ADLİ BİLİŞİM

GÜNCEL YAKLAŞIM VE UYGULAMALAR

Hazırlayanlar

Nevin Göksal
Müberra Öztürk

RAPOR

POLİS AKADEMİSİ YAYINLARI

ADLİ BİLİŞİM
GÜNCEL YAKLAŞIM VE UYGULAMALAR

POLİS AKADEMİSİ YAYINLARI

Adli Bilişim
Güncel Yaklaşım ve Uygulamalar

Hazırlayanlar

Doç. Dr. Nevin GÖKSAL
Arş. Gör. Müberra ÖZTÜRK

Polis Akademisi Yayınları: 165
Rapor No: 75
ISBN: 978-605-72770-1-5
2022, Ankara
Tasarım: Yunus Emre Ocak

Sertifika No: 45724
Polis Akademisi Başkanlığı Basım ve Yayım Şube Müdürlüğü,
Fatih Sultan Mehmet Bulvarı No: 218 06200 Yenimahalle – Ankara

POLİS AKADEMİSİ BAŞKANLIĞI
Necatibey Caddesi No: 108 Anıttepe 06400 Çankaya-Ankara/Türkiye
Tel: +90 (312) 4624312 / +90 (312) 4629075 / +90 (312) 4629035
www.pa.edu.tr

İçindekiler

Yönetici Özeti

Bilişim teknolojileri hız üzerine kuruludur. Hız kavramı bir yandan bilişim aletlerinin, aygıtlarının ışık hızına yakın bir işlem yapma kapasitesini, öte yandan ise bu teknolojinin dünya üzerindeki yayılma hızını ifade etmektedir. Bugün yeryüzünde 4,6 milyar internet kullanıcısı bulunmaktadır. Buna her yıl yaklaşık 300 milyon yeni kullanıcı eklenmektedir. 4,2 milyar mevcut sosyal medya kullanıcısına her yıl yaklaşık 500 milyon yeni kullanıcı eklenmektedir. Mobil cihaz kullananların sayısı ise 5,2 milyara yani dünyadaki tüm nüfusun % 66'sına tekabül etmektedir.

Türkiye'de ise Türkiye İstatistik Kurumu'nun 2021 yılı için hane halkı bazlı yaptığı araştırmaya göre 16-74 yaş arası yetişkinlerin % 82'si bir şekilde internet kullanmaktadır. Her 100 haneden 92'sinin geniş bant, yüksek hız ve çeşitli varyasyonlarda internet erişiminin bulunduğu görülmektedir.

Sayılar da açıkça göstermektedir ki; internet eğitimden sağlığa, güvenlikten mal ve hizmet alım satımına kadar birçok alanda hizmet alabildiğimiz çok işlevli bir siber alana dönüşmüş durumdadır. Bu etkileşim kaçınılmaz olarak iki farklı gerçeklik düzlemini bir DNA sarmalı gibi birbirinin içine geçirmektedir. Düzlemlerden ilki bildiğimiz haliyle maddi gerçeklik diğeri ise siber gerçekliktir. Siber gerçeklik tıpkı maddi gerçeklik gibi kendi iyisini ve kötüsünü yaratmış durumdadır. Bu yeni alanda karşılaşılan suç ve suçla mücadelenin hızı deyim yerindeyse dünyanın etrafını saniyede 7 kere dolaşabilecek bir hırsızı kovalamak gibi olacaktır. Bir başka deyişle siber uzayda bizden bir adım önde

olan suçlu ışık hızı ölçeğinde bir adımla öndedir. Dolayısıyla bu yeni alanda zaman, toplum, suç, fail, fiil ve kolluk gibi birçok kavram yeniden tanımlanmaya muhtaçtır. Bir bakıma bu tanımlama ihtiyacı Adli Bilişim alanındaki çalışmaları doğurmuştur.

Adli Bilişim çalışmaları siber alanda işlenen suçları aydınlatmada bilimsel metotlar kullanarak delil incelemeyi ve ortaya koymayı amaçlamaktadır. Bilişim, teknoloji, mühendislik, hukuk gibi interdisipliner çalışmaların bir araya gelmesi ile doğru bilgiye ulaşmayı mümkün kılan bu çalışma alanı kolluğa yeni ve önemli görevler yüklemektedir.

Bu kapsamda, alanda uzman, uygulayıcı ve akademisyenlerden oluşan 50 kişilik katılım ile 3 Kasım 2022 tarihinde Polis Akademisi Anıttepe Yerleşkesinde Adli Bilişim Çalıştayı düzenlenmiştir. Çalıştayda "Türkiye'de ve Dünyada Adli Bilişime Güncel Yaklaşımlar", "Adli Bilişim ve Kolluk Faaliyetleri" ve "Hukuki Perspektiften Adli Bilişim Uygulamaları" başlıkları altında sunumlar gerçekleştirilmiş ve tartışmalar yürütülmüştür. Çalıştay neticesinde ortaya çıkan bu rapor alana küçük bir katkı sunmayı amaçlamaktadır.

Giriş

Adli Bilişim, dijital cihazlar üzerinde gerçekleşen suçların adli delil olarak kullanılabilmesi için yasal prosedürleri takip eden bir disiplindir. Bu disiplin, dijital verilerin toplanması, analiz edilmesi ve sunulması konularında uzmanlaşmıştır. Adli Bilişim uzmanları, özel yazılım ve donanımlar kullanarak dijital verileri toplar, analiz eder ve suçların işlenmesiyle ilgili kanıtları sağlarlar.

Adli Bilişim, sadece adli süreçlerde değil, aynı zamanda dijital güvenlik konularında da önemli bir rol oynamaktadır. Dijital verilerin güvenliği ve bütünlüğünün korunması, kurumlar arasında veya kişiler arasında büyük bir öneme sahiptir ve Adli Bilişim uzmanları bu konuda da uzmanlaşmışlardır. Uzmanların dijital verilerin toplanması, saklanması, analiz edilmesi ve sunulması konularında yasal prosedürleri takip etmesi sağlıklı ve adil bir hukuki sürecin gerçekleşmesi bakımından ciddi önemi haizdir. Buradan hareketle Adli Bilişim disiplinin suçluların yakalanması ve adil yargılanmalarının sağlanması için önemli bir araç olduğu ortaya çıkmaktadır.

Dijital çağın yaşandığı günümüzde dijital verilerin güvenliği ve bütünlüğünün korunması gündelik hayattaki akıştan önemli yasal süreçlere kadar geniş bir alanda önemli bir rol oynamaktadır. Özellikle suç işleme yöntemleri ve delil toplama teknikleri ise giderek karmaşık hale gelmektedir. Bu nedenle, Adli Bilişim gibi disiplinlerin önemi de artmaktadır. Zira suç işleme sürecindeki dijital izlerin toplanması, analizi ve sunulması ile ilgilenen

alan olan Adli Bilişim, bu alanda faaliyet gösteren uzmanları ile bilgi teknolojilerinin kullanımına, suç faillerini tespit etmeye ve nihayetinde adaletin tecellisine hizmet etmektedir.

Adli Bilişim, suç soruşturması sırasında dijital verilerin nasıl toplanacağı, saklanacağı, analiz edileceği ve sunulacağı ile ilgili yöntemler geliştirir. Bu yöntemler, sadece suçlu bulunmasına değil, aynı zamanda masumiyetin de kanıtlanmasına yardımcı olur. Ancak bu noktada birtakım zorluklarla da karşı karşıya kalınabilmektedir. Örneğin, dijital verilerin değiştirilmesi veya silinmesi gibi müdahaleler, doğru sonuçlara ulaşmayı zorlaştırabilmektedir.

Adli Bilişim, çeşitli bilgi teknolojilerinin kullanımını da içerir. Bu teknolojiler arasında bilgisayar korsanlığı, veri kurtarma, veri analizi ve dijital imza gibi alanlar yer alır. Bilgisayar korsanlığı, bir bilgisayar veya ağa izinsiz olarak erişmek veya bunları yönetmek için kullanılan bir yöntemdir. Veri kurtarma, hasarlı veya silinmiş dijital verilerin kurtarılmasına yardımcı olur. Veri analizi, dijital verilerin incelenmesi ve sonuçların çıkarılması için bir yöntemdir. Dijital imza ise, dijital verilerin doğruluğunu ve bütünlüğünü garanti etmek için kullanılır.

Hukuk sistemi de Adli Bilişim alanında önemli bir rol oynamaktadır. Adli Bilişim, hukuk sistemi ile iş birliği içinde çalışarak, suçlu veya suçsuz olduğu henüz kanıtlanmamış kişilerin haklarını korumak için çaba gösterir. Bu noktada adalet zincirinin önemli bir halkası olan kolluk görevlilerine de önemli bir pay düşmektedir.

Adli Bilişim sürecinde, kolluk görevlilerinin rolü oldukça önemlidir. Kolluk görevlileri, dijital verilerin doğru bir şekilde toplanması, saklanması ve analiz edilmesi sürecini yönetmektedirler. Bu süreçte, kolluk görevlilerinin görevleri arasında, ya-

salara uygun bir şekilde dijital verilerin toplanması, muhtemel delillerin ortaya çıkarılması, dijital verilerin güvenli bir şekilde saklanması, doğru bir şekilde analiz edilmesi ve yargı sürecinde kullanılmak üzere sunulması yer almaktadır. Kolluk görevlileri, dijital verilerin yasal prosedürlere uygun bir şekilde toplanmasını ve saklanmasını sağlamak için yasal çerçeveleri yakından takip etmektedirler. Bu süreçte, dijital verilerin Adli Bilişim uzmanları tarafından toplanması, analiz edilmesi ve raporlanması için uygun şekilde yönlendirmelerde bulunmaktadırlar.

Kolluk görevlilerinin Adli Bilişimdeki rolü, dijital verilerin analiz edilmesi sürecinde de oldukça önemlidir. Kolluk görevlileri, Adli Bilişim uzmanları ile birlikte çalışarak, dijital verilerin muhtemel delilleri ortaya çıkarmak için analiz edilmesini sağlarlar. Bu analizlerin doğru bir şekilde yapılabilmesi için, Adli Bilişim uzmanları tarafından kullanılan analiz araçlarının teknik yeterliliğini takip etmektedirler.

Son olarak kolluğun Adli Bilişimdeki önemli bir diğer rolü, dijital verilerin yargı sürecinde kullanılması aşamasına sunduğu katkıdır. Bu aşamada, mahkemelerde dijital delillerin sunulması ve yorumlanması konusunda uzmanlık sağlarlar. Bu süreçte dijital verilerin doğru bir şekilde yorumlanmasını sağlamak için mahkemelerde teknik danışmanlık görevi de üstlenebilirler. Kolluk görevlilerinin Adli Bilişim süreçlerinden aldıkları görevleri yerine getirirken, yasalara ve etik kurallara uygun hareket etmeleri de elzemdir. Bu kapsamdaki düzenlemeler Türk Ceza Kanunu ve ilgili diğer mevzuatta yer almaktadır.

Bu bilgiler ışığında, Adli Bilişimin ne olduğu, bilgi teknolojilerinin suç bakımından rolünün hukuki bir perspektiften irdelenmesi ve nihayetinde kolluğun Adli Bilişim sürecindeki rolü ele alınması gereken güncel ve elzem konular olarak de-

ğerlendirilmiştir. Bu kapsamda, üç bölümden oluşan raporda oturumlarda Polis Akademisi tarafından gerçekleştirilen Adli Bilişim Çalıştayı sırasında gerçekleştirilen sunumlar tematik bir akış oluşturacak biçimde bir araya getirilmiştir. Raporun tamamında ifade edilen yargı ve öneriler katılımcıların bilimsel ve kişisel görüşleri çerçevesinde oluşturulmuştur.

I

Türkiye'de ve Dünyada Adli Bilişime Güncel Yaklaşımlar

"Türkiye'de ve Dünyada Adli Bilişime Güncel Yaklaşımlar" ana başlığı ile düzenlenen ilk oturumda akademisyen ve uygulayıcılardan oluşan katılımcılar sırasıyla "Gelecekte Adli Bilişim", "Adli Bilişimde Güncel Gelişmeler", "Adli Bilişimde Dijital Dezenformasyon ve Deepfake Uygulamaları", "Ulusal Siber Olaylara Müdahale Merkezi'nin (USOM) Siber Güvenlik Dünyasında Adli Bilişim Süreçleri" ve "Adli Bilişimde Kurumlar Arası Bulut Sistemlerinin Kullanılması" başlıklarına ait sunumlarını gerçekleştirmiştir. Yapılan sunumlar ve tartışmalar neticesinde katılımcıların bilgi ve görüşlerinden derlenen bölüm özeti şu şekildedir;

Adli Bilişim

Bilişim teknolojilerinin sürekli olarak değişimi ve gelişimi; insan yaşamına kolaylık sağlamakla ve yeni imkanlar doğurmakla beraber, birçok tehlikeyi de beraberinde getirmektedir. İnternetin sosyal hayattan iş hayatına kadar her alanda kullanılır hale gelmesi, bu alanda işlenen suçların etkinliğini ve kapsamını arttırmaktadır. Siber suçlar ya da diğer adıyla bilişim suçları, kötü amaçlı insanlar tarafından internet ve bilgisayar sistemlerindeki güvenlik açıklıkları kullanılarak işlenmekte; kişilere, kurumlara hatta devletlere maddi veya manevi büyük kayıplar verebilmektedir. Bu durum devletleri tedbir almaya yönlendirmiş;

siber alanda mevzuat boşluklarının giderilmesi için çalışmalar yürütülmüş ve artan uzman kişi ihtiyacı karşısında bu suçlarla mücadele edebilecek beceri ve eğitime sahip kişilerin yetiştirilebilmesi için eğitim ve öğretim kurumlarında çeşitli düzeylerde programlar oluşturulmuştur.

Bilişim sistemleri, bilgisayar ve ileri teknoloji cihazlar olarak değerlendirilen karmaşıklığı ve kabiliyetleri sürekli artan donanım-yazılım tabanlı sistemler için verilen genel bir adlandırmadır. Bu bağlamda bilişim sistemlerinin tüm bilim alanları ile başta hizmet ağırlıklı olmak üzere iş birliği ve kullanımları bulunmaktadır. Bir bilişim sisteminin temelinde ise; verilerin saklanması, saklı olan ya da anında elde edilen verilerin işlenmesi ve anlamlandırılması, ham ya da işlenmiş-anlamlandırılmış verilerin iletilmesinin gerçekleştirilmesi bulunmaktadır.

Salt verilerden anlamlandırmaya giden yolun her kesiminde gittikçe artan katkı bilişim dünyası ile her geçen gün artmaktadır. Bu süreç kısaca; hukukun kabul ettiği en küçük veri parçaları, verilerin düzenli biçimi olan enformasyon, veriler arası ilişkilerin belirlendiği bilgi ve sonuç özet-anlamlı bilgi biçiminde ifade edilebilmektedir. Burada önemli olan ise verilerden neyin anlaşılması ve yorumlanması isteniyorsa ona ilişkin problemin tanımlandığı senaryonun-algoritmanın belirlenmesidir. Örnek olarak kişilerin kredi kartı limitlerinin belirlenmesinde olduğu gibi ilgili kuruluşun müşteri temsilcileri ile kişiler arasındaki ilişkinin kurulması verilebilir. Burada gerekli olan hukuk tanımları çerçevesinde kişisel bilgilerden anlam çıkartmaktır. Dikkat edildiği gibi ilk karşımıza çıkan engel kişilerin verilerine ilişkin hakları olmaktadır. Mevcut bilişim sistemleri bu hakları şu anda test etmemektedir. Verilen bu örnekte senaryo aslında çok yalın olmakla birlikte hukuk bağlamı ile değiştirilmek zorunda kalın-

maktadır. Kısaca yazılacak kodun kimi sınırlar için yeniden olgunlaştırılması gerekmektedir. İçinde yaşadığımız ortamdan kısa bir örnek senaryo da bile karmaşık tanımları içeren bir probleme dönüşebilmektedir. Bu örnekteki durum yazılım dünyasının bilinen ancak pek dillendirilmeyen kesimidir. Herhangi bir problem için her şeyin uygun ortamdaki tanımı kolaylıkla çalışabilir ya da çalıştırılabilir. Bu kesim ancak yazılım oluşturmadaki tasarım ile birlikte belki %20'lik kesimidir. Ancak ortaya konulan problem ve çözümündeki yazılımı içinde bulunduğu koşullarda çalıştırılması istenildiğindeki sorunların giderilmesi ise işin yaklaşık %80'lik kesimi olarak tanımlanabilir. Öngörülmeyen bu sorunlar ve sonuçlar bilişim sistemlerinin korkulu rüyası ancak Adli Bilişimin de ana konularındandır.

