki metin açıklamalarını okumaktan daha yüksek olduğu gerçeğinden hareketle olay ve olaya ait tüm maddi unsurların bir ekranda görsel motiflerle ifade etme tekniğine dayanmaktadır. Bu yöntem, soruşturmada eksik kalan noktaların tespitinde kolaylık sağlanmaktadır. Soruşturma konusu olan olayla ilgili elde edilen tüm veri ve delillerin birbirleri ile ilişkili olarak görsel olarak sunumu *elde edilmesi gereken delillerin ve soruşturmada odaklanılması gereken hedeflerin* tespitinde yardımcı olmaktadır.

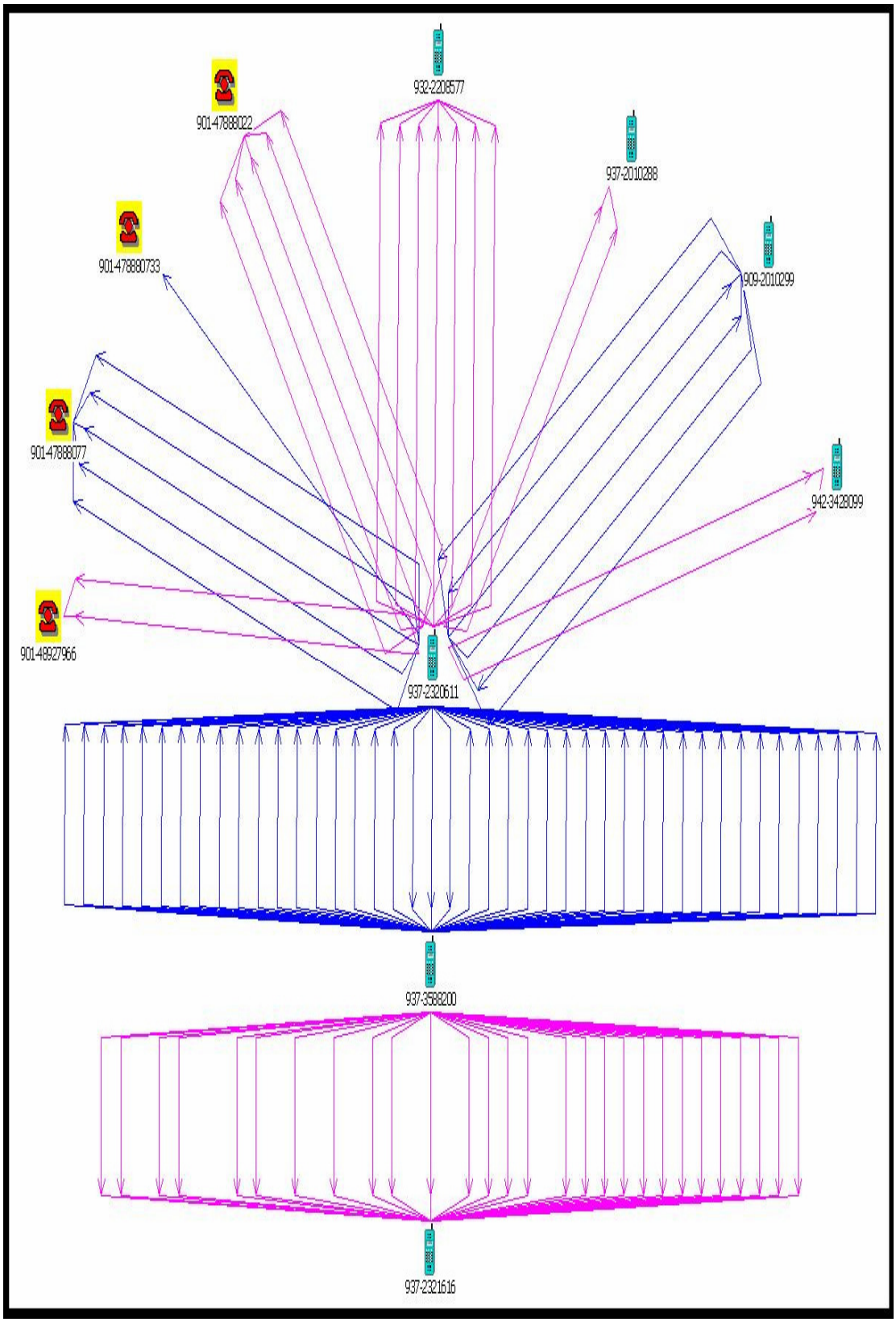


(I2-Analyst's Notebook Yazılımında örnek veri ile hazırlanmıştır)

Şekil 3.4.1. Görsel analiz örneği

3. **Mükerrerliklerin tespiti ve Eşleştirme:** Birden fazla kaynaktan gelen delil ve veriler içinde mükerrerliklerin olması doğal bir sonuçtur. Bazen gereksiz verilerin temizlenmesi, bazı durumlarda da aynı tür verilerden gizli ilişkilerin tespit edilmesi maksadıyla bu teknik kullanılmaktadır (birden fazla dokümanda aynı ve/veya benzer isme rastlanması gibi). Örneğin, özel eşleştirme algoritmaları kullanılarak mevduat sahiplerinin kimlik bilgilerini de içeren farklı bankalara ait binlerce banka hesabı içinden; JOHN D. DHEXMI, J. DANIEL DHEXMI, JOHN DANIEL DHEXMI, J.D. DHEXMI, JOHN DANY DHEXMI, J.DANY DHEXMI isimlerine ait hesapların aynı kişiye ait olduğunun tespiti bu tekniğin en yaygın kullanımıdır.

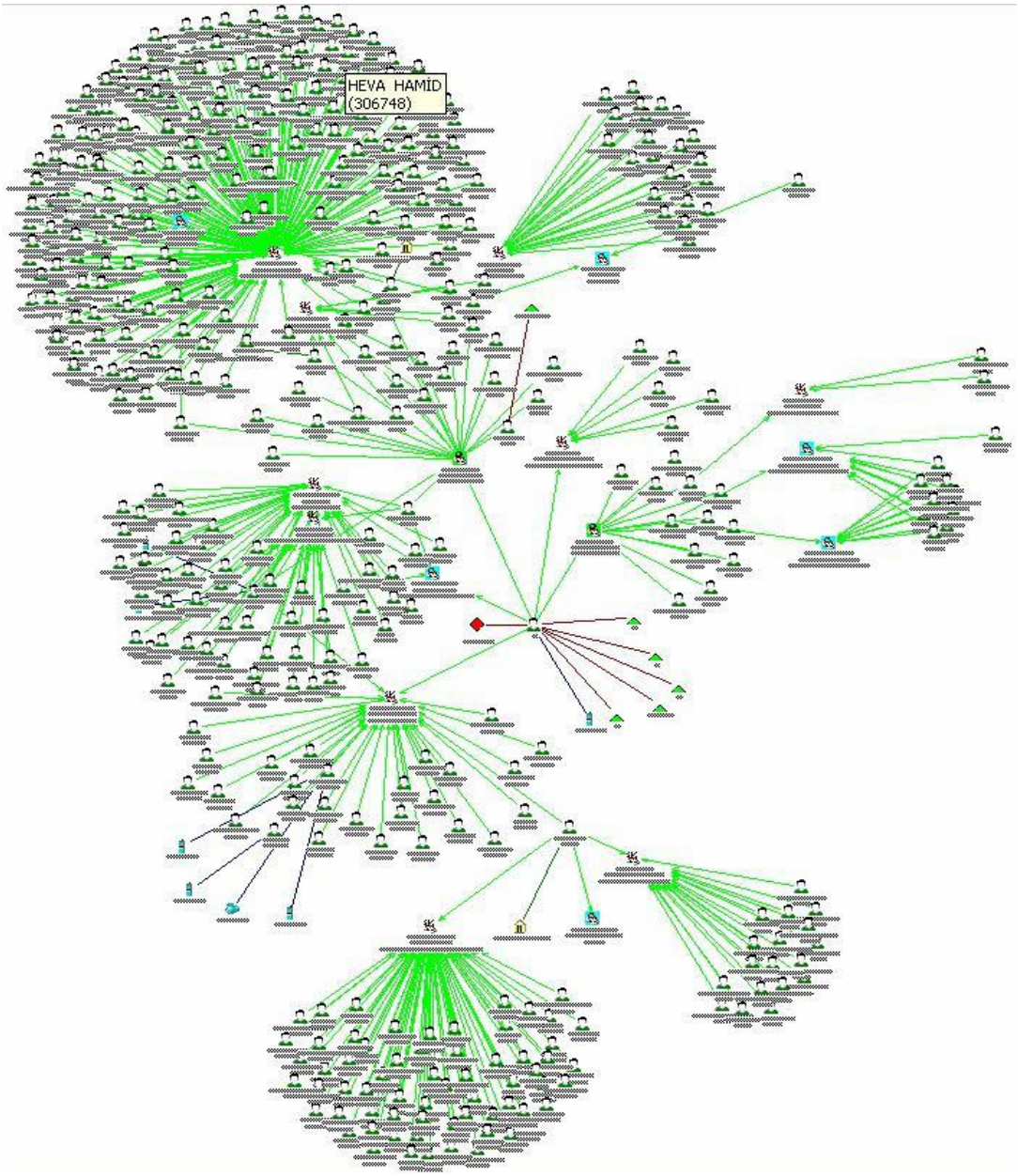
4. **İlişki analizi:** Tek başına anlamsız olan ve insan gücü analizleri mümkün olmayan yığın şeklinde veri içinden gizli ilişkilerin ortaya çıkarılması maksadıyla kullanılmaktadır. Özellikle telefon görüşmeleri ve mali kayıtların incelemesinde sıklıkla kullanılan bir yöntemdir. Örneğin binlerce telefon görüşmesinin insan emeği ve gücü incelenmesi ve aralarında mevcut bulunan bir takım ilişkilerin ortaya çıkarılması mümkün değildir. Bu nedenle bu görüşmeler bilgisayar destekli olarak incelenerek, kayıtları bulunan aboneler arasında soruşturmacı tarafından belirlenen sıklıktan daha fazla sayıda yapılan görüşmeler (üçten fazla görüşen aboneler, her gün görüşen aboneler vb.) mercek altına alınmakta olup bu görüşmelerin çevresinde (öncesinde ve/veya sonrasında) yapılan görüşmelerle beraber görsel olarak sunumu sağlanabilmektedir. Bu sayede çoğunlukla perde arkasında kalan asıl faillerin, organizatörlerin veya azmettiricilerin ortaya çıkarılması sağlanmaktadır.