Bilişim ya da içinde yaşadığımız sosyal ortamda veri çok önemlidir. Verilerin işlenmesi çok daha önemlidir. Ancak veri anlamlandırma bunların da üzerinde bir önemi haizdir. Bunun günümüzdeki karşılığı büyük veri ve veri madenciliği olarak kurgulanmaktadır. Enformasyon ise veritabanı olarak bildiğimiz formatlı verileri ifade etmede kullanılmaktadır. Enformasyona dayalı çıkarımlar ya da ilişkiler ağı ise kısaca bilgi olarak bilinen kesimi oluşturmaktadır. Burada üretilen ilişkiler ağının kurulması ise insan üstü yeteneklerin oluşturulmaya çalışıldığı makina öğrenmesi, yapay zeka gibi unsurların tanımlandığı ve kullanıldığı kesimdir. Özü itibariyle çok yalın gibi görünmesine karşın oldukça karmaşık yazılım-donanım teknolojilerinin kullanıldığı ve işin yakın gelecekteki kesimidir.

Adli Bilişim özünde hukuk ve bilişimin kesişimi olmasına karşın tüm adli bilimlerle doğrudan ya da dolaylı olarak ilgilidir. Bu ilişkiyi üç ana kesimde özetlemek ya da bakmak mümkün olmasına karşın hiçbir zaman bunların arasında keskin bir sınır çizilememektedir. Bu ilişkileri kısaca; Bilişim sistemlerine karşı

işlenen suçlar, bilişim sistemi kullanılarak işlenen suçlar ve bilişim sistemleri ile suç ve suçluların analizi biçiminde sınıflamak mümkündür.

Genelde Adli Bilişim, adli bilimlerde çok dar anlamıyla "disk inceleme" ya da "sistem- network güvenliği" gibi algılanmaktadır. Oysa bilişim ortam bir hizmet ortamı olarak her noktada bulunmaktadır. Öyle ki bu hukukun toplumun bireyleri arasındaki ilişkilerden insan - makina ya da makina - makina ilişkilerine kadar etkilemektedir ya da etkileyecektir. Bu biçimde değerlendirildiğinde "disk inceleme" ya da "sistem-network güvenilirliği" çok küçük bir kesimini kapsadığı ifade edilebilmektedir. Adli Bilişimin ulaştığı nokta ise bir bakıma Tersine Mühendislik olarak da anılmaktadır. Aslında adli olaylardaki tüm süreçlerin bilişim ortamında gerçekleştirilerek suç ve suçluların bulunması süreçleriyle birebir aynıdır. Bu yönüyle bilgisayar ortamının analiz için kullanılması suçlu profillerinin çıkarılması, büyük veriden suç eğilimlerinin belirlenmesi gibi çalışmalar günümüz öne çıkan konularıdır.

Adli Bilişimin bir hukuk kesişimi de bilişim sistemlerine yapılan saldırı ya da karşı işlenen suçlardır. "Hacker" olarak halk arasında nitelendirilen bu tür girişimlerin niceği ve niteliği her geçen gün artmakta olduğu da görülmektedir. Artık toplumlarda alınır-satılır meta haline gelen veri buradaki hedefi oluşturmaktadır. Fikri mülkiyet ya da yetkisiz erişimler, patent ihlalleri vb. bu tür girişimlerdendir. Oysa bu girişimler batı dünyasında Adli Bilişimin çok önemli ilgili alanlarındandır. Bunların ortaya çıkarılması da yine veri analizleri teknikleri ile sağlanabilmektedir.

Üçüncü olarak adli bilişimin konularından biri de bilişim araçları kullanılarak işlenen suçlardır. Bu suçlara yönelik çalışmalar yapılması da artan ve gelişen bir biçimde önem kazanmak-

tadır. Sonuçta bilişim sektörü herkese açık bir sektördür ve suçluların da elinde son derece gelişkin araçlar bulunmaktadır. Bu durumu virüs programı yazanlar ve virüs engelleyici yazanların arasındaki mücadelede görmek mümkündür. Kim daha önce bir açık bulursa ya bu açığı kullanmakta ya da bulunan açığı kapatarak potansiyel tehlikeyi engellemektedir. Bunun sonucunda oldukça maliyetli bir ortam ortaya çıkmaktadır. Özellikle bu tür bir tehdidin bilişim sistemine olmaması bilgisayar maliyetlerini azaltacağı ya da daha hızlı ve verimli çalışan bilgisayarlara sahip olacağımız gerçeğini ortaya çıkartmaktadır.

Adli Bilişim Zekası

Yapay Zeka ve Makine öğrenimi (ML- Machine Learning), dünya çapında hızla büyüyen moda teknoloji olarak yakın zamanda yerini almıştır. ML teknolojisi, Yapay Zekanın (AI- Artificial Intelligence) bir alt kümesidir ve bilgisayarları programlanmadan yapay öğrenme yeteneği kullanılarak kısaca geçmiş deneyim ve verilerden algoritma üretebilmektedir. Son on yıldan beri, ML teknolojisi, uyarlanabilirlik, sağlamlık, öğrenilebilirlik ve beklenmedik zorluklara karşı gerçek zamanda harekete geçme yeteneği gibi sayısız ilginç özelliğe sahip olduğu için çok çeşitli alanlarda kullanılmaktadır.

Geleneksel siber güvenlik sistemleri kurallar, saldırı imzaları ve sabit algoritmalar üzerine kuruludur. Bu nedenle, sistemler yalnızca kendilerine verilen “bilgi” ile hareket edebilir ve geleneksel siber güvenlik sistemlerinin düzgün çalışması için sürekli olarak insan müdahalesi gerekmektedir. Öte yandan, ML teknolojisi geçmiş deneyimlerden çeşitli kalıpları tanıyabilir ve görülen ya da görünmeyen verilere dayalı (veri madenciliği) olarak gelecekteki saldırıları tahmin etme veya tespit etme yetene-

ğine sahiptir. ML teknolojisi, geleneksel siber güvenlik sistemlerinde mevcut olan çeşitli sorunların üstesinden gelinmesine izin veren büyük hacimli gerçek zamanlı ağ verilerini işleyebilir.

ML algoritmalarının bir bilgisayarın davranışı hakkında varsayımlarda bulunma ve gerçekleştirdiği işlevleri ayarlama yeteneği, aslında onu tehditlerden korumak için bir fırsat oluşturur. Milyarlarca ya da trilyonlarca dosyayı tarama ve potansiyel olarak kötü amaçlı olanları belirleme anaomalileri tespit edebilme kabiliyeti ile, siber güvenlik alanında ML algoritmalarının kullanımı son birkaç yıldır artmıştır. Günümüz senaryosunda, makine öğrenimi kavramı olmadan sağlam, akıllı ve başarılı bir siber güvenlik sistemi hayal etmek neredeyse imkansızdır. ML, siber güvenlik sistemlerine, benzer kalıplara ya da imzalara sahip gelecekteki saldırıları tespit etmek ve önlemek için tehdit kalıplarını analiz etme ve bu deneyimden öğrenme gücü verir. Bu, siber güvenlik sistemlerinin makinelerin değişen davranışlarına yanıt vermesini sağlar. ML, siber güvenlik sistemlerinin kötü niyetli faaliyetleri önlemede akıllıca proaktif olmasını ve aktif saldırılara karşı gerçek zamanlı olarak yanıt vermesini sağlar. ML'nin gücü ile işletmeler, düzenli görevlere harcanan süreyi azalttığı için kaynaklarını daha verimli kullanabilir. Basit bir deyişle, ML siber güvenlik uygulamasını daha basit, daha proaktif, daha etkili ve açıkçası daha ucuz hale getirir.

Ancak, siber suçlular da kötü niyetli amaçları için yapay zeka ve makine öğreniminden yararlanmaktadırlar. Birçok özel ve kamu kuruluşu, siber saldırıları her zamankinden daha etkili bir şekilde belirlemek ve azaltmak için ML kullanıyor olsa da, son derece etkili veri güvenliği sistemleri geliştirmesi için yatırımlarını arttırmaktadırlar. Siber güvenlik alanında ML'ye fazla güvenmek de zafiyet oluşturacaktır. Makine öğrenimi geliştirici-

leri, bir makinenin verilerden her şeyi öğrenebileceğini varsayar, ancak bu her zaman doğru değildir; insan müdahalesi göz ardı edilemez ve alan uzmanları siber güvenlikte çok önemli bir rol oynayabilir. ML, yalnızca ona güvenmeden önce önemli ölçüde iyileştirilmesi gereken gelişmekte olan bir teknolojidir. Dünyanın dört bir yanındaki birçok uzman, AI ve ML'nin kesinlikle siber güvenliğin geleceği olacağını tahmin ediyor olsa da uzman katkısı yatsınamaz.

Bugünlerde siber güvenlikte ML, dünya genelinde hızla büyüyen bir modadır. Dünya çapında tanınmış birçok şirket, Nesnelerin İnterneti (IoT), Büyük Veri ve AI gibi çağdaş teknolojilere yatırım yapmaktadır. Bu nedenle yeni teknolojilerin gelişmesiyle birlikte ML tabanlı güvenlik çözümlerine olan talep de artmaktadır.

ML teknikleri, çeşitli gerçek dünya uygulamaları için yaygın olarak kullanılmaktadır ve siber güvenlik uygulayıcıları, kuruluşlarının siber yönlerini korumak için bunları benimsemiştir. Son on yıldan beri, makine öğrenimi teknolojilerinin siber güvenlik uygulamaları üzerine kapsamlı araştırma çalışmaları yürütülmektedir. ML'nin siber güvenlikte uyarlanması, güvenlik uzmanlarının eksikliğini tamamlayan otomatik güvenlik sistemlerinin geliştirilmesine yardımcı olacağı düşünülmektedir. ML tabanlı otomatik siber güvenlik sistemleri, çeşitli kuruluşların insan kaynaklarına daha az yatırım yapmasına ve verileri insan analistlerinden daha doğru bir şekilde analiz etmesine olanak tanır. Makine öğrenimi modellemesinde veri hazırlamanın önemi sunulmakta ve yanlış-pozitif (false positive) oranları azaltmak ve modern siber saldırıları tespit etmek için doğru şekilde eğitilmiş makine öğrenimi modellerinin etkisi tartışılmaktadır. Alan uzmanlarının kilit rol oynadığı kritik güvenlik senaryolarında insan müdahalesinin ihmal edilemeyeceği için makine öğreniminin otomatik potansiyelinin fazla tahmin edilmemesi gerektiği görülmektedir.

Bilgisayar ve buna bağlı gelişen internet ortamı insanoğlunun sosyal yapısını büyük ölçüde değiştirmiş ve değiştirmeye de devam etmektedir. Bilgisayar, sosyal yapıyı değiştirmenin ötesinde yeni kavramları da birlikte getirmektedir. Bunun sonucunda da adli bilimlerin birden fazla niteliği ve işlevselliği içinde yer almaktadır. Adli bilimler, suç ve suçlular bütün olarak düşünüldüğünde, bilgisayar ya da daha genel bir ifade ile bilişimi; bilişim ortamına karşı işlenen suçlar, bilişim ortamı kullanılarak işlenen suçlar, bilişim teknikleri ile suç ve suçluların ortaya çıkarılması olarak tanımlanabilir. Kısaca tüm bu tanımlar sonucunda Adli Bilişim olarak ayrı bir bilim dalının da ortaya çıktığı görülmektedir.

Sonuç olarak, Adli Bilişim olarak yeni bir boyut kazanan bilişim alanı ile disiplinler arası özelliği bulunan Adli Bilişim Teknikleri ortaya çıkmıştır. Her geçen gün bu tekniklere yenileri eklenmekte ve geliştirilmektedir. Bu teknik alanda uzmanlaşmış olan Adli Bilişim mühendisleri dijital ortamda işlenen suçlara ilişkin olarak suç işlenmeden önce gerekli önlem ve tedbirlerin alınması için ortam oluşturan, suç işlendiği anda eşzamanlı olarak savunma yapabilen ve suç işlendikten sonra hukuki süreçte yardımcı olarak görev yapan bir mühendislik dalıdır. Dünyada 1990'lı yıllardan itibaren popüler hale gelmeye başlayan Adli Bilişim mühendisliği silinen verilerin geri getirilmesi üzerine temel tekniklerin ortaya çıkması ile bir bilim dalı olarak gelişmiştir. Türkiye'de ve dünyada Adli Bilişim teknikleri alanında Adli Bilişim mühendisliği eğitimleri lisans ve lisansüstü düzeyde verilmektedir.

Adli Bilişimde Dijital Dezenformasyon ve Deepfake Uygulamaları

İçinde bulunduğumuz çağ, yeni iletişim teknolojilerinin fiziksel katılım sağlanılan nesnel yaşama entegre olması ile birlikte

hibrit yaşam pratiklerinin kendini gösterdiği çağdır. Özellikle hem sanal hem de nesnel gerçekliğin kurucu unsuru olan sosyal medyanın, nesnel gerçekliğe bir alternatif olduğu bu çağ, aynı zamanda yapay zekâ algoritmalarının nesnel gerçeğin sanal gerçeklikte yeniden inşa edildiği gelişmeyi de kapsamaktadır. Yapay zekânın yeni iletişim teknolojilerinde etkinliği özellikle içerik üretme ve dağıtma süreçlerinde kendini göstermektedir.

Deepfake teknolojisi, yapay zekâ teknolojisinin derin öğrenme algoritmalarını kullanarak canlı objelerin yeteneklerini öğrenme ve taklit etme hatta manipüle etme kapasitesi ve yetilerine sahip bir çıktıdır. İlk olarak 2018 yılında kötü niyetli çevrimiçi aktörler tarafından kullanılmaya başlayan bu teknoloji, özellikle sinema sanatına görsel ve anlamsal olarak farklılıklar katarken, dijital uzamlarda daha çok derin sahtekârlıklar için kullanılmaktadır. Dijital uzamlar dijital kimliklere fiziksel yaşam alanlarında pek fazla bulamadığı saklanabilme ve sınırsız hareket etme özgürlüğü sunmaktadır. Dijitalleşmenin kullanıcılarına sunduğu bu imkan ve fırsatlar aynı zamanda deepfake gibi teknolojilerin çevrimiçi alanlarda daha fazla kullanılmasına neden olurken, bu teknolojiler ile oluşturulan içeriklerin dijital uzamlarda dolaşıma sokulması, gerçeğin sorgulanması gibi algısal tutarsızlıklara işaret eden derin sorunları da ortaya çıkarmaktadır.

Bilgi yönetimi, büyük veri başta olmak üzere veriyi etkin bir şekilde yönetme, veri kaynaklarını koruma, kontrol etme ve en iyi şekilde kullanma gibi bir dizi sorunu da beraberinde getirmektedir.

Ülkeler ve devletler ve de o ülkeleri ve devletleri yönetenlerin bu bilgileri, siyasetten ekonomiye, savunmadan savaşa, bilimden teknolojiye, uluslararası ilişkiden diplomasiye varıncaya kadar her alanda etkin ve yetkin kullanmaktadırlar. Diğer yandan bu kadar büyük ölçekte verinin ve bilginin dolaştığı siber ortamda bilginin doğruluğu, güncelliği ve güvenilirliği kritik bir öneme sahiptir.

Dijital çağda kullanılan başta DeepFake, DeepWeb, DarkWeb gibi kavramlar bilginin boyut, içerik ve yayılma ortamlarını ve yöntemlerini büyük ölçüde değişmiştir. Dijital enformasyon ve dijital dezenformasyon yöntemleri, günümüzde çok farklı kullanım biçimleri, amaçları, etkileri ve sonuçları ortaya çıkartmıştır. Bunların başında Enformasyon Savaşları ve Dijital Dezenformasyon gelmektedir.

"*Dezenformasyon*" terimi, "*özellikle bir devlet kurumu tarafından rakip bir güce veya medyaya verilen propaganda olmak üzere yanlış yönlendirmeyi amaçlayan yanlış bilgiler*" anlamında kullanılmaktadır.

Dünya çapındaki demokrasiler, geçtiğimiz on yılda yeni bir tür bilgi operasyonlarının hedefi haline gelmişlerdir. Hükümetlerin sıklıkla hazırlanmakta, tanımakta veya etkin bir şekilde yanıt vermekte başarısız olduğu bu savaş, yeni tanımlar, tanımlamalar ve etiketler gerektiren bir savaş niteliğindedir.

Sosyal medya ortamlarının açıkça kötüye kullanılmasına yönelik önlemler alınırken, bu ortamları kötü amaçlı kullanmak isteyen aktörler tarafından da yeni yöntem ve teknikler geliştirilmektedir. Bu ortamlarda, dezenformasyonun yayılması, sosyal mühendislik saldırıları için yaygın olarak kullanılmaktadır. Özellikle, yapay zekâ alanında devam eden "*deepfake*" türü teknolojik gelişmeler, yeni video ve ses teknikleri, kimliğe bürünme saldırılarını gelecekte daha da gerçekçi ve inanılır hale getirecektir.

Dezenformasyonu yaymak için kullanılan yöntemler ve platformlar her geçen gün değişmekte ve gelişmektedir. WhatsApp veya kapalı Facebook grupları gibi şifreli platformların artan kullanımı, mahremiyet ve güvenliği artırırken, kötü niyetli aktörlerin kolaylıkla gizlenmesine ve izlerinin takip edilmesinin zorlaşmasına yardımcı olmaktadır.

İletişim ve internet çağı olarak nitelendirilen günümüz dünyasının en önemli araçlarından birisi de sosyal medya dünyasıdır. Başta Twitter, Instagram, Linkedin, Facebook, vb. sosyal medya araçları olmak üzere sosyal medyanın tüm araçları her alanda olduğu gibi, dijital diplomasi aracı olarak da tüm dünya ülkelerinin liderleri tarafından yeni bir araç ve yöntem olarak yoğun bir şekilde kullanılmaktadır. ABD, Çin, Rusya gibi ülkeler ve bunların liderleri başta olmak üzere tüm dünya ülkelerinin iletişimlerini, mesajlarını geleneksel yöntemlerin yanı sıra sosyal medya üzerinden gerçekleştirdiği göz önünde bulundurulduğunda, bilgi savaşlarının temel unsurları olan dijital enformasyon ve dijital dezenformasyon kavramları yeniden ele alınması gereken bir konu olduğu kolaylıkla görülmektedir.

Bütün bunların sonucu ortaya çıkacak ulusal ve uluslararası hukukta yeni birtakım kavramları ve uygulamaları yakın gelecekte tartışıyor olacağız. Bunlar Adli Bilişim alanında yeni bir başlık olarak karşımıza çıkacaktır. Bunun sonucunda bütün dünyada bu alanda yeri düzenleme yaklaşımları da son derece önemli ve kritik bir hale gelecektir.

Adli Bilişimde Bulut Sistemlerinin Kullanılması

Teknolojinin gelişmesi ile ekonomik, sosyal ve çevresel yenilikler meydana gelmektedir. Bu yeniliklerle birlikte bireylerin ve işletmelerin bu yeniliklere ayak uydurması bir zorunluluk haline gelmektedir Bu yeniliklerden biri de Bulut Bilişimdir. Bulut Bilişim, bulut servislerini kullanarak resim, belge, müzik gibi her tür dosyanın buluta yüklenerek ihtiyaç duyulan durumlarda internet aracılığıyla her zaman erişilebilmesini sağlamaktadır. Bu teknoloji bireylerin gereksinimine göre kapasite artırma veya azaltma, zaman ve mekân fark etmeksizin ulaşım kolaylığı

sağlamaktadır. Ayrıca güvenlik, yazılım güncellemeleri, enerji tasarrufu ve maliyet bakımından avantaj sağlamaktadır .

Bilirkişilik faaliyeti gösteren kurumlar, delilleri kilitli bir delil dolabında tutma ve görüş alanında olması konusunda oldukça ihtiyatlı davranırlar. İlgili kurumlar ucuz, taşınabilir ve kolayca bulunabildikleri için depolama yöntemi olarak USB sürücüleri tercih edilebilmektedirler. Ancak kanıtlara veya bunların dijital kopyalarına yetkisiz kişiler tarafından erişilmesi, kopyalanması ya da çalınması oldukça endişe vericidir. Benzer şekilde dijital kopyaların veri merkezlerinde saklanması çeşitli fiziksel ve dijital tahribatlara neden olabildiği gibi ilgili kurumların zaman ve maliyet yükünü de arttırmaktadır.

Bu nedenden dolayı ilgili kurumların geleneksel depolama ve transfer yöntemleri yerine daha gelişmiş bir yöntem olarak Bulut Sistemlerine (SaaS) geçiş yapabilirler. Bulut hizmetleri: Verilere bir web tarayıcısı üzerinden kolayca erişebilmesine, kontrolsüz kopyaların ve manipülasyonların önüne geçmesine, yargı makamlarının istenilen zaman da dijital kopyaya erişebilmesine ya da yeni bir incele talebinin hızlandırılmasına olanak tanır. Bulut depolama, fiziksel bir sürücüden daha güvenli olmasının yanında kimlerin kopyalara eriştiğini veya görüntülediğini de kayıt altında tutar. En önemlisi bulut depolama mağdurların korunmasına yardımcı olur. Mağdurlar zaten zarar görmüşse, güvenli bir kanıt depolama yönetimi ile bunun önüne geçilebilir.

Bulut sistemlerinin kullanılmasında dezavantaj olarak değerlendirilebilecek birkaç husus ise internet kesintisi halinde delil kopyalama da indirme sonuçlarına erişim sağlanamaması, bulut hizmeti veren şirketlere yapılan kapsamlı siber saldırıların olması, sunucuların fiziksel bir tahribata maruz kalması şeklinde sayılabilir.

II

Hukuk Perspektifinden Adli Bilişim Uygulamaları

"Hukuk Perspektifinden Adli Bilişim Uygulamaları" ana başlığı ile düzenlenen üçüncü oturumda akademisyen ve uygulayıcılardan oluşan katılımcılar sırasıyla "Adli Bilişimde Elde Edilen Delilin Hukuki Değeri", "Lafzi ve Uygulama Olarak CMK 134'ün Adli Bilişimdeki Rolü", "Adli Bilişim Uygulamalarında Yaşanan Hukuki Sorunlar" ve "Adalet Bakanlığının Adli Bilişim Suçları Kapsamında Yaptığı Çalışmalar" başlıklarına ait sunumlarını gerçekleştirmiştir. İkinci oturum dahilinde yapılmış olan uygulamaya yönelik sunumlarda hukuki alt yapıya ilişkin tartışmalar yürütüldüğünden, hukuki tartışmaları içeren üçüncü oturumun rapor yazımında öne alınması uygun görülmüştür. Yapılan sunumlar ve tartışmalar neticesinde katılımcıların bilgi ve görüşlerinden derlenen bölüm özeti şu şekildedir;

Hukuki Perspektiften Adli Bilişim

Cep telefonu, bilgisayar gibi ileri teknoloji cihazlar günümüz dünyasının vazgeçilmez temel unsurları haline gelmiştir. Karmaşıklığı ve kabiliyeti sürekli olarak artan donanım yazılım tabanlı bilişim sistemleri başta hukuk alanı olmak üzere hemen her bilim alanı ile sıkı bir ilişki içerisindedir. Toplumsal düzenin korunması esasıyla ceza yargılamasında bilgisayar ile işlenen suçlar, başkaca suçlara ilişkin delil elde edebilme ve suçla etkin mücadele edebilme alanlarında Adli Bilişim süreçleri önemli yer

tutmaktadır. Maddi gerçekliğe ulaşmayı temel amaç sayan ceza muhakemesi hukuku ceza hukukunda teknoloji ile gelişen yeni suç tiplerini, bilişim sistemleri üzerinden alınabilecek koruma tedbirlerini geliştirmiş, elektronik ortamlarda bulunan ve adli süreçlerde veri olarak kullanılabilecek bilgileri bir ispat vasıtası haline getirmiştir.

Hukuki süreçte delil değeri taşıyan dijital delillerin ortaya çıkarılması ve mahkemeye sunulması teknik bilgi ve uzmanlık gerektirmektedir. Adli Bilişim alanı bilişim alanında uzman personel yetiştiren, delil niteliğindeki verileri inceleyip raporlayarak adli mercilere ulaştıran disiplindir. Dolayısıyla Adli Bilişimi adalet sistemi ve hukukumuzun vazgeçilmez bir unsuru haline gelmiştir.

Ceza Muhakemesinde Adli Bilişim

Bir suçun işlendiği izlenimi veren hâlin öğrenilmesi ile başlayan ve hükmün kesinleşmesine kadar devam eden ceza muhakemesi süreci basit suç şüphesinin öğrenilmesi ile başlamaktadır. Yeterli şüpheye ulaşılması durumunda Cumhuriyet savcısı tarafından hazırlanan iddianamenin kabulüne kadar devam eden süreç soruşturma evresidir. İddianamenin kabulü ile başlayarak, hükmün kesinleşmesine kadar devam eden evre ise kovuşturma evresidir.

Ceza muhakemesinin amacı maddi gerçeğin ortaya çıkarılmasıdır. Maddi gerçeğin ortaya çıkarılmasında mahkeme ile birlikte Cumhuriyet Savcısı ile adli kolluk birimlerinin ve diğer birçok aktöre önemli görevler düşmektedir. Bu adalet sürecinin ilk ve en önemli aşamalarından birisi de delillerin elde edilmesi ve sunulmasıdır.

Ceza muhakemesinde delil suç teşkil eden uyuşmazlık konusunda olayın gerçekleşip gerçekleşmediği hakkında mahkemede bir kanı oluşturmaya yarayan kanıt aracıdır. Muhakeme sürecini

ve adaletin gerçekleşmesini temelden ilgilendiren delilin güvenilir olması ve bilimselliği ceza muhakemesi bakımından delil değeri taşınmasında vazgeçilmez unsurlardır. Adli Bilişim yoluyla elde edilen delilin bilimselliğinin temini delilin elde edilmesi, değerlendirilmesi, rapor edilmesinin uzman kimselerce ve bilimsel metotlarla yapılması ile mümkündür.

Delil, Elektronik Delil ve Hukuka Aykırı Delil

Ceza muhakemesinde delil serbestisi ilkesi esastır. Hâkimin deliller üzerinde takdir yetkisi bulunmaktadır. Ancak bir şeyin delil sayılabilmesi için bazı temel özelliklere sahip olması beklenir. Bu temel özelliklerden ilki delilerin gerçekçi ve akılcı olmasıdır. Gerçekçi ve akılcı olması maddi gerçeği objektif niteliklere dayanan verilerle ispat ediyor olduğu anlamını taşır. Muhakemede dikkate alınan deliller çatışmalı olan olayın tamamı yahut bir kısmını aydınlatıcı nitelikte olmalıdır. Ayrıca delilin elde edilebilir olması, yani aynı yöntemler uygulandığında yeniden ulaşılabilir olması gerekmektedir. Delillerin hem kendisi hem de elde edilme biçimi kanuna uygun olmalıdır. Bir başka deyişle, mahkemeye sunulan deliller kanuna uygun yollardan elde edilse dahi içerikleri kanuna uygun değilse delil olarak kullanılamazlar. Delil içerikleri mahkeme makamının yanı sıra mahkemenin tarafları tarafından da bilinmelidir. Bu delillerin müşterekliği ilkesi gereğincedir.

Elektronik delil bir elektronik aygıt üzerinde saklı olan ve içeriği çatışmaya konu hukuki soruşturma açısından değerli olan bilgi ve veridir. Ceza muhakemesi bakımından kabul edilen klasik deliller beş duyu organı ile algılanabilir nitelikte olduğundan el koyma ve muhafaza altına alma kararları kolayca uygulanabilir. Ancak elektronik deliller soyut dijital deliller olduğunda

muhakemeye konu olması özel bir ihtimam ve düzenlemeler gerektirmektedir. Elektronik delillerin hukuka uygun biçimde elde edilmesi muhakemenin sıhhati bakımından elzemdir. Zira hukuka aykırı delil muhakemeye esas alınamayacaktır.

Hukuka aykırılık herhangi bir fiilin, iş ya da işlemin hukuk düzeninin bütünü ile çelişki ve çatışma halinde olması durumudur. Anayasa Mahkemesi de hukuka aykırılığı "*anayasa, usulüne uygun olarak kabul edilmiş uluslararası sözleşmelere, kanunlara, kanun hükmünde kararnamelere, tüzüklere, yönetmeliklere, içtihadı birleştirme kararlarına ve teamül hukukuna aykırı uygulamaların tümü…"* şeklinde tanımlamıştır.

Ceza Muhakemesi Kanunu da "217/1'de "yüklenen suç, hukuka uygun bir şekilde elde edilmiş her türlü delille ispat edilebilir" maddesi ile hukuka aykırı delillerin muhakemede delil teşkil edemeyeceğini hüküm altına almıştır. Yine 206/2'de mahkemenin "kanuna aykırı elde edilen delilin" reddedeceğini bildirmektedir.

Özellikle kolluğun olay yerine ilk ulaşan olması, ifade alma, olay yeri inceleme, arama, el koyma işlemlerinin delil zincirinin ilk halkasını oluşturması hukuka uygun delil elde edilmesi hususunu kolluk eğitimi bakımından özel önemi haiz bir noktaya taşımaktadır. Örneğin kolluğun arama işlemini hukuka uygun olarak yapmadığından hareketle, Yargıtay CGK, 28.04.2015, 2013/464, 2015/132 sayılı kararında arama tanıklarının bulunmadığı durumlarda yapılan aramayı hukuka aykırı kabul etmiştir. Buna göre; *"… kolluk tarafından aramanın 5271 sayılı CMK'nın aramanın güvenirliliği ile ilgili 119/4. maddesinin "Cumhuriyet savcısı hazır olmaksızın konut, işyeri veya diğer kapalı yerlerde arama yapabilmek için o yer ihtiyar heyetinden veya komşulardan iki kişi bulundurulur" amir hükmüne aykırı olarak o yer*

ihtiyar heyetinden veya komşulardan iki kişi hazır bulundurulmaksızın yapılması nedeniyle icrası bakımından hukuka aykırı olduğu ve arama sonucu elde edilen suça konu mermilerin hukuka aykırı yöntemle elde edilmiş delil niteliğinde bulunduğunun kabulünde zorunluluk bulunmaktadır. Bu itibarla, hukuka aykırı olarak gerçekleştirilen arama işleminde elde edilen delilin ve buna ilişkin düzenlenen tutanağın, yerel mahkemece hükme esas alınmasında ve Özel Dairece de bu hükmün onanmasında isabet bulunmamaktadır…"

Delillerin toplanması, arama ve el koyma kararının alınması ve uygulanması gerek Adli Bilişim uygulama teknikleri, gerekse muhakemeye yardımcı kolluk işlemleri bakımından özel olarak ele alınmalıdır.

CMK 134'ün Adli Bilişimdeki Rolü

Ceza Muhakemesi Kanunu'nda Arama ve El Koyma hükmü gereğince arama kararı verilebilmesinin şartları CMK m. 119'da düzenlenmiştir:

"(1) Hâkim kararı üzerine veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının yazılı emri ile kolluk görevlileri arama yapabilirler.

(2) Arama karar veya emrinde;

a) Aramanın nedenini oluşturan fiil,

b) Aranılacak kişi, aramanın yapılacağı konut veya diğer yerin adresi ya da eşya, c) Karar veya emrin geçerli olacağı zaman süresi,

Açıkça gösterilir.