(I2-Analyst's Notebook Yazılımında örnek veri ile hazırlanmıştır)

Şekil 3.4.2. İlişki analizi örneği

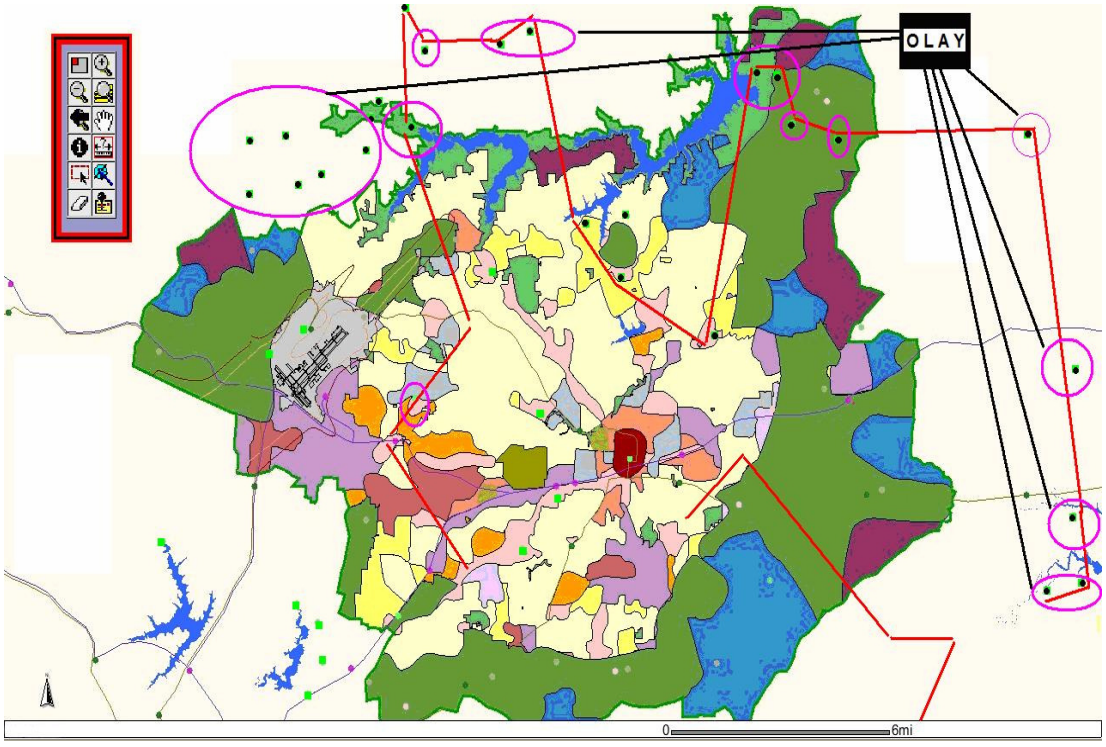
5. **Küme analizi:** Yığın veriler içerisinden yoğunlaşan ilişkilerin tespit edilmesi, bağlantı veya düğüm noktalarının tespit edilerek soruşturmanın yönlendirilmesi maksadıyla kullanılmaktadır. Özellikle organize suç örgütlerinin kilit isimlerinin tespiti için etkili bir yöntemdir. Bir veya daha fazla münferit olaydan elde edilen yığın verilerin (bazı durumlarda milyonlarca) incelenerek bu verilerin yoğunlaştığı noktaların tespit edilebilmesi mümkün olmaktadır.



(I2-Analyst's Notebook Yazılımında örnek veri ile hazırlanmıştır)

Şekil 3.4.3. Küme analizi örneği

6. **CBS (Coğrafi Bilgi Sistemi) analizi:** Soruşturmanın her aşamasında olay, adres gibi coğrafi değeri olan bilgilerin harita üzerinde gösterilmesi maksadıyla kurumun varolan Coğrafi Bilgi Sistemi ile entegre çalışabilen bir analiz tekniğidir. Coğrafi temelli olarak zaman aralıklarına göre suç dağılımları gibi suçluluk analizlerinin yapılmasına ve suç ile coğrafi konum bilgileri arasındaki ilişkinin tespitine imkân sağlamaktadır. Örnekte zanlının kredi kartı harcaması ve tanık ifadelerine göre yolculuk güzergahı ve aynı dönemde bu güzergahtaki hırsızlık olaylarının tespiti amaçlanmıştır.

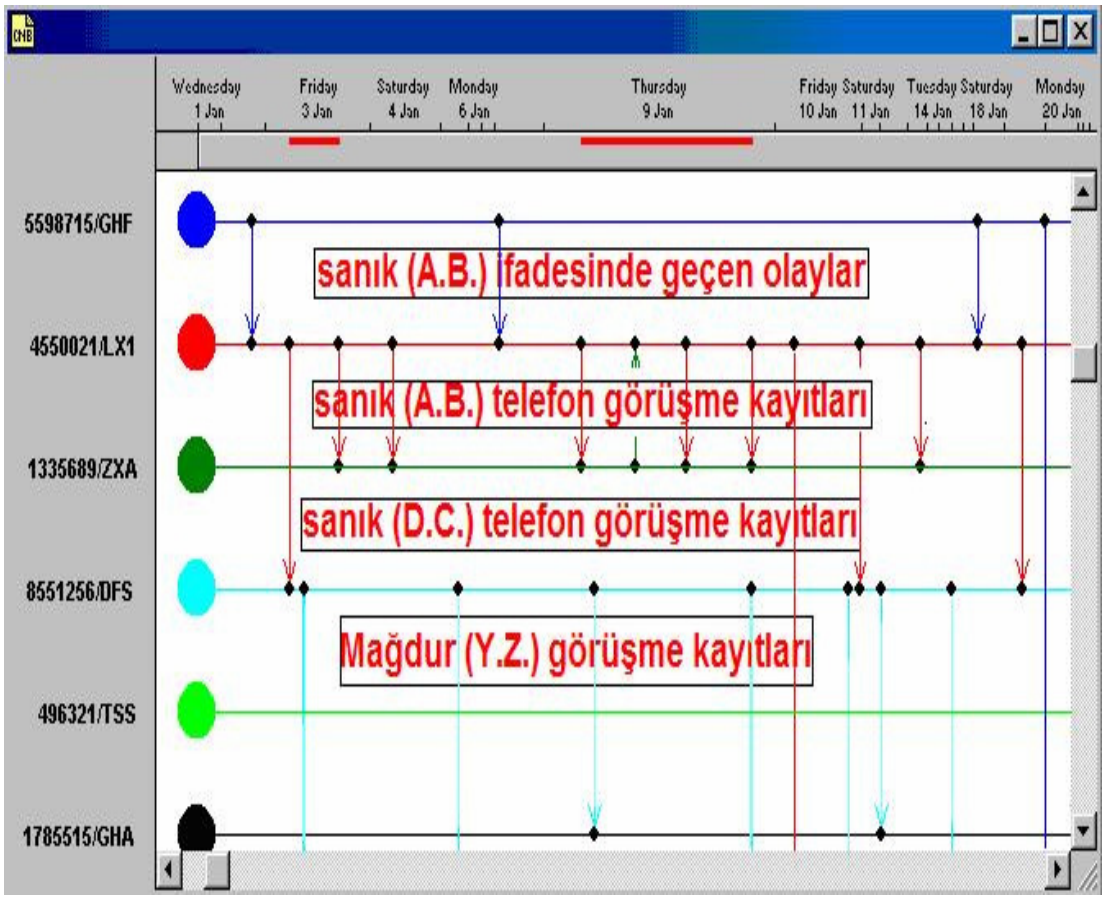


(GIS Vision Yazılımında örnek veri ile hazırlanmıştır)

Şekil 3.4.4. CBS analizi örneği

7. **Olay – zaman analizi**: Elde edilen her tür delilin ve verinin olay ile ilişkisini zaman esasına göre sıralanması ve sonuçlarının görsel olarak gösterimi esasına dayanmaktadır. Bu yöntemle var olan delil ve bilgilerin doğruluğu ve olayın taraflarına ait ifadelerin tutarlılığı onaylanır. Aksi durumda yargılama başlamadan delilin

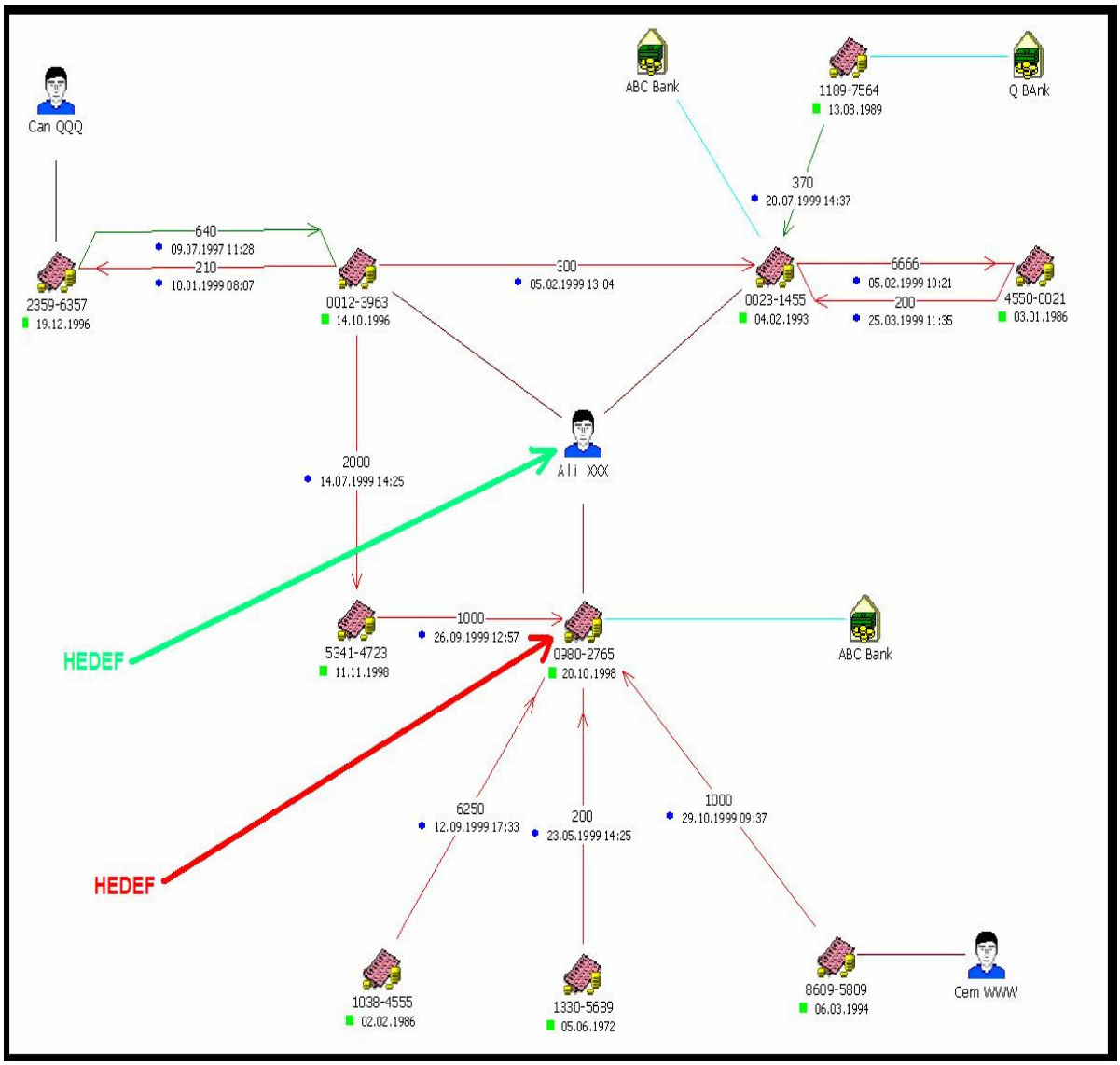
sorgulanmasına neden olarak, hazırlık aşamasının daha sağlıklı yapılmasına imkân sağlamaktadır.



(I2-Analyst's Notebook Yazılımında örnek veri ile hazırlanmıştır)

Şekil 3.4.5. Olay - zaman analizi örneği

8. **Akış (mal – para) analizleri:** Suça konu olan maddi kazanç adli soruşturmaların en önemli delillerinden birini teşkil etmektedir. Suçun maddi unsurları ile fail arasındaki ilişkinin kurulması maksadıyla akış analizleri tekniği kullanılmaktadır. Mali denetimlerde ve suç araştırmalarında sıklıkla kullanılan bu teknik sayesinde paranın ulaştığı son noktaya kadar takibi sağlanabilmektedir. İstendiğinde günlük yapılan binlerce işlem içinden çeşitli kriterlere göre yapılan sorgu sonuçlarına göre (5.000 YTL üzerindeki yurtdışından Türk bankalarına yapılan transferler vb.) analizler üretilebilmektedir.

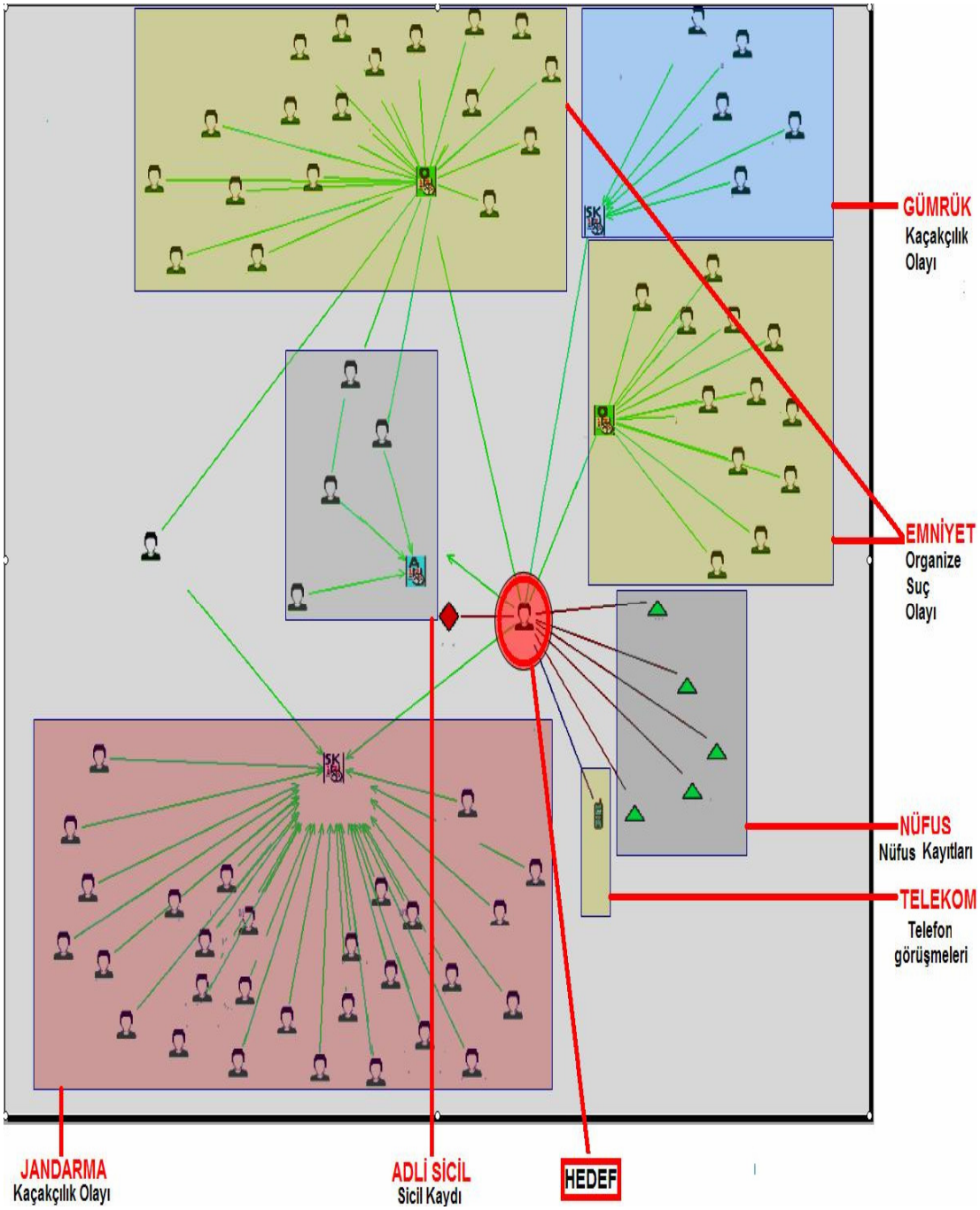


(I2-Analyst's Notebook Yazılımında örnek veri ile hazırlanmıştır)