(3) Arama tutanağına işlemi yapanların açık kimlikleri yazılır. Arama sonu- cunda bazı eşyaya elkoyma söz ko-

nusu olduğunda 127nci maddenin birinci fıkrası hükmü uygulanır. (4) Cumhuriyet savcısı hazır olmaksızın konut, işyeri veya diğer kapalı yerlerde arama yapabilmek için o yer ihtiyar heyetinden veya komşulardan iki kişi bulundurulur. (5) Askerî mahallerde yapılacak arama, hâkim veya Cumhuriyet savcısının istem ve katılımıyla askerî makamlar tarafından yerine getirilir."

Madde hükmü gereğince özellik arz etmeyen eşya ve delil kaynakları bakımından yapılacak aramalar 119. maddeye uygun biçimde yapılmaktadır. Yine Ceza Muhakemesi Kanunu 116. Maddesinde şahısların üzerinde, evinde ve iş yerinde yapılabilecek adli arama bakımından makul şüphe aranırken 134.madde hükmü kuvvetli şüpheyi gerekli kılan özel bir düzenleme yapmıştır. Gerekli görülen kuvvetli şüphe yalnızca bir suçun işlendiğine dair somut şüpheyi değil aynı zamanda üzerinde arama ve inceleme yapılacak cihazlarda suç delili bulunacağı yönündeki yoğun şüpheyi de ifade etmektedir.

Klasik suçlara ilişkin genel arama rejimi dışında bilişim materyallerinde arama ve el koymaya ilişkin olarak Ceza Muhakemesi Kanunu 134. maddesi bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma işlemini özel olarak ve ayrıca hüküm altına almıştır. Buna göre CMK m. 134 uyarınca;

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

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

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

(4) Üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

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

Kolluğun bilişim sistemleri üzerindeki bulunan delilleri elde etmek üzere uyguladığı bu tedbirin şartlarından birisi daha önce belirttiğimiz üzere kuvvetli şüphenin bulunmasıdır. Bunun yanı sıra bir diğer önemli şart başka surette delil elde etme imkanının bulunmaması gerekliliğidir. Bu itibarla kolluğun olay yerinde öncelikli olarak bilgisayarda inceleme yani arama yapması, bu şekilde delil elde etmesi mümkün olmazsa ancak o durumda el koymaya başvurması öngörülmüştür. Nihayet bu tedbirin uygulanması için Cumhuriyet Savcısı'nın istemi ile sulh ceza hakiminin kararı gerekmektedir. Ceza Muhakemesi Kanunu'nda öngörülen usul ve esaslara eksiksiz biçimde uyulması delillerin hukuki olması ve ceza yargılaması neticesinde verilecek hükme esas teşkil edebilmesi bakımından son derece önemlidir.

Ancak Ceza Muhakemesi Kanununda ayrıntılı olarak düzenlenmiş olsa da arama ve el koyma, diğer Adli Bilişim uygulamaları hususunda önemli hukuki ve pratik sorunlarla karşılaşılmaktadır. Bu sorunların tespiti çözüme ulaşılması bakımından önemli bir ilk adım niteliğindedir.

CMK 134 Özelinde Ortaya Çıkan Hukuka Aykırılıklar ve Sonuçları

Ceza Muhakemesi Kanunu'nun 134'ncü maddesi bireylerin temel hak ve özgürlükleri ile ilgili olan ve çoğunlukla durağan verilerde uygulanan sayısal delillerle ilgili tek maddesidir. Söz konusu madde özel bir arama ve el koyma hükmüdür. Bundan dolayı madde özelinde değerlendirmeler yapılarak olası ve mevcut hukuka aykırılıkların ortaya konması gerekmektedir.

Öncelikle CMK m. 134, bilişim sistemlerinde arama, kopyalama ve el koyma tedbiri bakımından arama kararının varlığını düzenlemektedir. Özel bir arama kararı olmasından dolayı, CMK m. 116 çerçevesinde verilen arama kararının, bilişim sistemlerinde aramayı da kapsamayacağını değerlendirmektedir. Bu durumda arama kararı olmayan yapılan arama sonucunda elde edilen delillerin muhakemede kullanılamayacağı kanaati ifade edilmelidir.

YCGK, 26.06.2007 tarih ve 7-147/159 sayılı kararında bu hususa temas etmiş ve arama kararı olmadan elde edilen delillerin muhakemede kullanılamayacağını düzenlemiştir.

"Sanık tarafından işletilen iki ayrı işyerinde arama yapılmasına karar verilmesine karşın, aynı işyerinde bulunan ***bilgisayarlar üzerinde arama yapılabilmesine olanak tanıyan hükümlere göre verilmiş bir arama kararı bulunmadığı anlaşılmakla****, işyerinde bulunan bilgisayarlar üzerinde yapılan arama sonucunda e lkonulan ve içerisinde müşteki firmaya ait lisanssız ya-*

zılımların olduğu belirtilen harddiskler ve CD'ler hukuka aykırı delil niteliğinde olup hükme esas alınamayacağından" (Yargıtay 19. CD, 6.5.2015, 2015/2092-1175).

Söz konusu arama kararının koşulları maddede düzenlenmiştir. Buna göre *"somut delillere dayanan kuvvetli suç şüphesi"* nin varlığı gereklidir. Kuvvetli suç şüphesinin bulunmadığı veya somut delillere dayandırılamadığı durumlarda, bilişim sistemlerinde arama kararı verilemeyecektir. Burada yer alan kuvvetli şüphenin iki hususa yönelmesi gereklidir. Öncelikle suçun işlendiği hususunda kuvvetli şüphe ikinci olarak ise suç delillerinin bilişim sistemlerinde bulunacağı noktasındaki kuvvetli şüphedir.

Yargıtay'ın yukarıda incelenmiş olan kararında görüleceği üzere "makul şüphe" yi gerektiren olgular ve buna bağlı olarak da arama kararı veya emri verilebilmesinin koşulları bulunmadığı halde, sanık hakkında yalnızca "çeşitli suçlardan kaydı bulunduğu" gerekçesiyle, hukuka aykırı bir şekilde yapılan arama sonucu elde edilen deliller hukuka aykırı kabul edilmektedir. Bu kapsamda, kuvvetli suç şüphesi bulunmadan verilen arama kararı da hukuka aykırı olarak kabul edilebilecektir.

CMK m. 134, arama, kopyalama veya el koyma tedbirine soruşturma evresinde başvurulabileceğini belirtmiştir. Buna rağmen kovuşturma evresinde de söz konusu kararlar verilmekte ve hukuka uygun kabul edilmektedir.

Tedbire kural olarak hakim tarafından karar verilebilecektir. Bununla birlikte 7145 sayılı Kanunla yapılan değişiklikle, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da karar verilebilecektir. Gecikmesinde sakınca bulunan bir durum olmadan verilen karar sonucu elde edilen deliller hukuka aykırı olacağı gibi böyle bir karar Cumhuriyet savcısının da sorumluluğunu gerektirecektir.

Gecikmesinde sakınca bulunan durumlarda Cumhuriyet savcısı tarafından verilen kararın 24 saat içinde hakim onayına sunulmaması veya hakim tarafından belirlenen süre içerisinde cevap verilmemesi veya aksine karar verilmesi durumunda elde edilen deliller hukuka aykırı olacaktır.

CMK'nın 134'ncü maddesinin 2'nci fıkrasında el koyma şartları düzenlenmektedir. Söz konusu maddede, el koymanın gerçekleşebilmesi için sınırlı sayıda gösterilen 3 şarttan biri gösterilmelidir. Söz konusu 3 şarttan birinin gerçekleşmemesi durumunda el koyma sonucu elde edilen deliller hukuka aykırı olacaktır.

"Kural olarak bulundukları mahalde incelenmeleri gereken suça konu sabit disklere gerek CMK'nın arama tarihi itibarıyla yürürlükte bulunan ***134/2. maddesinde "Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması..." şeklinde belirtilen hükme; gerekse objektif olarak kabulü gereken zorunlu nedene dayalı bir gerekçe gösterilmeden el konulması,*** *yine somut olayın özelliklerine göre engel bir durum bulunmadığı hâlde el koyma işlemi sırasında sistemdeki bütün verilerin yedeklenmesi gerektiği ve istenmesi hâlinde bu yedekten bir kopya çıkartılarak arama sırasında hazır bulunan sanığa verilmesi gerektiğinin gözetilmemesi suretiyle CMK'nın* 134'ncü maddesinin üç ve dördüncü fıkralarına aykırı hareket edilmesi sebebiyle usulüne uygun olmayan el *koyma işlemi sonucu suça konu sabit disklerden elde edilen verilerin hukuka aykırı olarak elde edilen delil niteliğinde olduğu…"* (YCGK, 25.2.2020, 2016/8-544, 2020/127).

CMK m. 134/2 gereğince bilişim sistemlerine delil elde etmek amacıyla el konulması durumunda, şifrenin çözümünün yapılması veya gerekli adli kopyaların alınması durumunda el

konulan cihazların iadesi gereklidir. Gerek Anayasa Mahkemesinin Ercan Demirbaş kararı gerekse de AİHM Smirnov v. Rusya kararı gereğince, makul sürede iade edilmeme mülkiyet hakkının ihlali olacaktır. Ancak bu durumlarda, elde edilen deliller hukuka aykırı hale gelmeyecektir.

Diğer Bilişim Suçları

Siber Suç, diğer bir deyişle bilişim suçu; bilgisayar, tablet, cep telefonu gibi çağdaş iletişim araçları veya pos makinası gibi alışveriş araçları kullanılarak elektronik ortamda işlenen her türlü suç olarak tanımlanabilir. Bilgisayar ve internete özgü suçlar olarak da adlandırılan Siber Suçlar, bir bilişim sisteminin güvenliğini ve/veya buna bağlı verileri ve/veya kullanıcısını hedef alan ve bilişim sistemi kullanılarak işlenen suçlardır. Siber Suçu diğer suçlardan ayıran özelliği bir bilişim sistemi olmadan işlenememesidir. Bu suç türü bir bilişim sistemine izinsiz ve hukuka aykırı olacak şekilde girilmesi ve sonrasında yapılan eylemdir. Bu suçta hedef bir kişi olabileceği gibi kişinin malvarlığı veya bir sistemin kendisi de olabilir. Örneğin, bir sisteme girerek, zarar verme, verileri silme, şifreleme, ele geçirme, veri ekleme, sistemin kullanımını engelleme, özel hayatın gizliliğine müdahale etme, iletişimi engelleme, iletişimi izinsiz izleme ve kayıt etme gibi eylemler siber suç kategorisinde değerlendirilir.

EGM Siber Suçlarla Mücadele Daire Başkanlığı koordinesinde yürütülen Siber Suç Soruşturmaları kapsamında; çevrimiçi çocuk istismarı, bilişim sistemleri, ödeme sistemleri, yasa dışı bahis, suç gelirleri, konularında Türk Ceza Kanunu'nda tanımlanmış 17 farklı suç türü hakkında yapılan çalışmalar ile suç ve suçluların tespitine yönelik etkin bir şekilde suçla mücadele edilmekte ve önleyici faaliyetler yapılmaktadır. Bilişim sistemlerine yönelik beş temel başlıkla ele alınabilecek suçlar, ödeme sistem-

lerine yönelik işlenen suçlar, çevrimiçi çocuk istismarı suçları, suç gelirleri suçları ve çevrimiçi yasa dışı bahis suçlarıdır. Genel olarak bilişim suçlarını ifade etmek gerekirse;

- Bilgisayar Sistemlerine ve Servislerine yetkisiz erişim
- Bilgisayar sabotajı
- Bilgisayar yoluyla dolandırıcılık
- Bilgisayar yoluyla sahtecilik
- Yazılımın izinsiz kullanılması
- Kişisel verilen kötüye kullanılması
- Sahte kişilik oluşturma ve taklidi
- Yasadışı yayınlar
- Ticari sırların çalınması
- Terörizm içerikli faaliyetler
- Hacking

Bilişim suçlarının temel ortak özellikleri işlenmesinde bilgisayar sistemleri ve teknolojilerinin kullanılmasıdır. Bilişim suçunun sonucunda çok yüksek kazancın kolay ve daha az riskle temin edilmesi bu suça eğilimi arttıran bir unsur olarak sayılabilir. Suçların yeni tipler olması nedeniyle gerekli kanun ve düzenlemelerin eksik ve yetersiz olabilmektedir. Zira büyük bir hızla gelişen teknolojiler neticesinde hızlı suçlu ve suç yöntemi de hızlı bir şekilde değişip ve gelişebilmektedir. Bilişim suçlarının işlenmesinin neticesinde diğer suç türlerine göre daha ağır maddi ve manevi suçlar doğmaktadır. Bu suçun mağdurları genellikle bilinçsiz kullanıcılar, failleri ise adi ve münferit olabileceği gibi organize de olabilmektedir. Suçun genellikle uluslararası boyutu bulunmaktadır. Gerek bilişim suçu gerekse bilişim yoluyla yahut bilişime karşı işlenen suçların tamamında Adli Bilişim süreçleri işletilmektedir. Bu bağlamda kolluğun Adli Bilişim teknikleri, hukuki süreçleri ve mevcut ve olası problemleri ile ilgili uygulamaları özel önemi haizdir.

III

Adli Bilişim ve Kolluk Faaliyetleri

“Adli Bilişim ve Kolluk Faaliyetleri” ana başlığı ile düzenlenen ikinci oturumda akademisyen ve uygulayıcılardan oluşan katılımcılar sırasıyla “Dijital Delillerin Elde Edilmesi ve Güvenliği”, “Mobil Cihaz Adli Bilişiminde Dikkat Edilmesi Gerekenler”, “Hard Diskler ve Nand Belleklerde Veri Kurtarma” ve “Siber Suç Soruşturmaları ve SİBERAY” başlıklarına ait sunumlarını gerçekleştirmiştir. Yapılan sunumlar ve tartışmalar neticesinde katılımcıların bilgi ve görüşlerinden derlenen bölüm özeti şu şekildedir;

Adli Bilişim Uygulamaları ve Kolluk Faaliyetleri

Ceza soruşturmasının en temel maksadı maddi gerçeğin ortaya çıkarılmasıdır. Adaletin doğru ve zamanında tecellisi için zincirin ilk halkası olan adli kolluk ve Cumhuriyet Savcılığının iş ve işlemleri son derece önemlidir. Adli Bilişim bilimi adli kolluk ve savcıları doğrudan ilgilendirmektedir. Adli kolluğun bilişim sistemleri yoluyla işlenen suçlar, bilişim sistemlerine karşı işlenen suçlar ve bilişim sistemlerinin yardımı ile işlenen suçların aydınlatılmasında ve suçlunun tanımlanmasında alacağı etkin rol başarılı bir adalet sisteminin hızlı, verimli ve etkin bir biçimde yürütülebilmesine yardımcı olacaktır.

Dijital Deliller, Elde Edilmesi ve Güvenliği

Dijital/elektronik delil (e-delil), "bir elektronik araç üzerinde saklanan veya bu araçlar aracılığıyla iletilen soruşturma açısından değeri olan bilgi ve veriler"dir. Dijital deliller elektronik ortamda bulunan veriler olduğundan bunların temel özellikleri; rahatlıkla kopyalama işlemi yapılabilmesi ve çoğaltılabilmeleri, manyetik alan, sıcaklık, nem gibi etkenlerden dolayı bozulabilmeleri, veriler üzerinde işlem yapmak kaydıyla rahatlıkla değiştirilebilir olmalıdır. Yine elektronik veriler şifreleme algoritmalarıyla şifrelenmiş, gizlenmiş verileri üzerlerinde barındırabilirler ve tekrar elde edilmesi mümkün olmayacak şekilde silinebilirler.