Şekil 3.4.6. Akış analizi örneği

9. **Örgütlü suç analizi:** Suçların ve faillerinin örgütlü bir suç emareleri taşıyıp taşımadığının tespiti maksadıyla kullanılır. Bu tekniğin uygulanabilmesi için kurumsal olarak olay ve suçlu arşivinin var olması ve diğer bilgilere erişim gereklidir. Bu teknikle suçlu-suçlu, suçlu-olay ve olay-olay bağlantıları kurulabilmektedir. Terör amaçlı örgütler ile organize suç örgütlerinin hiyerarşik çözümlemelerinin yapılabilmesinde en etkin tekniklerden biridir. Bu tekniğin uygulanmasındaki en önemli

unsur hukuk kuralları çerçevesinde tüm kurumların varolan veri kaynaklarını paylaşmaları konusunda göstereceği iradedir. Bu sayede kurumların kendi amaçlarına uygun olarak kayıt altına alıp sakladıkları küçük veriden kamu güvenliğinin sağlanması adına önemli büyük sonuçların çıkarılması sağlanabilecektir.



(I2-Analyst's Notebook Yazılımında örnek veri ile hazırlanmıştır)

Şekil 3.4.7. Örgütlü suç analizi örneği

4. TARTIŞMA

Bilişim cihazlarındaki delillerin tespiti ve değerlendirilmesi ihtiyacı, teknolojinin sosyal yaşamı yoğun olarak etkilemesi ve yönlendirmesi ile ortaya çıkan bir durumdur. Hızlı gelişen, öngörülen ve çoğu bilim insanı tarafından dikkat çekilen bu sürece özellikle ülkemizde kurumlar hazırlıksız yakalanmıştır.

Adli bir olayın vuku bulması ile görevi başlayan kolluk birimleri açısından, bilişim cihazlarındaki delillerin tespiti konusunda kurumsallaşma sağlanamamıştır. İzbilimin (kriminalistik) diğer alt disiplinleri kuraların belirlenmesinde, iş akışlarının oluşturulmasında ve eğitim programlarının oluşturulmasında uygulama birliği sağlamışlardır. Hukuk alanında ileri düzeyde olan ülkelerde adli bilişim ile ilgili kurumlar yaklaşık 10 yıldır faaliyet göstermektedir. Operasyonel birimler ile çok ileri seviyede koordinasyon halinde çalışan adli bilimler laboratuarlarının bünyesinde kurulan adli bilişim laboratuvarlarının yanında sadece sayısal/elektronik/internet suçları ile ilgili özel bir konuda (siber suçlar, siber terörizm, kara para aklama, ileri teknoloji suçları vb.) uzmanlaşmış başka birimlerde faaliyet göstermektedir. Söz konusu birimler sahadaki personelin eğitimini üstlenmekte, müştereken araştırma-geliştirme faaliyetlerini yürütmekte, mevzuat üzerinde çalışmalar yapmakta ve uzmanlıkları ile ilgili olaylara müdahale etmektedirler. Ayrıca başka ülkelerin kendileri ile emsal birimlerinin eğitim faaliyetleri ile ülkelerine kazanç bile sağlamaktadırlar.

Emniyet Genel Müdürlüğü 1998 yılında adli bilişim ve ileri teknoloji suçları ile mücadele alanında faaliyetlerine başlamıştır. Ancak özellikle personel konusunda yeterli yatırımın yapılmaması nedeniyle bugün az sayıdaki yetkin personeli ile bu görevleri ifa etmeye çalışmaktadır. Halen Adli Tıp Kurumu ve J.Gn.K.lığında benzer işlevlere sahip yapılanmalar mevcut

olup benzer sorunlar bu kurumlarda da yaşanmaktadır. Kısacası sorun personelin yetkinliğinde değil sayısal yetersizlik ve kurumsal ilgisizliktir.

Adli bilişim kapsamında güncel olarak yaşanılan vakalar incelendiğinde, müdahale gerektiren cihaz, müdahale yöntemi, aranacak delil türleri hakkında bir işlem, bilgi ve belge standardına ulaşılamamıştır. Düzenlenen raporlarda kurumsal bir standart mevcut değildir. Bir çok olayda, olayın türüne göre bilgisayarın incelemeye gerek olmadığı veya ilk incelemelerin yeterliliği yönünde kişisel inisiyatif kullanılmaktadır. Olay yerinde sadece göze çarpan bilişim malzemeleri yüzeysel olarak incelenmekte, diğer cihazlarda da delil olabileceği düşünülmemektedir. Olay yerinde bulunan başka bilişim cihazları ihmal edilmektedir. Tüm bu tespitlerin ortaya çıkardığı gerçek, adli sürece katkı ve etki yapan kurum ve bireylerde adli bilişim ile ilgili eğitim ve/veya bilinç yetersizliğinin var olduğudur.

Yeterli eğitimin sağlanamaması ve buna bağlı olarak idari tedbirlerin geliştirilememesi nedeniyle ayrıntılı adli bilişim incelemelerinin önemi bilinmemekte ve uygulanmamaktadır. Ayrıntılı inceleme yapılmayan cihaz ve ortamlarda pek çok delil ıskalanmaktadır. Ayrıntılı incelenmesinin uygun görülen cihazlara müdahalede yaşanan yanlışlıklar ve cihazların bir bütün olarak incelenememesi (sadece diskinin incelenmesi) delillerin kararmasına neden olmaktadır. Ayrıntılı incelemenin yeterli uzmanlığı olmayan kişi ve kurumlarca yapılması, delillerin manipüle edilmesine neden olmaktadır. Kısaca **neyin, nerede, nasıl aranıp bulunacağı ve bunların nasıl sunulacağı** konusunda diğer adli bilimlerle ilgili disiplinlere kıyasla kurumsal ve kişisel yeterlilikler oluşmamıştır. Aşağıda verilen kıyaslama, izbilimin ilgi alanına giren delil türleri ile sayısal delillerin kurumsal önemleri konusunda yeterli fikir vermektedir.

			Adli Süreç içinde				
Delil Türü	Bilinme Düzeyi	Geçtiği yönetmelikler	Sertifikalı Uzman Personel Eğitimi	Standart İş Akışı	Standart Raporlama	Standart örnek alma ve delil koruma yöntemleri	Disipline Özel Laboratuvar
Otopsi	Yüksek	Adlî Tıp Kurumu Kanunu Uygulama Yönetmeliği	Var	Var	Var	Var	Var
Biyolojik Deliller	Yüksek	Adlî Tıp Kurumu Kanunu Uygulama Yönetmeliği Emniyet Genel Müdürlüğü Kriminal Polis Laboratuarları Dairesi Başkanlığı ve Kriminal Polis Laboratuvarı Müdürlükleri Kuruluş, Görev ve Çalışma Yönetmeliği Jandarma Genel Komutanlığı Kriminal Daire Başkanlığı ve Bölge Kriminal Laboratuar Şube Müdürlükleri Görev ve Yetkileri Yönetmeliği	Var	Var	Var	Var	Var
Kimyasal Deliller	Yüksek	Adlî Tıp Kurumu Kanunu Uygulama Yönetmeliği Emniyet Genel Müdürlüğü Kriminal Polis Laboratuarları Dairesi Başkanlığı ve Kriminal Polis Laboratuvarı Müdürlükleri Kuruluş, Görev ve Çalışma Yönetmeliği Jandarma Genel Komutanlığı Kriminal Daire Başkanlığı ve Bölge Kriminal Laboratuar Şube Müdürlükleri Görev ve Yetkileri Yönetmeliği	Var	Var	Var	Var	Var
Fiziksel Deliller	Yüksek	Adlî Tıp Kurumu Kanunu Uygulama Yönetmeliği Emniyet Genel Müdürlüğü Kriminal Polis Laboratuarları Dairesi Başkanlığı ve Kriminal Polis Laboratuvarı Müdürlükleri Kuruluş, Görev ve Çalışma Yönetmeliği Jandarma Genel Komutanlığı Kriminal Daire Başkanlığı ve Bölge Kriminal Laboratuar Şube Müdürlükleri Görev ve Yetkileri Yönetmeliği	Var	Var	Var	Var	Var
Sayısal Deliller	Düşük	Adlî Tıp Kurumu Kanunu Uygulama Yönetmeliği	Yok	Yok	Yok	Yok	Kuruluş Aşamasında
İzler	Yüksek	Adlî Tıp Kurumu Kanunu Uygulama Yönetmeliği Emniyet Genel Müdürlüğü Kriminal Polis Laboratuarları Dairesi Başkanlığı ve Kriminal Polis Laboratuvarı Müdürlükleri Kuruluş, Görev ve Çalışma Yönetmeliği Jandarma Genel Komutanlığı Kriminal Daire Başkanlığı ve Bölge Kriminal Laboratuar Şube Müdürlükleri Görev ve Yetkileri Yönetmeliği	Var	Var	Var	Var	Var
Diğer Deliller (Böcek, Polen, vb.)	Orta	Adlî Tıp Kurumu Kanunu Uygulama Yönetmeliği Emniyet Genel Müdürlüğü Kriminal Polis Laboratuarları Dairesi Başkanlığı ve Kriminal Polis Laboratuvarı Müdürlükleri Kuruluş, Görev ve Çalışma Yönetmeliği Jandarma Genel Komutanlığı Kriminal Daire Başkanlığı ve Bölge Kriminal Laboratuar Şube Müdürlükleri Görev ve Yetkileri Yönetmeliği	Var	Var	Var	Var	Var

Şekil 4.1. Delil türlerine göre kurumsal önem kıyaslaması

Bilişim teknolojilerinin suç ilişkisi çoğu kişi tarafından bilişim suçları düzeyinde algılanmaktadır. Oysa olayların pek çoğunda suçta kullanılan veya olayın taraflarına (zanlı, mağdur) ait bir GSM telefon bulunmaktadır. Bu yanılgı, adli süreçle ilişkili kurumların yapılanmalarını da doğrudan etkilemiştir. Bilişim suçları ile mücadele konusunda eksik de olsa yatırım yapan kurumlar, adli bilişim incelemelerinin yapılmasını sağlayacak yeterli bir laboratuvar kuruluşunu gerçekleştirememişlerdir. "**Bir tabela bir oda, bir amir bir memur**" yaklaşımı ile bilişim suçlarıyla mücadele etmeyi yeterli gören kurumların, adli bilişim konusunda daha profesyonel çalışmalara mecbur kalmaları çok uzak değildir.

Henüz adli bilişim adına kapsamlı bir laboratuvarın kurulamadığı ülkemizde, bilişim teknolojileri kullanılarak işlenen suçların çoğu organize suçlar kapsamında değerlendirilmektedir. Organize suç olaylarının gizlilik içinde soruşturulmasında gösterilen hassasiyet nedeniyle bilişim teknolojileri kullanılarak işlenen suçlarla ilgili olay sayısı, işleniş şekli, ele geçen malzeme sayısı, bilişim malzemelerine yapılan adli incelemeler hakkında bilgi almak mümkün olmamaktadır.

Bilişim teknolojileri konusunda mahkemeleri aydınlatmakla görevli olan adli bilişim uzmanlığı konusunda ülkemizde lisans ve lisansüstü eğitimi bulunmamaktadır. Bu disiplin ile ilgili personel ihtiyacı özel kurslar ve görev başı eğitimleriyle giderilmeye çalışılmaktadır. Adli bilişim uzmanlığı, iyi bir bilişim uzmanlığına ilave olarak hukuk ve suçla mücadele yöntemleri ile ilgili eğitime de sahip olunmasını gerektiren uzun soluklu bir tecrübedir. Bu nedenle geniş hukuk ve bilişim müfredatına sahip, kendi içinde uzmanlaşmaya yönlendiren ve her aşamasında saha çalışmaları ile desteklenen bir adli bilişim eğitim programına ihtiyaç duyulmaktadır.

Önleyici kolluk ve güvenlik hizmetleri kapsamında, farklı kaynaklarda aslında var olan milyonlarca verinin yeterince hızlı ve sağlıklı şekilde analiz edilememesi nedeniyle güvenlik zinciri ilk halkasından kırılmıştır. 11 Eylül saldırıları ile zirve yapan bu eski ancak göz ardı edilen ihtiyaç, başta devletler olmak üzere tüm kurumların yeniden yapılanmalarını gündeme getirmiştir. Kurumlar ve bireyler, teknolojinin hayatı zamanla yarıştırdığını, bu nedenle tepki süresindeki anlık gecikmelerin telafi edilemez sonuçlara yol açtığını anlamıştır. Asli sorumlulukları güvenlik olan organizasyonlar, bir uzmanlık alanı olarak sadece veri analizi yapan personel ve birimlere ihtiyaç duyulmuştur. Ayrıca, ses getiren her olayda gündemin bir anda güvenlik zaafiyetine kolaylıkla yoğunlaştırılması, veri analizi ile ilgili personel ve teknoloji yatırımlarını kaçınılmaz hale getirmiştir.

Avrupa Birliği ülkelerinde ve A.B.D.'de operasyonel birimler tarafından sahada elde edilen veri, bilgi ve delilleri değerlendirmekten ve analizler yaparak kolluk birimlerini yönlendiren yapılanmalar mevcuttur. Üstelik adli bilim laboratuvarları, analiz birimleri ve soruşturmacılar farklı sorumluluklara sahip olmasına rağmen olayın başından sonuna kadar müşterek çalışmaktadırlar. Bu esnek ve dinamik yapılanma vuku bulan olayların hızla ve doğru olarak çözümlenmesini sağlamakta, bu sayede adalet mekanizmasının hızlanmasını sağlamaktadır. Üstelik müşterek çalışma kültürü önleyici kolluk görevlerinde önemli olayların olmadan önlenmesi konusunda başarılı sonuçlar üretmektedir.

Ülkemizde adli bilişim konusunda çoğunlukla kişisel çabalarla yetkinlik kazanan personel, genellikle sadece görevlendirildiği alanın dışına çıkmamaktadır. İşbirliği ve birlikte çalışma konusunda kurum içinde/kurumlar arasında yaşanan kişisel/kurumsal direnç ve organizasyon eksikliği nedeniyle arzulanan noktaya gelmek mümkün olmamıştır. Hukuki mevzuatta son dönemdeki yapılan düzenlemeler tek başına yeterli değildir. Yazılı kurallarda yapılan düzenlemelerin başarılı olmasını sağlayacak uygulanmada görev

alan personel teknik bilgi ve değer yaratma kültürü açısından istenen başarı seviyesine ulaştırılamamıştır.

Bilişim cihazlarındaki delillerin tespit edilmesi kadar muhakeme sürecinde karar desteğine esas değerlendirme ve analizlerin yapılması da önem verilmesi gereken bir konudur. Binlerce telefon görüşmesi kaydı arasından anlamlı görüşme trafiğini ortaya çıkarmak veya internet bağlantı kayıtları arasından suçla ilgili olanları süzerek bir zaman çizelgesine yerleştirmek işi **soruşturmacı–adli bilişim uzmanı–mahkeme** üçgeninde ortada kalan bir görevdir. Bu tür analizler için özel bir yapılanmaya gidilmemiş olup birileri tarafından yapılması gereken bu önemli görev sahibini aramaktadır.

Adli süreç, her birinin görevleri yasa ve yönetmeliklere belirlenen kurumlar tarafından müşterek çalışma ile yürütülmektedir. Her kurum, kanun ve kurallara hilaf olmayacak şekilde en doğru, hızlı ve düşük maliyetle görev yapma yöntemlerini belirleme hakkına sahiptir. Ayrıca, ifa ettikleri görevlerle diğer kurumları desteklemektedir. Yasaların kâğıt üzerinde kurduğu bu işbirliği zincirinin son halkası, idari tedbirlerle teorideki işbirliğini pratiğe geçirmektir. Suçla mücadelede gerekli verilerin paylaşımı, bu işbirliğinin en somut ve gerekli uygulamasını oluşturacaktır. Gerek bir takım mevzuat zorlamaları, gerekse kurumsal dirençler, kurumların bu alandaki işbirliğini güçleştirmektedir.