Dijital delil oluşturabilecek bulgular genel olarak üç grupta toplanabilir. Bunlardan ilki somut elle tutulabilen ve gözle görülebilen fiziksel delillerdir. İkincisi bir olaya tanık olmuş kişiler tarafından ileri sürülen tanığa dayalı delillerdir. Son olarak somut yahut tanığa bağlı olmaksızın şüpheyi destekleyen, sanal dünyanın ikincil derecede delil kabul edeceği emarelerdir. Delil oluşturabilecek bulgulardan bazıları şu şekilde sayılabilir;

- Video görüntüleri
- Fotoğraflar
- Yazı dosyaları (word, excel, open office vb. dosyaları)
- Çeşitli bilgisayar programları
- İletişim kayıtları (SMS, Whatsapp, vb. kayıtları)
- Gizli ve şifreli dosyalar / klasörler
- Dosyaların oluşturulma, değiştirilme ve erişim tarih kayıtları
- Son girilen ve sık kullanılan internet siteleri
- İnternet ortamından indirilen dosyalar
- Ve bu türden olup, silinmiş dosya/klasörler

Elde edilen bu verilerin dijital delil olarak nitelendirilebilmesi ve mahkemeye sunulabilmesi için hukuka uygun, doğru ve güvenilir yollarla elde edilmiş olması, şüpheli durumu açıklığa kavuşturacak özelliklerde bir neden sonuç ilişkisini ihtiva ediyor olması, sanık veya şüpheli şüpheli kimseyi ilgilendiren olumlu yahut olumsuz tüm hususları eksiksiz olarak içermesi, delil bütünlüğünün bozulmamış olması, mahkeme tarafından anlaşılabilir ve inanılabilir nitelikte, aynı metotlar kullanıldığında yeniden ulaşılabilir özellikte olması gerekmektedir.

Adli kolluğun yukarıda bahsettiğimiz özellikteki dijital delilleri elde etmek üzere yapacağı işlemlerde teknik donanımlara sahip olması elzemdir. Bu tip işlemlerde operasyon çantası olarak ifade edilen donanım da bulunması gerekenler şu şekilde sayılabilir:

- TD cihazları ve şarj adaptörleri
- SATA, IDE veri aktarım kabloları
- Tableau Ultra Block cihazlardan SATA, IDE, SCSI VE USB BRIDGE ve dönüştürücü aparatları
- SD/Micro SD kart okuyucuları ve dönüştürücü aparatları
- Daha önce kullanılmamış boş imaj HDD ve CD/DVD Yeteri kadar (Operasyonda kullanılacak olan imaj diskleri soruşturmacı birimden talep edilir.)
- FTK Imager yüklü bir adet flash bellek
- Deft zero yüklü bir adet flash bellek
- Linux ve Helix programlarının yüklü olduğu bellek
- HDD Docking Station
- Delil çuvalı ve delil poşeti
- Tek tarafı yapışkanlı etiket, A4 kâğıdı, mavi tükenmez kalem ve mühür bandı
- Klavye, mouse

- Tornavida takımı
- Laboratuvar eldiveni

Kolluk görevlileri operasyon çantasında bulunan her araç gerecin sağlamlığını kontrol edecektir. Operasyona hazır olan görevliler soruşturmacı birimle irtibata geçerek mahkeme kararının olup olmadığını, varsa CMK 134. Maddesinin kararda olup olmadığını kontrol eder. Kararın içeriğinde yalnızca el koyma yetkisini verilmiş olduğunu yoksa imaj alma ve inceleme yetkisinin de olup olmadığını kontrol eder. Zira mahkeme kararı da verilen yetki dışında hiçbir işlem yapılması mümkün değildir. Savcı talimatı, yeteri kadar personel ve teçhizatın temini için mahkeme kararında kaç adres olduğu gibi hususlar teyit edilerek operasyon adresindeki güvenlik önemleri alınacaktır.

Dijital Delillerin Bulunduğu Alandaki Kolluk İşlemleri

Dijital delillerin elde edileceği alana ulaşan kolluk görevlilerinin delilleri elde etme koruma ve gerekli yerlere ulaştırma konusunda bilgili ve eğitimli olmaları son derece önemlidir. Operasyon bakımından olayın meydana geldiği alanlar kişisel bilgisayarlarda yapılan dar kapsamlı incelemeler, kurum ya da kuruluşlarda çoklu bilgisayarlarda yapılan kapsamlı incelemeler olabilir. Suç olgusunun tespitine dayalı olarak alan değişebilecektir.

İlk aşamada delillerin değiştirilmesi yahut bozulması gibi durumların önüne geçilmek üzere delillerin güvenliği sağlanmalıdır. Bu sebeple olay mahalli ve çevre güvenliğinin sağlanması gerekir. Ellerinde bulunan operasyon adresine ulaşan kolluk görevlileri adrese ulaştıklarında bulunan şahısların kimliklerini kontrol eder, üst aramalarını yapar ve işlemler bitene kadar bir personeli gören görevlendirerek güvenliği sağlar. Bu önlemler hem delillerin güvenliği hem de görevde olan kolluk personelinin güvenliği için son derece önemlidir.

Herhangi bir işleme başlamadan önce farklı ve geniş açılardan çok sayıda fotoğraf çekilmelidir. Operasyon sırasında yapılacak olan aramalarda ve olay yerinden elde edilecek delilleri temin-de laboratuvar eldiveni kullanılmalıdır. Zira olay yerinden elde edilecek olan delillere şüpheli tarafından itiraz edilmesi halinde biyolojik inceleme veya parmak izi incelemesi gibi çalışmalar yapılmaktadır. Arama yapıldığı sırada arama yapılan bölge video kaydına alınmalı, elde edilebilecek olan delillerin olay yerinden alındığı açıkça görünecek şekilde kayıtlar oluşturulmalıdır.

Sonraki aşamada imajların alınması ve depolanması son de-rece titizlikle işletilmelidir. Veri depolama (sabit disk, flash bel-lek, hafıza kartı vb.) veya geçici barındırma, (RAM bellek vb.) bu özelliğe sahip dijital materyallerin, başka bir veri depolama dijital materyaline kopyalarının alınması işlemine denir. Olay yerinde fiziksel imaj yahut mantıksal imaj alma yöntemi uygula-nabilir. Fiziksel imaj, imaj alma işleminde fiziksel sürücünün(P-hysicalDrive0, PhysicalDrive1 vb.) seçildiği, sıfırıncı sektörden sonuncu sektöre kadar tüm sektörlerin kopyasının çıkarıldığı imaj türüdür. Mantıksal imaj ise imaj alma işleminde mantıksal sürücünün (C:\, D:\, E:\ vb.) seçildiği, yalnızca seçilen mantıksal sürücüdeki verilerin kopyasının çıkarıldığı imaj türüdür.

İmaj alma işlemine başlamadan önce mahkeme kararları, arama tutanakları kontrol edilmelidir. Bu aşamada şahsın adı soyadı, T.C. kimlik numarası, mahkeme kararında CMK 134. Maddenin yer alıp almadığı, şahsa ait ele geçirilen materyallerin kararda ve/veya tutanakta ayrıntılı şekilde (marka, model, seri numarası, kapasite yazılıp yazılmadığı) yazılıp yazılmadığı, TD cihazına materyalleri bağlamadan önce cihazın sistem ayarları-nın kontrol edilmelidir. Özellikle tarih ve saat ayarının güncel olması gerekmektedir. Kaynak diski ve hedef disklerin bağlantısı

sağlam yapılmalıdır. Aksi durumda disklere zarar gelme durumu kaçınılmazdır.

İmaj almaya başlarken adımlar dikkatli bir şekilde izlenmelidir. İmaj alma esnasında kaynak ve hedef disklere dokunulmamalıdır. Elde edilen deliller dikkatlice paketlenerek listeye kaydedilmelidir. Alınan her bir cihaz için etiketlendirme yapılmış olması gerekir. Elde edilen verilerin taşınması ve korunmasında ise elektromanyetik alandan, nemli ortamlardan uzak tutulması, taşımasının anti statik ve darbe emici bulgu poşetleri ile yapılması önemlidir.

Veri Kurtarma: Mobil Cihazlar, Hard Diskler ve Nand Bellekler

Suçla mücadelede faaliyet gösteren kolluğun gelişen teknoloji ile birlikte karşılaştığı delil çeşitleri büyük bir hızla artmaktadır. Bu alanda çalışan birimlerin gelişen her bir teknoloji ile yeni incelemeci ve uzmanlara ihtiyacı olacağı doğaldır. Özellikle günümüz Adli Bilişim dünyasında mobil cihazların hacminin artışı bu alanda ciddi bir uzmanlığı ve Adli Bilişim inceleme metotlarını gerekli kılmaktadır. Keza yürütülen Adli Bilişim faaliyetleri kapsamında suç mahallinde ele geçirilen fiziksel darbe almış, yazılımsal arızaları olan, suya atılmış vb. sebeplerden dolayı normal koşullarda adli kopyası alınamayan hard disk, flash bellek, hafıza kartları, CD, DVD, Bluray, görüntü kayıt cihazları gibi dijital delillerden veri kurtarma konusu da benzer şekilde en çok karşılaşılan ve özel uzmanlık gerektiren temel alanlardan biridir. Bu her iki işlemde de kolluk uzmanları tarafından kullanılan inceleme teknik ve donanımları, kullanım amaçları ele alınacaktır.

Ulaşılabilirliği artan mobil cihazların taşınabilir olması ve kişiselleştirilebilir olması günlük hayatımızın neredeyse her alanına

sirayet etmelerini sağlamıştır. Mobil cihazlar yardımı ile kolayca internete bağlanılabilmesi, kişisel verilerin buradaki paylaşımı bir suçun aydınlatılmasında önemli bir veri hatta ilk akla gelen delil kaynağı olarak görülmesini kaçınılmaz kılmaktadır. Bugün mobil cihazlarla ilintili olmayan bir suç neredeyse kalmamıştır.

Mobil cihazlar kendine özgü işletim sistemleriyle hücresel bağlantı ve Wi-fi gibi diğer kablosuz bağlantı kanallarını kullanarak verileri iletmek, işlemek, depolamak amacıyla tasarlanmış cihazlardır. Mobil cihaz Adli Bilişiminin delil niteliği kazanması söz konusu olduğunda akla gelen işlemler adli kopya(imaj) almak, verilerin çıkarımı(export), ön inceleme, inceleme, analiz yapmak, işlemlerin raporunu oluşturmak ve arızası sebebiyle imajı alınamayan telefon, tablet vb. mobil cihazlara yazılımsal ve fiziksel müdahalede bulunarak adli kopya oluşturma, inceleme, raporlama, şifre kırma gibi iş ve işlemlerinin yapılması olacaktır.

İncelemeciler mobil cihazlar üzerindeki başlıca bilgi kaynaklarına aşina olmak için araştırma yapmaktadır. Bu kapsamda; sosyal medya, mesajlar, arama kayıtları ve multimedya dosyaları gibi silinmiş ögeler kurtarılır. Aktif ve kurtarılmış ögelerdeki dosya adı, zaman damgası, mesajın okunup okunmadığı, aramanın gelen, giden ya da cevapsız çağrı olması gibi üst veriler (metadata) toplanır. Kanıtların bulunması için anahtar kelime veya soruşturmaya özel bilgiler gibi metodolojik bir araştırma yürütülür. Olayların zaman çizgisi ve ilişki tablosu dahil edilerek, cihazın belleğinden elde edilen bilgilerin zamansal ve ilişkisel analizi yapılır. Adli Bilişim araçlarının hataları ve açıkları olabileceğinden önemli sonuçların doğruluğu sağlanır.

Bir mobil cihaza ilk müdahale yapılırken olay yerinin, cihazın ve cihaza ait ekranının fotoğrafları çekilmelidir. Mobil cihazın faraday çantasına konulması ya da uçak moduna alınması

gerekmektedir. Cihaza ait marka, model, imei numarası ve seri numarası kayıt altına alınır. Mobil cihaz açıksa kapatılmaz, kapalıysa açılmaz. Cihaza ait şifre, hafıza kartı ve seri numaralar tespit edilir.

Mobil alanda üç farklı imaj alma yöntemi vardır. Bunlar mantıksal imaj alma yöntemi, dosya sistemli imaj alma yöntemi ve fiziksel imaj alma yöntemidir. Mantıksal imaj alma yöntemi, en hızlı ve en dar kapsamlı imaj alma yöntemidir. Bu yöntemde adece telefonun içindeki veriler gelmektedir. Çok fazla sayıda cihaz desteği vardır. Dosya sistemli imaj alma yöntemi fiziksel imajı desteklemeyen telefonlarda fiziksel imaja en yakın veriyi getiren imaj alma yöntemidir. Son olarak fiziksel imaj alma yöntemi ise silinmiş veriler dahil tüm verileri getiren imaj alma yöntemidir. Daha çok veri getirdiği için imaj alma işlemi daha uzun sürer. Desteklediği cihaz sayısı diğerlerine göre daha azdır. İlk olarak başvurulan yöntem fiziksel imaj alma yöntemidir. Bunun mümkün olmadığı durumlarda diğer yöntemler denenmektedir.

Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı imaj elde etmede 8 farklı lisanslı yazılım kullanmaktadır. İşlemi gerçekleştirecek mobil incelemeci hangi yazılımı kullanacağını uygunluğuna göre seçmektedir. Son olarak başvurulan çare ise ana kart üzerinden hafıza çipinin sökülerek anlamlandırması işlemidir. Chip off denilen bu işlem cihazın lisanslı yazımları kullanarak imajının alınamadığı ve parçalanmış aşırı neme maruz kaldığı durumlarda cihazın hafıza çipinin ana kart üzerinden sökülerek özel aparatlar vasıtası ile okutulması işlemidir.

İncelemeciye ulaşan cihazların açılır vaziyette olmadığı, yazılımsal olarak çökmüş veya mevcut android sürümünün yüksek olması sebebi mevcut Adli Bilişim yazımları tarafından desteklenmiyor olması durumunda ise yazılımsal müdahale

yapılmaktadır. Yazılımsal müdahale ROM, Root atma ve Jailbreaktir. ROM işleminde Android işletim sistemli cihazlarda sorunların recovery bozulmalarında modele göre stock rom dosyası yüklenerek yazılım düzeltilir. Root atma işleminde Android işletim sistemli cihazlarda kök klasöre erişim sağlanarak admin (yönetici) yetkisi alma işlemidir. Bu sayede üretici tarafından yazılım düzeyinde alından güvenlik tedbirlerinin aşılması hedeflenmektedir. Son olarak Jailbreak işlemi ise Root işleminin iOS işletim sistemli telefonlardaki halidir. iOS işletim sistemli telefonlara daha fazla erişim sağlamak için yapılan işlemdir.

İşlemler neticesinde mobil cihazın servis sağlayıcısından elde edilecek bilgiler arama kaydı detayları (CDR), abonelil bilgisi, sesli mesajlar, izleme bilgisi ve kullanım bilgisidir. SIM karttan elde edilecek bilgiler telefonun numarası (MSISDN), cihaza ait uluslararası mobil abone kimliği (IMSI), cihaza ait bütünleşmiş devre kart tanımlayıcısı (ICCID) yani kartın seri numarası, cihazın servis sağlayıcı adı (SPN), cihazın dil tercihleri ve telefon kapatıldığındaki konum bilgisidir. Mobil cihazlardan elde edilecek bilgiler, cihaza ait uluslararası mobil ekipman kimliği (IMEI), mobil Cihaz bilgisi (CDMA seri numarası), ağ trafik bilgisi, cihazda kullanılmış olan GPS konum bilgisi, mobil cihazda yer alan takvim, hatırlatma, yapılacak listesi ve radyo işlevlerinin durumu, kullanılan baz istasyonu ve kanal durumu, Gateway bilgisi, cihazın kaynakları kullanım durumu gibi iletişim loğlarıdır. Yine mobil cihaz yahut hafıza kartı yoluyla elde edilebilecek bilgiler, Cihaza ve hafıza kartına ait fotoğraflar, videolar ve ses dosyaları, E-postalar, dokümanlar vb., internet kullanım bilgisi, tarayıcı geçmişi, favori sitelerin listesi, kurulan uygulamalara ait bilgiler: anlık mesajlaşma bilgileri, sosyal medya kayıtları, uygulama veri tabanları, GPS kullanım bilgisi verileri olarak sayılabilir.

Son derece titizlik ve uzmanlık gerektiren bu işlemleri yapan Adli Bilişim uzmanlarının gerekli eğitimleri almış olması, hukuki süreçlere hakim olması, delil zincirine dikkat etmesi, mobil alanındaki yazılım ve donanımların kullanımına hakim olması, güncellemeleri yakından takip edebilmesi, AR-GE yapabilmesi, gelişime açık olması ve kendini hızlı yenileyebilmesi ve etik ve ahlaki kurallara dikkat etmesi aranılan temel özelliklerdendir.