Özünde sıfır ve birlerden oluşan ve yorum yeteneği işlediği verilerle sınırlı olan bir cihazın insan hayatına bir anda bu denli etki yapmasını kabullenmek kolay değildir. Hayatın sosyal yönüne daha dönük bir bilim olarak hukukun ve mesleklerinin doğal getirisi olarak her olayı sorgulama alışkanlığındaki hukuk personelinin, bilişim çağına uyumunun yavaş olduğu gözlenmektedir. Bilişim teknolojilerini yeterince ciddiye almayan, bilişim ile ilgili delilleri başka delillerle ispata çalışan ve teknoloji korkularını mesleklerine yansıtma eğiliminde olan yargı personeli halen mevcuttur. Bu

durumda, sürecin olması gerektiği işlem adımlarında ve zamanda yürümesi mümkün olmamaktadır. Teknolojinin yarattığı sosyal değişimlerin, hukukun temsil ettiği tüm değerlere karşı elde ettiği sahte galibiyet toplumun güvenlik reflekslerini kırmaktadır. Güvenli toplum ve kendine güvenen toplum olarak kalabilmenin ön şartı olarak kabul edilen hukuk yerini hızla teknoloji korkusuna bırakmaktadır.

Bilişim teknolojilerinin kapsama alanına giren suçlar, artık milli sınırları yok saymaktadır. Bilgisayarların kullanımı ile suçun etkinliği, kapsamı ve kazancı büyümüştür. Milli hukuk kuralları ile mücadelenin hiçbir işe yaramadığı artık anlaşıldığından suça eğilim de artmıştır. Teknoloji üreticilerinin ticari kaygıları, devletlerin milli çıkarları ve henüz kayıtsız kalınabilecek düzeydeki sanal suç ortamı, müşterek bir hukuki altyapısının oluşturulması ve uluslararası mücadelenin başlatılmasını engellemektedir.

5. SONUÇ VE ÖNERİLER

Toplumsal ve bireysel dengelerin hızla değiştiği, tüm yaşama kanallarının elektronik sinyaller ile daraldığı, idare etme ve idare edilme felsefelerinin evrensel boyutlarda şekillendiği günümüz dünyasında her olgu kendini bu yeni akışa uydurmuştur. Toplumsal yaşamı şekillendiren ilişkilerde nasıl ki daha önceki dönemlerde teknolojinin yaptığı değişiklikler gözlemlenmişse, bu türden değişimler bilişim ve onu izleyecek ilerlemelerle de sürecektir. Bu nedenle mevcut teknolojiyi reddetmek veya sadece nostalji yaparak geçmişteki ilişkileri, yaşam koşullarını, kurumları veya meslekleri aramak zaman kaybıdır.

Demokratik bir hukuk devletinde bireyler, müdahale ve yargılanma korkusu olmaksızın fikirlerini açıklama, mahremiyet ve haberleşme hakkına sahiptirler. Bireylerin mahremiyeti, devlet, ekonomik düzen ve diğer üçüncü tarafların ihlaline karşı hukuk tarafından korunur. Diğer taraftan ise, tüm devletler kamu güvenliğini korumak ve yurttaşlarının hak ve özgürlüklerini güvenceye almak amacı ile sosyal düzeni muhafaza etmek, suç ve suçlularla mücadele etmek zorundadırlar. Bu evrensel bir ikilemdir.

Suçun bilişimle olan ilişkisinin tespiti, delillendirilmesi ve değerlendirilmesi hususlarında hukuk sistemlerinin göstereceği gelişimin hızı ve kalitesi, toplumun adalete olan güvenini sınamakta kullanılacak bir ölçü olacaktır. Adli sürecin arzu edilen “makul süre” ortalamasını yakalaması ancak, **iş akışlarının eksiksiz olarak belirlenmesi, personelin iş akışlarına uygun olarak görev ve sorumluluklarında uzmanlaştırılması ve kurumsal bir bilgilendirme ve bilinçlendirme sisteminin** kurulması ile gerçekleştirilebilir.

Bu anlamda hâkimler, savcılar, avukatlar, adli kolluk ile adli sürecin diğer bireylerinin düşünce sisteminde, **yazılı hukukun gelişmesine paralel olarak güçlü bir değişimin** gerçekleşmesine ihtiyaç vardır. Yazılı hukuk, kuralları, uygulayanların tutum ve davranışlarıyla şekillenmektedir. Adli sürecin tüm uygulayıcılarında bu olumlu değişim gerçekleşmedikçe ve adliye kültüründe bu yönde bir gelişme yaşanmadıkça amaçlanan değerlere ulaşılması mümkün değildir.

Teknolojinin veya daha özelinde bilişim ve iletişim teknolojilerinin zararları, ancak onu denetleyen kurumların daha iyi örgütlenmeleriyle asgariye indirilebilir. Bu çalışmaya konu olan delillendirme ve delil kavramları, en basit kelime anlamlarıyla, denetim mekanizmasının önemi reddedilemez bileşenleridir. Birey haklarının ve toplumsal menfaatlerin sosyal adalet ilkeleri içerisinde korunması için, **her şartta ve her durumda (sanal ve/veya gerçek) delillendirme** mekanizmasına ihtiyaç duyulacaktır. Bu nedenle idari ve hukuk sisteminde sayısal delillerin kabullenilmesi, tespiti, korunması, kıymetlendirilmesi ve sunulması konusunda güncel müşterek esasların belirlenmesi zorunluluktur.

Teknolojik gelişim, toplumsal değişim ve hukuki zorlamaların ortaya koyduğu gerçek, hukuk içinde adli bilişim disiplinine duyulan ihtiyacın gün geçtikçe artacağıdır. Bu kapsamda;

1. Muhakeme sürecine katkıda bulunan tüm personelin teknoloji korkusunu yenebilmelerini, bilişim teknolojilerinin görev etkinliklerine olumlu katkısına inanmalarını ve adli bilişim uygulamasının temel kavramlarını öğrenmelerini sağlayacak **kurumsal, standart ve sürekli bir eğitim** uygulanmalıdır.

2. Adli bilişimin uygulamalarının kurumsallaşmasını sağlamak, adli bilişim uzmanların eğitiminde görev almak ve gelişen bilişim teknolojisinin hukukla olan ilişkisini araştırmak maksadıyla birbirleri ile **koordineli çalışan adli bilişim laboratuvarları** kurulmalıdır.

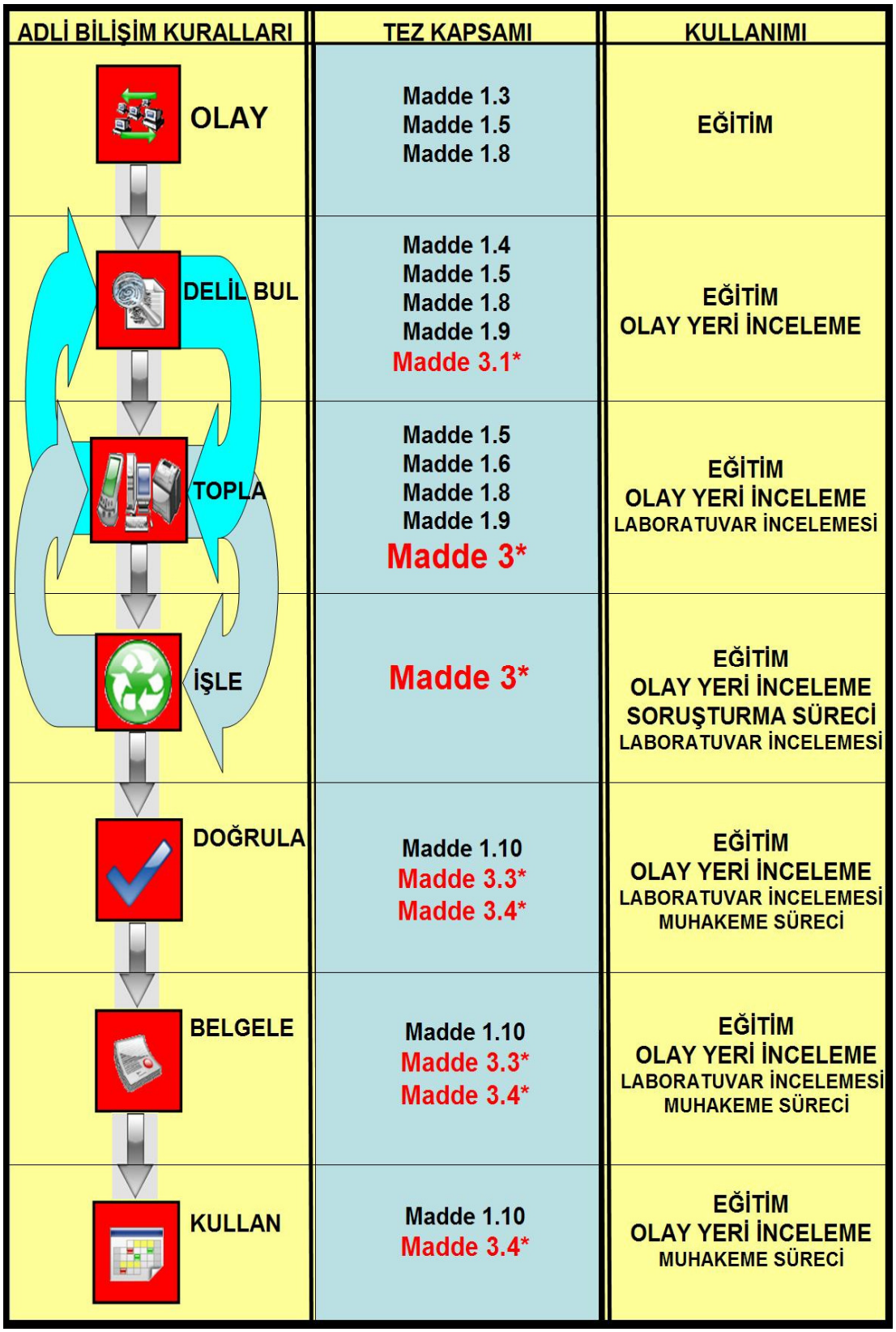
3. Kolluk birimleri, adli bilim laboratuvarları ve savcının **sürecin tamamında müşterek çalışabilmesini** sağlayacak mevzuat ve organizasyon değişiklikleri tamamlanmalıdır.