Veri kurtarmaya konu bir diğer önemli husus hard disk ve nand çipli bellekler gibi hafıza barındıran donanımların, fiziksel ve yazılımsal müdahalede bulunarak arızasının giderilmesi ve verinin okunmasını sağlama işlemidir. Bu kapsamda CD, DVD, BLU-RAY, HDD, SSD, SD Kart, USB Bellek, DVR cihazları gibi kısaca hafıza birimi bulunan her türlü depolama aygıtından veri kurtarma çalışmaları yapılmaktadır. Bu aygıtlar genellikle çeşitli programlar vasıtasıyla depolama biriminde bulunan hataların giderilerek yapılan yazılımsal veri kurtarma işlemi ile yahut fiziksel arıza, düşme, kırılma, darbe alma, ekonomik ömrünü doldurma gibi sebeplerle depolama cihazının çalışamaz hale geldiği durumlarda, fiziksel müdahale yoluyla verilerin kurtarılması işlemidir.

Her veri kurtarma vakası ayrı değerlendirilmelidir. Ancak genel itibariyle adımlar depoloma cihazının arıza tespiti (fiziksel/yazılımsal), arızanın çözümüne yönelik çalışmalar ve tamiri, verilere ulaşma, verilerin kurtarılması ve adli kopya alınması olarak sıralanabilir.

Daha önce başka biri tarafından yapılmış başarısız veri kurtarma denemeleri, diskin fiziki olarak (kapağının açılması, devre elemanlarının değiştirilmesi vb.) kurcalanması, mekanik disklerden olağan dışı sesler gelmesi, gözle tespit edilebilen fiziksel hasar, darbe, kırık, sel veya yangın hasarı vb. zorluklar veri kurtarma işlemini zorlaştıracak temel unsurlardır. Yazılımsal olarak

ise genellikle insan hatasının yol açtığı durumlar, başarısız güncellemeler, hatalı uygulama yazılımları, bilgisayar donanım hataları, işletim sistemi hatalarının sistemi çökertmesi, virüs hasarı, delilleri yok etmek amaçlı sabotajlar karşılaşılan zorlukların en başlıcalarıdır.

Nand çipli belleklerden veri kurtarma işlemlerinde öncelikli olarak materyallerin yazılımsal veya donanımsal arızaları tespit edilmektedir. Yazılımsal arızası olduğu değerlendirilen materyallerin veri bütünlüğü bozulmadan Adli Bilişim yazılım ve donanımları kullanılarak uygun komutlarla arızası giderildikten sonra adli kopyaları alınmaktadır. Donanımsal arızası olduğu değerlendirilen materyallerin ise hafıza çipi, chip-off yöntemi ile uygun sıcak hava ve flux yardımı ile sökülerek bağlantı bacakları izopropil alkol ve fırça yardımı ile temizlenir. Daha sonra uygun okuyucu adaptör içerisine yerleştirilerek mevcut (PC3000 Flash, Rusolut VNR, Soft Center FE) özel yazılım ve donanım marifeti ile nand hafıza çipinin ID bilgisinin okunması sağlanır. Okunan ID bilgisine uygun olarak Raw Data okuması yapılır ve dump (raw datanın bulunduğu dosya-çöplük) dosyası oluşturulur. Oluşturulan ham verinin de çeşitli yazılımlar vasıtasıyla anlamlandırma işlemi gerçekleştirilerek adli makamlara teslim edilir.

Yukarıda bahsi geçen yöntem ve tekniklerle uzman kolluk personeli tarafından yürütülen işlemler neticesinde kritik delillere ulaşılmıştır. Yanmış ve toprağa gömülmüş hard disklerden veri kurtarılması, darbe girişimi sonrası tanklarla imha edilmeye çalışılan hard disklerden veriler kurtarılması ve yine 15 Temmuz sonrası F-16 ve askerî helikopterlerin rota kayıt sistemleri ve iç kameralarının görüntülerinin elde edilmesi bu hususta başlıca iyi uygulama örneklerindendir.

Adli Bilişim Uygulama Sürecinde Olası Riskler

Adli Bilişim işlemlerinin gerçekleştirilmesi için bilişim sistemlerine ve diğer cihazlara usulüne uygun şekilde el konulması, Adli Bilişim kurallarına uygun bir şekilde yedeklenmesi, alınan yedeklerin incelenmesi, mahkemeye sunulacak şekilde hazırlanması uygun şekilde paketlenmesi, taşınması ve saklanması gerekir.

Dijital cihazlar üzerindeki Adli Bilişim işlemleri; Bu cihazların kişiler tarafından işlenen suçta araç olarak kullanılması, suçun işlenmesinde doğrudan kullanılmayıp kişilerin bu cihazları aralarındaki iletişimi sağlamak için kullanılması ve bilgileri yedeklemek amacıyla kullanmaları durumunda gerçekleştirilmektedir.

Adli Bilişim, yargı organlarına yardımcı olmanın yanı sıra günümüzde bazı şirketler ve kişiler tarafından veri kurtarma, imha etme veya sair amaçlarla ihtiyaç duyulan bir alan haline gelmiştir. Adli Bilişim sürecinin belirleyici iki unsurundan birisi Adli Bilişim uzmanı iken diğeri uzmanın yararlanabileceği donanım ve yazılım programlarıdır. Gerek donanım ve yazılım yahut uzman kişilerden kaynaklı, gerekse başka gerekçelerden kaynaklı olarak Adli Bilişim sürecini sekteye uğratacak olası risk ve problemler şu şekilde sayılabilir;

- Bazı materyallerin kaybolması, Adli Bilişim sürecine hiç başlanamaması ya da atılı suça ilişkin delillerin toplanamaması,
- Ağ trafiği analizinde delilin doğruluğunun ya da gerçekliğinin sağlanamaması,
- Mobil cihazlarda ileri uzmanlık gerektiren teknik yöntemler veri kaybı ya da verinin gerçekliğine şüphe düşürme riski,
- Adli Bilişim ilke ve standartlarının belirlenmemesi, elektronik delilin elde ediliş sürecine ilişkin sorumluluklar ile bilirkişi görevlendirilmesine dair yasal düzenlemelerin bulunmaması (ISO standartı),

- Laboratuvarların yeterli seviyeye gelmemiş olması, delil elde etmede kullanılan program, cihaz ve donanımın zamanla eskiyeceği gözetilerek yenilenmemesi, bu standartların birtakım sertifikalarla kanıtlanması gereği,
- Uygulayıcıların yeterince eğitilmemesi, elektronik delilinin sahip olduğu farklı özellikler Adli Bilişim sürecinde görev alan teknik personel tarafından bilinerek bu doğrultuda araştırmaların yürütülmesi gerekir. Güncel teknolojinin takip edilmesi ve temel seviyede gerekli hukuk bilgisine sahip olunması gerekir. (ehliyetsiz kişilerin bilirkişi olarak atanmaları),
- Adli Bilişim sürecinde yaşanan hukuka aykırılık halleri.

Şifreli verilerde şifre çözme anahtarlarının cihaz sahibinin ya da üçüncü şahıslardan istenilip istenilemeyeceği hususunun kişinin kendi aleyhine delil göstermeye zorlanması kapsamında yasaktır. Bilişim cihazlarına uzaktan erişim yolu ile yapılan aramanın hukuka uygun olup – olmadığı sorununda da Avrupa Siber Suç Sözleşmesinin 32.maddesine göre *"..ancak bilgisayar sistemi üzerinden verilere erişim yetkisine sahip olan bir kişinin yasal izninin bulunması ya da bu verilerin herkesin erişimine açık olduğu durumlarda.."* sınır ötesi erişimin sağlanabileceği belirtilmektedir. Türk hukuk sisteminde ise buna cevaz veren bir görüşe göre CMK'nın 134.maddesindeki "Arama" ibaresinin "Elektronik Veri Takibi" şeklinde yorumlanması halinde bilişim sistemine uzaktan erişim sağlanarak yazılım üzerinden ve gizli olarak gerçekleştirilebileceği savunulmaktadır.

- Digital Kopyası alınan cihazların iadesi hususunda dikkat edilmesi gereken birtakım hususlar bulunmaktadır.

C.M.K. 134/2 nci maddesi "el konularak kopyası alınan cihazlar derhal sahibine iade edilir" hükmünü havidir. Bununla

beraber, bulundurulması bizatihi suç teşkil eden askeri casusluk, fikri ve sınai mülkiyet casusluğu, çocuk istismarı, kredi kartı bilgileri, özel hayatın gizliliğini ihlal gibi suçlara ilişkin verilir içeren asıl materyal veya digital kopyasının şüpheliye iade edilmesi telafisi giderilemeyecek zararlara yol açabileceği gibi, asıl materyalin iade edilmemesi halinin özel mülkiyet hakkının ihlaline yönelik sorunlara açabileceği değerlendirilmektedir. Bu hususta iç hukukumuzda bir düzenleme bulunmamaktadır. Bununla beraber Avrupa Siber Suç Sözleşmesinin 19/3-d maddesi buna cevaz vermektedir.

MADDE 19: Taraflardan her biri, yetkililerinin, paragraf 1 veya 2'ye göre erişilen bilgisayar verilerini elde etmek veya güvenlik altına alabilmesi için, o kişileri yetkilendirmeleri ile ilgili gerekli yetki ve diğer önlemleri benimseyecektir. Bu önlemlerin içinde;

a. Bir bilgisayar sisteminin veya bir bölümünün veya bir bilgisayar veri depolama ortamının elde edilmesi veya benzer şekilde güvenlik altına alınması

b. Bu bilgisayar verisinin bir kopyasının alınması tutulması.

c. İlgili depolanmış bilgisayar verisinin bütünlüğünün sağlanması.

d. Erişilen bilgisayar sistemindeki bu bilgisayar verisinin silinmesi veya erişilmez hale getirilmesi")

Anayasamızın 90/4. maddesi "usulüne uygun olarak onaylanmış Milletlerarası Anlaşmalar Kanun hükmündedir" hükmünü içerir. İçişleri Bakanlığı Emniyet Genel Müdürlüğü Siber Daire Başkanlığı da 2015 yılında bu konuda Adalet Bakanlığı Ceza İşleri Genel Müdürlüğünden mütalaa istemiş olup, Bilgi İşlem Genel Müdürlüğünün de önerileri ile suç içeren asıl materyalin "geri dönüştürülemeyecek şekilde verilerin silinerek"

(ToT5210.22-m veya Gutmann Metodu ile) şüpheliye iadesine dair görüş bildirmiştir. Uygulamada ise Sulh Ceza Hakimliklerinden bu hususta karar alınamamaktadır.

Sonuç olarak Adli Bilişim bir soruşturma kapsamında bilişim sistemlerinde bulunan elektronik delile ilk temas edildiği andan yargı makamları önüne getirileceği ana kadar geçen sürecin bütünüdür. Suçluların cezalandırılabilmesi, adil yargılamanın gerçekleşmesi ancak usulüne uygun elde edilecek delillerle mümkün olabilir. Adli Bilişim süreci sonucunda bilişim sistemlerinden ya da veri depolama birimlerinden elde edilen elektronik veriler çözümlenerek verinin kaynağının ne olduğu ne zamandan beri cihazda bulunduğu, üzerlerinde herhangi bir değişiklik ya da tahribat yapılıp yapılmadığı, yapılmış ise ne zaman ne şekilde yapıldığı sorusu tespit edilir. Bu süreçte ortaya çıkan birçok sorun elektronik delilin kaybolmasına ya kullanılmaz hale gelmesine neden olabilir.

Ulusal Siber Olaylara Müdahale Merkezi'nin (Usom) Siber Güvenlik Dünyasında Adli Bilişim Süreçleri

Bilgi Teknolojileri ve İletişim Kurumu bünyesindeki Ulusal Siber Olaylara Müdahale Merkezi (USOM), ülkemizde faaliyet gösteren kurumsal ve sektörel Siber Olaylara Müdahale Ekip'lerinin (SOME) koordinasyon, iletişim ve iş birliği sağlamaları amacıyla görev yürütmektedir. USOM'un görevlerinden bir diğeri de kritik altyapılarda sektörel güvenlik önlemlerinin belirlenmesi ve uygulanması amacıyla ülkemizde konumlandırılmış EKS/SCADA sistemlerinin güvenliğinin denetlenmesidir. USOM yaptığı tüm çalışmalarda tamamen kendi öz imkanlarıyla geliştirmiş olduğu proje ve araçları kullanarak bu sistemlerin erişim ve zafiyet tespitlerini gerçekleştirmektedir.

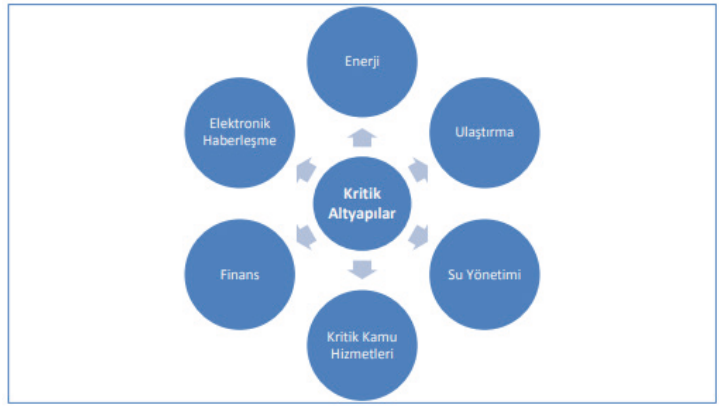
"Kritik Altyapı" son yıllarda hemen hemen dünyanın her yerinde oldukça tartışılan ve henüz ülkeler arasında ortak bir tanımı yapılmayan kavramdır. Fakat, ABD ve AB ülkeleri başta olmak üzere enerji, su, ulaşım, sağlık, bankacılık, nükleer/kimyasal tesisler ve haberleşme altyapılarını kritik sektörler olarak belirlemiş ve bu sektörlere ait altyapıları kritik altyapılar olarak nitelendirmişlerdir. AB komisyonunun 2004 tarihli "Terörizmle Mücadele Kapsamında Kritik Altyapıların Korunması" başlıklı tebliğinde ve ABD mevzuatında kritik altyapı tanımları yapılmış ve "insanların hayati sosyal fonksiyonlarının, sağlıklarının, emniyetlerinin, güvenliklerinin, ekonomik ve toplumsal refahlarının devamı için gerekli olan ve aksama veya yok edilmesi bu fonksiyonları sürdürmede yetersiz kalma sonucunda bir üye ülkede belirgin etki gösterecek varlık, sistem veya ilgili parçaları" olarak tanımlamışlardır. Ülkemizde ise "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"na göre; kritik altyapılar, işlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara ve ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar olarak tanımlanmıştır.

Başta enerji olmak üzere birçok sektörde aktif olarak kullanılan Endüstriyel Kontrol Sistemleri (EKS) kritik altyapıların en önemli bileşenlerinden biri olarak kabul edilmektedir. Ayrıca farklı sektörlerde faaliyet yürüten endüstriyel kuruluşların fiziksel olarak sahadan aldıkları verilerin izlendiği ve yine sahadaki ekipmanlara belirli komutlar göndererek istenilen fonksiyonel işlerin yapılmasını sağlayan SCADA (Supervisory Control and Data Acquisition - Danışmalı Kontrol ve Veri Toplama) sistemleri de endüstriyel sektörde faaliyet gösteren kritik altyapıların bileşenlerinden biridir. Bu bakımdan, ülkemizde faaliyet gösteren kurum ve kuruluşların kritik altyapılarının siber güvenlikle-

rinin sağlanması ve olası risk durumlarına karşı hazırlıklı olunması hayati derecede bir öneme sahiptir.

Özellikle bilgi ve iletişim teknolojisinin son derece hızlı bir şekilde yaygınlaştığı son yıllarda kurum ve kuruluşlar bilgi sistemleri altyapılarını internet teknolojisi vasıtasıyla uzaktan yönetmektedirler. Aynı durum EKS/SCADA sistemleri için de geçerlidir. İlgili kurum ve kuruluşlar kritik altyapılarının yönetimi, haberleşmesi, arıza kontrolü ve bilgi erişimi amacıyla çalışanlarına sistemlerini internet erişimine açma gereği duyabilmektedirler. Bu şekilde çalışanlar, ilgili sistemlere fiziksel olarak erişim gereği duymadan internet erişimi üzerinden gerekli işlemleri yapabilmektedirler. Fakat bu durum işleri kolaylaştırmasının yanında güvenlik risklerini de beraberinde getirmektedir. EKS/SCADA sistemlerinin internet erişimine açık olması durumunda endüstriyel faaliyet yürüten kurum ve kuruluşlar siber güvenlik ihlalleri ile karşı karşıya kalabilmektedirler.

Ülkemizde ilk olarak "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" kapsamında kritik altyapıların belirlenmesi ve bu altyapıların güvenliğinin sağlanmasına yönelik çalışmaların başlatılmasına karar verilmiştir. Belirlenen kritik altyapı sektörleri "Ulaştırma, Enerji, Elektronik Haberleşme, Finans, Su Yönetimi, Kritik Kamu Hizmetleri" olarak sıralanmıştır. Daha sonrasında yapılan strateji ve eylem planları ile birlikte ülkemizde bulunan bütün kritik altyapıların belirlenmesi, ilgili denetleyici / düzenleyici kurumlara sorumluluklarının verilmesi, kurumsal ve sektörel planların oluşturulması ve gerekli rehber, mevzuat ve yönetmeliklerin hazırlanması sağlanmıştır.



Şekil 1: Türkiye'nin Kritik Altyapı Sektörleri

EKS/SCADA Protokolleri ve Portları

EKS/SCADA Sistemleri'nin erişim ve zafiyet tespitleri için ilk olarak bu sistemlerin iletişim ve yönetim servisleri ve bu servislerin kullandıkları portlar analiz edilmiştir. Bu analizlerin gerçekleştirilmesinde literatür araştırmaları ve açık kaynaklı arama motorlarından faydalanılmıştır. Bu araştırmalar sadece ilgili servislerin hangi portlarda çalışabileceği ve USOM olarak yapılacak çalışmalarda nasıl optimize ve otomatik bir şekilde tespit edilebileceği amacıyla kullanılmıştır.

Tablo 1'de bugüne kadar çalışmaları yapılmış EKS/SCADA servis ve portları listelenmiştir. Burada bazı servisler aynı portlarda çalışabilmektedir; örneğin Siemens S7, ICCP ve IEC 61850 / MMS servisleri port 102 üzerinde çalışmaktadır. Aynı zamanda tek bir servis birden fazla port üzerinde de çalışabilmektedir; örneğin Niagara Tridum Fox servisi port 1911 ve 4911 üzerinde çalışabilmektedir.

Tek bir port üzerinde birden fazla protokolün çalışabileceği ve tek bir servisin de birden fazla port üzerinde çalışabileceği

durumuna istinaden sadece port numaralarını baz alarak EKS/SCADA sistemlerini tespit etmek yeterli değildir. Aynı zamanda EKS/SCADA cihazlarında çalışan servisler tarafından sağlanan meta veri bilgileri de kullanılabilmektedir.

Tablo 1: Sık Kullanılan EKS/SCADA Protokolleri ve Varsayılan Portları

Protokol	**Varsayılan Port**
Automated Tank Gauge (ATG)	10001
BACnet	47808
CodeSys	2455
Crimson 3	789
DNP3	20000
EtherCAT	34980
EtherNet/IP	44818,2222
GE-SRTP	18245,18246
HART-IP	5094
ICCP	102
IEC 60870-5-104	2404
IEC 61850 / MMS	102
KNX	3671
MELSEC Q	5006,5007
Modbus/TCP	502
Moxa	4800
Niagara Tridium Fox	1911,4911
OMRON FINS	9600
OPC	80, 4840
PcWorx	1962
ProConOS	20547
Siemens S7	102

EKS/SCADA Cihaz Tespitleri

Bir önceki bölümde bahsedilen EKS/SCADA sistemlerinin haberleşmesi sırasında en sık kullanılan protokol ve varsayılan port numaralarına ek olarak ilgili sistemlerin haberleşmesi ve yönetiminde kullanılan servis ve portlar tespit edilerek EKS/SCADA cihazlarının tespitleri de yapılmaktadır. İlgili cihazların tespitleri de yine USOM'un geliştirdiği proje ve araçlarla gerçekleştirilmektedir. Tablo 2'de bazı EKS/SCADA cihazları veya yazılımları ve bu cihazların bazılarının tespit edilebildiği servisler listelenmiştir.

Tablo 2: EKS/SCADA Cihazlarının Tespit Edildiği Varsayılan Portlar

Cihaz/Yazılım	Tespit Edilen Varsayılan Port
ABB	80,8080,443,502,47808
ComAp	80,8080,443
Enda PLC	23
Four-Faith	80,8080,443,23
GMTPLC	23
HMI-WebServer	5900
iGrid-iRTU	23
Lantronix	161
Moxa	23,80,8080,161,4800
Powerlogic	80,8080,443
Ricon	23,80,8080
Robustel	23,80,443,8080
Rockwell Automation / Allen Bradley	44818
Schneider	502,47808
Simatic	161
Siemens S7	80,8080,443,161,102
Siemens-Scalance	161
Solar-Log	80,8080,443
Stawiz Automation	80,8080,443

Cihaz/Yazılım	Tespit Edilen Varsayılan Port
Sunny-Webbox	80,8080,443
Teltonika	80,8080,443
Wago	80,8080,443
WinCC	1433,1434,49165

Türkiye'de Tespit Edilen Bulgular

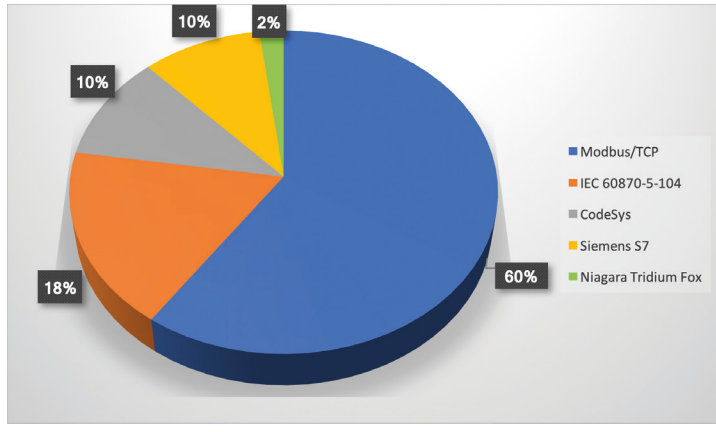
USOM tarafından yürütülmekte olan EKS Güvenliği çalışmaları kapsamında internet erişimine açık EKS/SCADA cihazlarının, haberleşme protokollerinin ve zafiyetlerinin tespiti için şu ana kadar toplamda 54 adet farklı tespit yöntemi kullanılmaktadır. Bu yöntemlerden bazıları EKS/SCADA sistemlerinin haberleşmesi sırasında kullandıkları protokol tespiti üzerine bazıları ise ilgili cihazların yine haberleşme ve yönetim servislerinin tespiti üzerinden gerçekleşmektedir. Yapılan çalışmalarda ilgili sistemlerin canlı çalışır sistemler olduğu ve fonksiyonel arızalanma riskleri de göz önünde bulundurulmuştur.

Bu bölümünde, USOM'un yürütmüş olduğu EKS Güvenliği çalışması kapsamında tespit edilen EKS/SCADA haberleşme protokollerinin ve cihazlarının istatistiki bilgileri sunulmuştur. Sunulan istatistiki bilgiler hem protokoller hem de cihazlar için en sık karşılaşılan ilk 5 protokol ve ürün bazında değerlendirilmiştir. Verilen istatistikler sadece bu ilk 5 protokol ve cihazlar arasındaki yüzdelik oranlarını ifade etmektedir. Bu kapsamda ülkemizde internet erişimine açık en sık karşılaşılan EKS/SCADA haberleşme protokolleri ve cihazları analiz edilmiştir.

Protokol Bazlı İstatistikler

EKS/SCADA güvenliği kapsamında ülkemizde faaliyet gösteren endüstriyel altyapıya sahip kurum ve kuruluşların siber güvenliğinin ve iş sürekliliğinin sağlanması, milli güvenliğimizin

öncelikli alanlarındandır. Daha önce de bahsedildiği gibi EKS/SCADA sistemlerinin yönetimi, haberleşmesi, arıza kontrolü ve bilgi erişimi amacıyla bu sistemler internet erişimine açılabilmektedir. Bu durumda olası siber güvenlik ihlallerinin olması söz konusu olabilmektedir. Bu bakımdan, USOM olarak ilgili EKS/SCADA haberleşme protokol ve servislerinin tespiti yapılmakta ve ilgili kurum ve kuruluşlara ihbar süreci işletilmektedir. Yapılan çalışmalar sonucunda EKS/SCADA haberleşme protokollerinin istatistiksel sonuçları paylaşılmıştır. Elde edilen bu istatistiki bilgiler, en sık karşılaşılan 5 EKS/SCADA haberleşme protokolü baz alınarak sunulmuştur. Bu sonuçlar sadece bu 5 protokol içerisindeki kullanım oranlarını ifade etmektedir. Protokol bazlı yapılan çalışma sonucunda elde edilen istatistiki bilgiler Şekil 2'de gösterilmiştir.



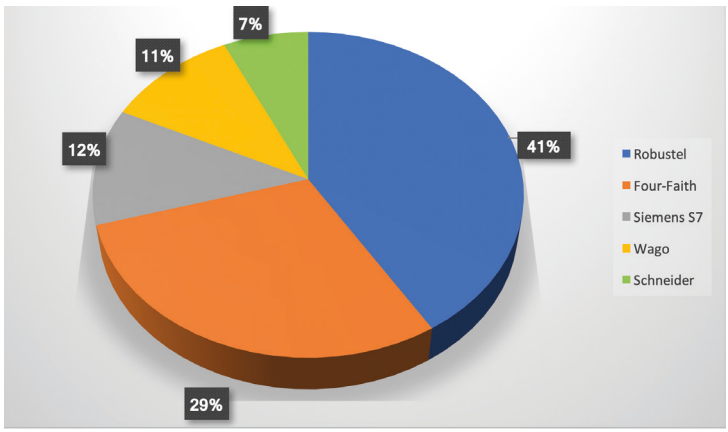
Şekil 2: Türkiye'de En Sık Karşılaşılan EKS/SCADA Haberleşme Protokol Oranları

Şekil 2'den de görüleceği üzere, ülkemizde en sık kullanılan EKS/SCADA haberleşme protokolü Modbus/TCP'dir. Bunun başlıca nedeni bu protokolün açık kaynaklı olması ve birçok üretici firmanın cihazları tarafından desteklenmesidir. Güvenlik açısından

bakıldığında ise, bu protokolün zafiyetlerinin istismar edilmesi oldukça kolaydır. İnternet erişimine açık Modbus/TCP üzerinden haberleşen bir EKS/SCADA sisteminin veri manipülasyonu ve hizmet engellemesi gibi tehditlere maruz kalması olasılığı yüksektir.

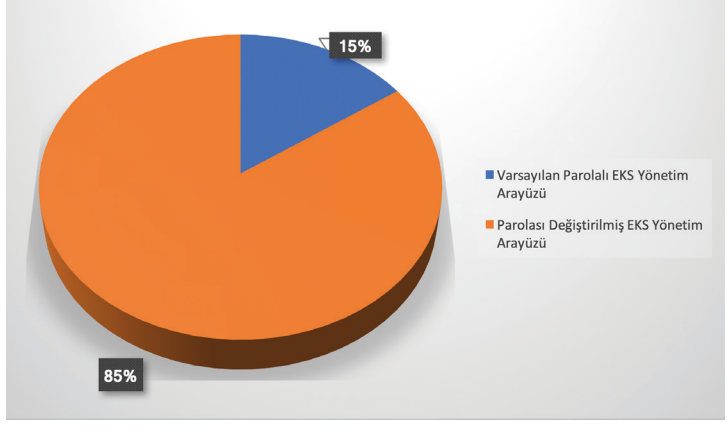
Cihaz Bazlı İstatistikler

EKS/SCADA güvenliği çalışmaları kapsamında bu sistemlerin haberleşme protokollerinin tespitlerinin yanı sıra yine bu sistemlerin haberleşme ve yönetim servislerinin tespiti sağlanarak hangi markalı cihazların kullanıldığı bilgisi de elde edilebilmektedir. Protokol bazlı çalışan yöntemlerden elde edilen sonuçlardan bazılarında yine cihaz tespitleri de yapılmaktadır. Örneğin, Modbus/TCP haberleşme protokolünün tespiti çalışmalarında Schneider markalı EKS/SCADA cihaz tespitleri de yapılmış ve istastiki bilgilere bu şekilde işlenmiştir. Ülkemiz genelinde endüstriyel alanda en sık kullanılan ilk 5 EKS/SCADA cihazlarının marka bilgilenin sunulduğu ististiki bilgiler Şekil 3'de verilmiştir. Yine bu sonuçlar sadece bu 5 cihaz içerisindeki kullanım oranlarını ifade etmektedir.



Şekil 3: Türkiye'de En Sık Karşılaşılan EKS/SCADA Cihaz Marka Oranları

Şekil 3'den görüldüğü üzere, ülkemizde en sık kullanılan EKS/SCADA cihazlarının markaları ağırlıklı olarak endüstriyel yönlendirici cihazlarıdır. Bu cihazlar fiziksel olarak diğer BT yönlendirici cihazlarına göre daha dayanıklı bir yapıya sahip olmalarına rağmen BT cihazlarında mevcut olan güvenlik zafiyetlerini de barındırmaktadır. İnternet erişimine açılmış olan bir endüstriyel cihaz üzerindeki bir zafiyetin sömürülmesi sonucunda ilgili kurum ve kuruluşun ciddi siber güvenlik ihlalleriyle karşılaşma olasılığı yüksektir. Bir saldırganın endüstriyel bir cihaz üzerinde ilk olarak tercih ettiği saldırı yöntemi cihazın kurulum esnasında verilen yönetim servisindeki varsayılan kullanıcı adı parolasını denemesidir. USOM olarak EKS/SCADA cihazlarının yönetim ara yüzlerinin parola güvenliği çalışmaları da yürütülmektedir. Ülkemizde faaliyet gösteren bu endüstriyel cihazların şu ana kadar tespit edilen varsayılan kullanıcı adı parola kullanım oranları Şekil 4.3'de gösterildiği gibidir.



Şekil 4: Türkiye'de Tespit Edilen Varsayılan Parolalı EKS/SCADA Yönetim Arayüzü

EKS/SCADA Güvenliği Kapsamında Alınabilecek Önlemler

Dokümanın daha önceki bölümlerinde de üzerinde durulduğu gibi EKS/SCADA sistemlerinin internete açık bir haberleşme altyapısı, yönetim ara yüzü / servisi veya cihazlarının bulunması, internet ortamından gelebilecek tehditlere karşı savunmasız kalmasına sebep olabilmektedir. Erişime açık EKS/SCADA sistemi, söz konusu servislere ağ seviyesinde internet üzerinden tüm kullanıcıların erişebiliyor olması durumudur. EKS/SCADA sistemlerinde kullanılan veri tabanlarına, yönetim web ara yüzlerine, endüstriyel yönetim konsollarına ve endüstriyel haberleşme servislerine internet üzerinden yetkisiz erişimin sağlanabildiği sistemlerdir. Bu yetkisiz erişim ile sistemin bütününü veya bir kısmını bozmaya yönelik girişimler olabilmektedir. Yapılan girişimlerin başarılı olması sonucunda, ilgili sistem ve/veya bağlı sistemlerde (MTU, RTU, HMI, IED, vb.) siber güvenlik ihlali yaşanabilir. Siber güvenlik ihlallerine örnek olarak depolanan kritik veya gizli verilerin çıkarılması, sistem üzerinde istenmeyen değişiklikler yapılması, cihaz üzerindeki sistemlerin hizmet verememesi gösterilebilir.