4. Bilişim cihazlarına müdahale ve ayrıntılı incelenmesi ile ilgili bu çalışma kapsamında **önerilen iş akışları kurumsal bir kural haline getirilmeli**, verilecek olay yeri inceleme eğitimlerinde bu kuralların olaya ve/veya cihaza göre nasıl özelleştirilebileceği öğretilmelidir.

5. Sayısal delillerin değerlendirilmesi konusunda çalışma kapsamında önerilen iş akışı ve analiz tekniklerinin uygulanması konusunda savcı ve hâkim emrinde görev yapacak **bir analiz birimi kurulmalı** veya soruşturmacılara bu konuda ilave eğitimler verilmelidir. Bu amaca yönelik kurumlar arası bilgi paylaşımının sağlanması maksadıyla hukuki, idari ve teknik altyapı oluşturulmalıdır.

6. **Bilişim teknolojileri ile ilgili milli politikaları belirlemek**, ülke genelindeki bilişim faaliyetlerini takip ve yönlendirmek ve bu çerçevede uluslararası koordinasyonları yapmakla **görevli, sorumlu ve yeterince yetkili bir kamu birimi** kurulmalıdır.

7. Üniversitelerle işbirliği yapılarak **adli bilişim alanında lisans** ve/veya yüksek lisans programlarının açılması sağlanmalı, adli bilişim uzmanlığının belgelenebilmesi için müşterek esaslar belirlenmelidir. Bilişim teknolojilerinin veri toplama ve veri işleme kurallarını hukuki mevzuata göre yorumlayan adli bilişim disiplinine ait temel kavramlar olan sayısal delil, sayısal delilin toplanması, işlenmesi, incelenmesi ve değerlendirilmesi kavramlarını ilgili personele daha hızlı ve etkin şekilde öğretmek için bu çalışmanın aşağıda belirtilen iş akışına uygun temel bir kaynak olarak kullanılabileceği değerlendirilmektedir.



* Adli bilişimin en temel ilkelerine göre özgün olarak hazırlanmıştır.

Şekil 5.1. Önerilen tasnif ve iş akışlarının Adli Bilişim disiplinine katkısı

Temel hak ve özgürlüklerin suç korkusuna feda edilmediği, ahlaki kurallara meydan okumayan, kamu güvenlik reflekslerini zaafiyete uğratmayan, teknolojinin tüm nimetlerinden sonuna kadar ve hızla faydalanmaya çalışan bir hukuk anlayışının egemen kılınması, muhasır medeniyetler seviyesine ulaşma çabalarında temel ve öncelikli bir veri olarak algılanmalıdır.

ÖZET

Bilişim Cihazlarındaki Sayısal Delillerin Tespiti Ve Değerlendirilmesinde İş Akış Modelleri

Bilişim teknolojilerinin günlük yaşama biçimlerinde ve yönetim felsefesinde yarattığı büyük değişimden insana dair her husus etkilenmiştir. İnsan olmanın sosyal bir tezahürü olarak suç, bilişim çağında daha da çeşitlenmiş, karmaşıklaşmış ve etkinliğini artırmıştır. Üstelik tehdit kapsamı kolayca ve hızla genişlemiş, sadece bireyler değil kurumlar ve devletler de hedef haline gelmiştir. Suç artık bilişim teknolojileri ile ilişkilidir. Dolandırıcılıktan hırsızlığa, politik cinayetlerden organize suçlara kadar pek çok önemli suçun bir yerinde cep telefonu, bilgisayar veya internet yer almaktadır. Gelişen ve değişen suç ortamı, adli süreçle ilgili kavramları ve görevleri de değiştirmiştir. Delil sayısallaşmış, bilgisayar suç unsuru olmuş, internetin sanal dünyası bir olay yeri haline gelmiştir.

Sayısal delil, sayısal delillerin tespiti ve adli bilişim laboratuvar incelemeleri ve verilerin bilgisayar destekli analizi ve değerlendirilmesi kavramları adli sürece yeni dâhil olan temel kavramlardır. Adli bilimler ile bilişim bilimlerini esas alan adli bilişim disiplininin ana çalışma sahalarını oluşturan bu yeni kavramların ticari kaygılardan arınmış, her şartta uygulanabilir, uzmanlık gerektirmeden anlaşılabilir ve genel esaslara kavuşturulması gereklidir.

Bu hedefle yola çıkan çalışmamızla, bilişim ve hukuki konularda eksik ve yetersiz bilgilere sahip bilişim ve adli personeli “***sayısal delil nedir?, sayısal delil nasıl tespit edilir?, sayısal delil nerelerden bulunur?, olay***

yeri inceleme esnasında sayısal delil tespiti ve müdahale esasları nelerdir?, sayısal delil içeren cihazların laboratuvar incelemesinde esaslar nelerdir?, sayısal delillerin bilgisayar destekli analizi ve değerlendirilmesinde kullanılan teknikler nelerdir?" sorularına uzmanlık gerektirmeyen, anlaşılır ve temel cevaplar bulacaktır. Bu çalışmamızın adli bilişim ile doğrudan ilgili hukuk ve bilişim personeli için başvuru kaynağı olarak; olay yeri incelemesi ve veri analizi ile uğraşan soruşturmacılar, kolluk birimleri ve adli bilişim uzmanları için ise temel eğitim kaynağı şeklinde kullanılacağı değerlendirilmektedir.

Anahtar Kelimeler: Adli bilişim, delil, sayısal delil, sayısal delil tespiti, veri analizi ve değerlendirmesi, bilişim suçu, bilişimle ilgili suç, olay yeri inceleme.

SUMMARY

Models Of Flowchart For Detecting And Evaluating Digital Evidences In IT Equipments

Every matter of human was affected by the great changes that information technologies (IT) created in daily life styles and management philosophy. As a social appearing of being a human, crime, in cyber age became more varied, complicated and increased its effectiveness. Moreover, the range of threat became vast easily and rapidly and not only the individuals but also the organizations and countries became the target. Now, the crime is related to the information technologies. Cell-phone, computer or internet takes part in many important crimes from fraud to theft, political murders to organized crime. The improving and changing crime environment changed the terms and duties related to judicial process too. The evidence digitalised, computer became an element of crime, the virtual world of internet became a crime scene.

The digital evidence, determining of digital evidences and computer forensic laboratory studies, the computer aided analysis of data and evaluation are the main concepts which have just included in judicial process. These new concepts which form the computer forensic discipline's main working areas, based on the forensic and the information technologies should be purified from commercial concerns, understanding without expertise and related to main bases.

With our study, which aims this target, the cyber and judicial staff who is inadequate in cyber and legal issues, will give understanding without expertise and main answers to the questions such as **"what is digital**

evidence?, how can a digital evidence be detected?, what are the bases of interference and digital evidence determination during the crime scene process?, what are the bases of the devices which include digital evidences in the laboratory examination?, what are the computer aided techniques used for during the analysis and evaluating digital evidences?". It is evaluated that our study will be used as a main reference for the judicial and IT staff who is directly related to computer forensic; investigators working on the crime scene investigation and data analysis and main training material for the law enforcement units and IT experts.

Keywords: Computer forensic, evidence, digital evidence, determination of digital evidence, data analysis and evaluation, cyber crime, cyber related crimes, crime scene investigation.

KAYNAKLAR

BAĞDATLI, S.(1995). Temel Hukuk Kavramları. İstanbul, Tabevi Yayınları, s.535.

CARRUTH, D.(2004). *Training for Analyst*. London, NCIS semineri sunumu.

CASEY E.(2004). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition. London, Academic Pres.

CASEY E.(2004). Network Traffic as a Source of Evidence: tool strengths, weakness and future needs, Digital Investigation, Elsevier.

CHISUM J.W.(1999). Crime Reconstruction and Evidence Dynamics, Presented at theAcademy of Behavioral Profiling sunumu, Monterey.

CİHAN, E., YENİSEY F.(1998). Ceza Muhakemesi Hukuku, 3. Tıpkı Bası. İstanbul, Beta Basım Yayım, s.235-250.

CONNOR, T.(2004). Digital Evidence. NCWC Faculty Press.

DEVLET PLANLAMA TEŞKİLATI (2005). e-Dönüşüm Türkiye Projesi 2005 Eylem Planı. Erişim : http://www.bilgitoplumu.gov.tr/2005EP/2005EylemPlani.pdf, Erişim : 17.11.2006.

DÜLGER, M.V.(2004). Bilişim Suçları. Ankara, Seçkin yayınları, s.64-83.

ETTER, B.(2001). Forensics Challenge of e-Crime. University of Western Australia Press.

HOSMER, C. (2002). Proving the Integrity of Digital Evidence with Time. *International Journal of Digital Evidence*. 2002-2.

KAYGISIZ, M.(2003). Adli Bilimler. Ankara, Seçkin Yayınları, s.29.

KAYGISIZ, M., YILMAZ, İ.(2004). Ceza Adalet Sistemi ve Suç Analizi. Ankara, *EGM Polis Dergisi*, Sayı: 39

KAYGUSUZ, Z. (2005). Olay Yeri İncelemesi Çalışmalarında Bilimsellik ve Hukukilik. Ankara, *EGM Polis Dergisi*, Sayı: 42.

KESER BERBER, L.(2004). Adli Bilişim. Ankara, Yetkin Yayınları, s.:39-44.

KORNBLUM, J. (2002). Preservation of Fragile Digital Evidence by First Responders. Digital Forensics Research Workshop Pres.

KUNTER, N., YENİSEY, F. (2003). Ceza Muhakemesi Hukuku, II Cilt, 12.Bası. İstanbul, Beta Yayınları, s.: 564-630.

KUNTER, N., YENİSEY, F. (2005). Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku. İstanbul, Arıkan Yayınları, s.:323-356.

LAWRENCE, R.(2002). Data Forensics Decrypted. Fraud Intelligence.

McCLELLAN, J.(1994). Netsurfers. *The Observer Life*, 13 Şubat 1994.

MESTHANE, E.(1976). Social Change, Technology as a Social and Political Phenomenon. New York, John Viley & Sons.

NELSON, B., PHILLIPS, A., ENFINGER, F., STEUART, C. (2006). Guide to computer forensics and investigations. Boston, Thomson Course Technology.

ÖZDİLEK, A.O.(2004). İnternet ve Hukuk. Ankara Papatya yayınları.

ÖZTÜRK, B., ERDEM M.R., ÖZBEK, V.Ö.(2001). Ceza Muhakemesi Hukuku. Ankara, Turhan Yayınları, s.: 258.

ÖZTÜRK, C.(2006). Ceza Muhakemesinde İz Bilimi. Ankara, Seçkin Yayınları, s.:77-80.

ÖZTÜRK, B., ERDEM, R.(2006). Uygulamalı Ceza Muhakemesi Hukuku. Ankara, Seçkin Yayınları, s.: 178-619.

PANDA, B., GIORDANO, J., & KALIL, D.(2006). Next-generation cyber forensics. Communications of the ACM.

ROBBINS, J.(2002). Computer Forensics. Kruse-Heiser.

SALMANER, H.(1988). Polisin Adli Görevleriyle ilgili El Kitabı. İstanbul, 2.B., s.34.

RONCZKOWSKI, M., COOPER, J., NELSON, E.(2001). Tactical / Investigative Analysis of Targeted Crimes, Results of the First Invitational Advanced Crime Mapping Topics Symposium sunumu. Denver.

SCOTTISH POLICE COLLEGE (2001). “Initial Detective Training Course” Kurs notları. Scotland.

SHINDER, D.L.(2002). Scene of CyberCrime. Syngress Press.

STALLABRASS, J.(1995). Empowering Technology: The Exploration of Cyberspace*, New Left Review*, No. 211, Mayıs-Haziran.

ŞAFAK, A.(1992). Hukuk Terimleri Sözlüğü. Ankara Rehber Yayınları, s.: 94.

TOROSLU, N.(2003). Ceza Muhakemesi Hukuku. Ankara, Savaş Yayınevi, s.:160-191.

TÜRK DİL KURUMU (2007). Erişim: http://www.tdk.gov.tr/tdksozluk/sozbul.ASP?kelime, Erişim Tarihi: 01.03.2007.

TÜRKEKUL, E.(2004). Bilgi Toplumunda Fikri Haklar. İstanbul, Güncel Hukuk, s.26-28.

YENİSEY, F. (2006). Yeni Ceza Adalet Sistemi. İstanbul, Arıkan Yayınları, s.36-75.

YILMAZ, D.(2005). Hacking Bilişim Korsanlığı ve Korunma Yöntemleri. İstanbul, Hayat Yayınları, s.231-379.

YURTCAN, E.(1996). Ceza Yargılaması Hukuku. Ankara, Alfa Yayınları, s.: 46.

WALL, D.(1999). Cybercrimes: New Wine, No Bottles? Invisible Crimes: Their Victims and Their Regulation. London, Macmillan Pres,

WHITTLE, D.B.(1997). Cyberspace: The Human Dimension. New York, W. H. Freeman and Company.

1086 Sayılı Hukuk Usulü Muhakemeleri Kanunu. Kabul Tarihi: 18.06.1927.

5237 Sayılı Türk Ceza Kanunu. Kabul Tarihi: 26.09.2004.

5271 Sayılı Ceza Mahkemesi Kanunu. Kabul Tarihi: 4.12.2004.

5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun. Kabul Tarihi: 04.05.2007.

I2 (2005). Analyst's Notebook Görsel İlişki Analizi Yazılımı. Sürüm 6.0.

GIS Vision (2003). GIS Vision Coğrafi Bilgi Sistemi Yazılımı.

ÖZGEÇMİŞ

I. Bireysel Bilgiler

Adı	:	Mustafa İlker
Soyadı	:	ÖZTÜRK
Doğum Yeri ve Tarihi	:	Ankara 25 MAYIS 1972
Uyruğu	:	T.C.
Medeni Durumu	:	Evli
Askerlik Durumu	:	Muvazzaf Subay
İletişim Adresi ve Telefonu	:	J.Gn.K.lığı Bil.Sis.D.Bşk.lığı II.Yzl. Şb.Md.lüğü Tel : 0 312 456 26 33 Cep : 0 555 583 77 83 Beştepe / ANKARA

II. Eğitimi

1. Yüksek Lisans	:	2005 Gazi Üniversitesi Fen Bilimleri Enstitüsü Elektronik Bilgisayar Eğitimi Anabilim Dalı.
2. Lisans	:	1992 Gazi Üniversitesi Endüstriyel Sanatlar E.F. Bilgisayar Eğitimi Anabilim Dalı.
3. Lise	:	1988 Aksaray Lisesi.
4. İlköğretim	:	1985 Kılıçarslan Ortaokulu. 1982 Zafer İlkokulu.

III. Unvanları : 1992 Programlama Subayı.
2001 İleri Programlama Subayı.

IV. Mesleki Deneyimi : İstihbarat ve Harekat konularında geliştirilen yazılım projelerinde programcı ve tasarımcı olarak göreve başladım. 1997 yılından bugüne kadar yazılım geliştirme proje sorumlusu olarak yaklaşık 50 yazılım projesini yönettim. Yurtiçi ve yurt dışında yazılım geliştirme, kaynak yönetimi, veritabanı yönetimi, tasarım teknikleri gibi bilişim ağırlıklı eğitimlerin dışında 2003 yılında Görsel İlişki Analizi Eğitimi, 2004 yılında Teknik Takip (İngiltere), 2005 yılında Bilişim Suçları, 2006 yılında kurumsal iş zekâsı ve 2007 yılında AR-GE yönetimi konusunda eğitimleri tamamladım. Halen yazılım geliştirme proje yöneticiliği, kurumsal ve kıymetlendirme seviyesi yüksek bir doküman arşivi projesinde tasarımcı ve yönetici, kurumsal iş zekâsı uygulamalarında yönetici ve görsel ilişki analizi proje uygulamasında tasarımcı, geliştirici ve yönetici olarak görev yapmaktayım.

V. Diğer Bilgiler : J.Gn.K.lığı bünyesinde programcıların üst düzey hizmet içi eğitimleri, J.Okll.K.lığında bilgisayar dersleri, bilgisayar destekli istihbarat analizi eğitimi ve kurumsal iş zekası eğitimi gibi seviye ve kapsam bakımından farklı eğitim programlarında eğitmen olarak da görev yapmaktayım.