Bu nedenle güvenlik sıkılaştırmaları yapılması, güncellemelerinin uygulanması, parola yönetimlerinin doğru şekilde yapılması ve erişim denetiminin gerçekleştirilmesi büyük önem arz etmektedir. İlgili servisin bilinen herhangi bir zafiyeti bulunmasa dahi sıfırıncı gün zafiyetlerinin de dikkate alınarak erişim kısıtlamalarının uygulanması gerekmektedir.[1] Bu bakımdan, ilgili sistemlerde alınabilecek güvenlik önlemleri kısa, orta ve uzun vadeli eylemler olarak listelenmiştir. Bu önlemler sayesinde olası bir siber ihlal durumunda yürütülecek Adli Bilişim sürecine katkısı olacağı değerlendirilmektedir.

[1] Tespit edilen sıfırıncı gün zafiyetlerinin yayınlandığı linke https://www.usom.gov.tr adresinden erişilebilir.

Kısa Vadeli Önlem ve Eylemler

- Söz konusu servislerin İnternet üzerinden erişimlerine ihtiyaç duyulmuyorsa erişimler kapatılmalıdır. Eğer ilgili servislerin internet üzerinden erişimine ihtiyaç var ise yalnızca yetkilendirilmiş IP adreslerin erişimine izin verilecek şekilde kısıtlama uygulanmalıdır.
- Endüstriyel kontrol sistemi servislerine ek olarak, bu sistemlere erişim için kullanılan ağ cihazları ve ilişkili tüm sunucu sistemlerindeki uzaktan yönetim servislerinin de İnternet üzerinden erişimlerine ihtiyaç duyulmuyorsa erişimler kapatılmalıdır. Eğer ilgili servislerin internet üzerinden erişimine ihtiyaç var ise yalnızca yetkilendirilmiş IP adreslerin erişimine izin verilecek şekilde kısıtlama uygulanmalıdır. Son kullanıcıların erişimleri kurumun mevcut ise süreli olarak VPN servisleri üzerinden yapılması sağlanmalıdır.
- Güçlü parolalar seçilmelidir. Parolasız veya varsayılan kullanıcı adı/parola ile olan hesaplar kapatılmalıdır. Ayrıca parolalar; kurum adı, kişi adı, uygulama adı gibi bilgiler içermemelidir.
- Hassas bilgilerin (kullanıcı adı, parola vb.) ağ üzerinde sadece güçlü algoritmalar kullanılarak şifrelenmiş (TLS vb.) bir şekilde iletildiğinden emin olunmalıdır. Şifrelenmemiş şekilde işlem yapan protokoller (telnet, ftp vb.) kullanılmamalıdır.

Orta Vadeli Önlem ve Eylemler

- Olası yetkisiz erişim ile söz konusu sunucu/sunucular üzerinden ağda yayılma durumları gerçekleşebilir. Bu durumu tespit etmek için sunucular üzerindeki gerekli iz kayıtları ile birlikte kurum ağında bulunan diğer cihazların ve güvenlik duvarı gibi ağ cihazlarının iz kayıtları ince-

lenmelidir. Olası anomalilerin tespiti için iz kayıt yönetimi araçlarından ve YARA kurallarından yararlanılabilir.

- Tespit edilen zararlı aksiyonlar ilişkili sistem/uygulama belirtilerek USOM ile paylaşılmalıdır.
- Endüstriyel kontrol sistemlerine dış ağdan teknik destek veya uzaktan bağlantı yapılması gereken durumlarda üçüncü parti yazılımlar kullanılması yerine VPN altyapısının kullanılması ve uzak bağlantı sırasında ilgili personelin yapılan işleri izlemesi gerekmektedir.
- Endüstriyel kontrol sistemlerini ve ilişkili sistemlerin dış ortamlardan ayırmak için kullanılan güvenlik duvarı yapılandırmalarında içe doğru (inbound) uygulanan kısıtlar gibi dışa doğru (outbound) da kısıt uygulanmalı, iç ağdan dışarı kontrolsüz erişim sağlanamamalıdır.
- Kurum iç ağında kritik sistemlere erişimin etkili bir şekilde kontrol edilmesi ve kısıtlanması gerekmektedir. Gerekli izinler 'en az yetki' ve 'görevlerin ayrımı' prensipleri göz önünde bulundurularak verilmelidir.
- Endüstriyel kontrol sistemlerini dış ağlardan ayıran ağ cihazları ve diğer ara katman cihazlarda ve bu cihazlar üzerindeki bulunabilecek servislerde güvenlik güncelleştirmeleri uygulanmalıdır.
- Endüstriyel kontrol sistemleri ile iletişimde olan diğer tüm cihazlarda (operatör bilgisayarları, HMI, SCADA sunucuları, PLC, RTU vb.) güvenlik sıkılaştırmalarının (sektörel iyi uygulamalar, USB ve benzeri donanımsal kısıtlamalar, tam disk şifreleme vb.) uygulanması önerilmektedir.
- İlgili sistemler üzerinde üretici firmaları ve USOM güvenlik bildirilerinde yayınlanan güncel zafiyetler takip edilmeli ve gerekli aksiyonlar ivedilikle uygulanmalıdır.

Uzun Vadeli Önlem ve Eylemler

- Sistemlerde gerçekleşebilecek veri hasarı/kaybı gibi durumlar için kritik verilerin (iz kayıt, yapılandırma, kritik dosyalar, vb) yedekleri düzenli olarak harici bir ortamda alınmalıdır.
- Endüstriyel Kontrol Sistemleri üzerinde bulunan kullanıcıların rolleri gözden geçirilmeli, erişim yetkileri kontrol edilerek yetkisiz erişimlerin olmadığından emin olunmalıdır.
- Kurumda siber olayların tekrar yaşanmaması için gerekli güvenlik önlemleri alınmalı ve güvenlik sıkılaştırmaları yapılmalıdır.
- Belirlenen tüm önlemlerin yeni kurulum yapılacak sistemlerde de uygulanabilmesi amacıyla, ilgili sistemler için kurulum prosedürü hazırlanması, erişim izinlerinin sıkılaştırılması, parola ve yama yönetimi konusuna yer verilmesi önerilmektedir.

Toplumsal Farkındalık Geliştirme; Siberay

Ulusal ve uluslararası platformlarda, siber güvenlik, teknoloji kullanımı, sosyal medya kullanımı, siber zorbalık ve teknoloji bağımlılığı gibi konularda farkındalık oluşturarak; internet, ekran, teknoloji bağımlılığı gibi kişiye ve topluma zarar veren alışkanlıklarla, siber zorbalıkla ve her türlü siber suçlarla eylem daha oluşmadan mücadele edilmesi için farkındalık oluşturulması ve bilinçlendirilmesi hedefleyen faaliyetler bütünüdür. Hedeflenen kitle Okul öncesi, ilköğretim, ortaöğretim öğrenim grupları, Yetişkin / Ebeveynler, İnternet ve mobil kullanıcılar, Kurumsal yapı ve organizasyonlardır. SİBERAY programının hedefleri ise siber farkındalık ve bilinç sağlamak, teknoloji bağımlılığının zararla-

rını önlemek, siber zorbalıkla mücadele etmek, güvenli internet kullanımını sağlamak ve web, mobil ve sosyal medya mecraları ile hedef kitleye etkili ve hızlı ulaşmak olarak sayılabilir.

EGM Siber Daire Başkanlığı ve 81 il birimlerinde görev yapmakta olan SİBERAY görevlileri ile okullarda sunum ve seminerler yapılmakta, halkın yoğun olarak bulunduğu yerlerde (şehir merkezleri, stadyumlar, alışveriş merkezleri, fuar ve festival alanlarında) stantlar kurularak siber suçların gerçekleşmeden önlenmesi, maddi manevi zararın en aza indirgenmesi amacıyla vatandaşlara yönelik farkındalık ve bilinçlendirme faaliyetleri gerçekleştirilmektedir. Çeşitli konularda hazırlanan afiş, billboard ve broşür çalışmaları ve sosyal medya paylaşımları ile farkındalık faaliyetleri desteklenmektedir. 2020 yılında faaliyete geçirilen *SİBERAY Programı* ile ulusal ve uluslararası platformlarda, siber güvenlik, teknoloji kullanımı, sosyal medya kullanımı, siber zorbalık ve teknoloji bağımlılığı gibi konularda farkındalık oluşturarak; internet, ekran, teknoloji bağımlılığı gibi kişiye ve topluma zarar veren alışkanlıklarla, siber zorbalıkla ve her türlü siber suçlarla eylem daha oluşmadan mücadele edilmesi için farkındalık oluşturulması ve bilinçlendirilmesi hedeflenmektedir.

Sonuç

Bilişim teknolojileri sayesinde çok büyük hacimlerdeki bilgiye kısa bir sürede ulaşabilmenin konforunu yaşamaktayız. Bu konfor ise artık günlük hayatımızda bir zorunluluk halini almıştır. Vazgeçilmez bir parçamız halini alan bilişim sistemleri herhangi bir suçun işlenmesinde araç yahut amaç haline gelmişse bunun tespitine ilişkin yapılan çalışmaların bütünü olan Adli Bilişim çalışmaları da aynı oranda bir zorunluluk haline gelmiştir. Her geçen gün artış kaydeden bilişim suçları aracılığıyla maddi ve manevi kayıplar ortaya çıkmaktadır. Bu suçlara paralel olarak adaletin tecellisine hizmet edecek her bir kişi, kurum ya da kuruluşun iş birliğine olan ihtiyaç artmıştır.

Adli Bilişim, hukuki bir soruşturmanın yürütülmesi veya davanın nihayetlendirilmesinde dijital verilerin toplanması, analizi ve yorumlanması sürecidir. Bu bağlamda dijital verilerin kullanımı yoluyla suçluların tespit edilmesi, kanıtların toplanması ve suçlamaların desteklenmesi için günümüde vazgeçilmez bir alan haline gelmiştir. Adli Bilişim uzmanlığı ise, dijital delillerin toplanması, incelenmesi, analizi ve raporlandırılması teknik ve hukuki bilgi becerinin bir araya geldiği özel bir uzmanlık alanıdır. Bu nedenle etkili ve adil bir yargı sürecine yardımcı olacak uzmanların yanı sıra bilişim hukuku, bilişim suçları ile mücadele yöntemleri ve Adli Bilişim uygulamaları özel önemi haizdir.

Polis Akademisi Başkanlığı ile Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı ortaklığında gerçekleştirilen Adli Bilişim Çalıştayı da Adli Bilişim gibi dinamik ve

son derece önemli olan bir konuda uzmanları bir araya getirerek gerek polislik eğitimi gerekse kurumlar/birimler arası iş birliği açısından önemli bir adım atmıştır. Bu bağlamda bir günlük çalıştay kapsamında adli bilişim alanındaki konuların tamamının el alması mümkün olmamakla beraber, gerçekleştirilen üç oturumda katılımcılar tarafından uzmanlık alanları dahilinde sunulmuş olan çok değerli görüş ve fikirler bu raporda özetlenmiştir. Çalıştay neticesinde çatışmalı olabileceği ifade edilen ve altı önemle çizilen hususları özetlemek gerekirse;

- Adli Bilişimde süreçlerinde birtakım hukuki sorunlar ve çatışmalar ortaya çıkabilecektir. Bu sorunların giderilmesi için dijital verilerin toplanması, depolanması, analizi ve yorumlanması sırasında, verilerin adli delil olarak kabul edilebilmesi için uygun yöntemlerin kullanılması gerekmektedir. Ayrıca, özel hayatın korunması, gizlilik, veri güvenliği ve yasal prosedürler gibi diğer hukuki konular da dikkate alınmalıdır.
- Adli Bilişim sürecinin ilk adımı, dijital verilerin toplanmasıdır. Ancak, dijital verilerin toplanması sırasında, verilerin değiştirilmesi veya bozulması riski vardır. Bu nedenle, Adli Bilişim uzmanları, uygun araçlar ve yöntemler kullanarak dijital verileri güvenli bir şekilde toplamalıdır.
- Dijital verilerin analizi, Adli Bilişim sürecinin en önemli aşamasıdır. Ancak, dijital verilerin analizi sırasında, verilerin yorumlanması konusunda hukuki birçok sorun ortaya çıkabilir. Örneğin, bir mesajın ne anlama geldiği veya bir belgenin neyi gösterdiği konusunda farklı yorumlar yapılabilir. Bu nedenle, Adli Bilişim uzmanları, dijital verilerin yorumlanması sırasında hukuki standartları dikkate almalıdır.

- Dijital verilerin adli delil olarak kabul edilmesi, hukuki bir sorun olabilir. Adli delil olarak kullanılmak istenen dijital verilerin doğruluğu ve bütünlüğü hakkında şüpheler olabilir. Bu nedenle, Adli Bilişim uzmanları, dijital verilerin toplanması, analizi ve yorumlanması sırasında uygun yöntemleri kullanarak, dijital verilerin doğruluğunu ve bütünlüğünü sağlamalıdır.
- Özellikle kolluk olay yerine ilk ulaşan birim olduğundan ifade alma, olay yeri inceleme, arama, el koyma işlemlerinin delil zincirinin ilk halkasını oluşturması hukuka uygun delil elde edilmesi bakımından kolluğun eğitimini önemli bir noktaya taşımaktadır. Dijital deliller ve elde edilişleri konusunda uzmanlaşmış kolluk personeline olan ihtiyaç günün temel gerekliliklerinden biri haline gelmiştir.

Sonuç olarak, çalıştay kapsamında ele alınan adli bilişim konusunun güncel, sürekli ve hızla ilerleyen bir alan olması hasebiyle teorik araştırma ve uygulama bağlamında yeni tartışmalara da açık olduğu katılımcılar tarafından vurgulanmıştır. Emniyet teşkilatına amir ve memur yetiştiren ve yine lisansüstü düzeyde bilimsel araştırmalar yaparak bilgi üreten bir akademik kurum olarak Polis Akademisi'nin böylesine kritik önemi haiz ve dinamik bir alanda ortaya koyduğu katkının öneminin altı çizilmiş ve benzer çalışmaların devamı konusundaki temenniler iletilmiştir.

Konuşmacılar

- Prof. Dr. Yılmaz ÇOLAK (Polis Akademisi Başkanı)
- 2. Sınıf Em. Md. Seyit Ahmet DİKİCİ (Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkan Yardımcısı)
- Doç. Dr. Coşkun TAŞTAN (Polis Akademisi Adli Bilimler Enstitüsü Müdürü)
- Doç. Dr. Nevin GÖKSAL (Polis Akademisi Adli Bilimler Enstitüsü)
- Doç. Dr. Harun ARTUNER (Hacettepe Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü)
- Doç. Dr. Şengül DOĞAN (Fırat Üniversitesi, Teknoloji Fakültesi, Adli Bilişim Mühendisliği)
- Prof. Dr. Mustafa ALKAN (Gazi Üniversitesi, Bilişim Enstitüsü)
- Mühendis İsmail ERKEK (Bilgi Teknolojileri ve İletişim Kurumu, Ulusal Siber Olaylara Müdahale Merkezi (USOM))
- Mühendis Adnan KEÇE (Adalet Bakanlığı, Adli Tıp Kurumu Başkanı Adli Bilişim İhtisas Daire Başkanı)
- Emniyet Amiri Furkan YILMAZ (Emniyet Genel Müdürlüğü)
- Arş. Gör. Müberra ÖZTÜRK (Polis Akademisi Adli Bilimler Enstitüsü)
- Komiser Mehmet SEVİNÇ (EGM Siber Suçlarla Mücadele Daire Başkanlığı)
- Komiser Bilal USLU (EGM Siber Suçlarla Mücadele Daire Başkanlığı)
- Komiser Fatih DEMİR (EGM Siber Suçlarla Mücadele Daire Başkanlığı)
- Komiser Birol MEN (EGM Siber Suçlarla Mücadele Daire Başkanlığı)

- Doç. Dr. Ali Rıza TÖNGÜR (Polis Akademisi Adli Bilimler Enstitüsü)
- Prof. Dr. Olgun DEĞİRMENCİ (TOBB Ekonomi ve Teknoloji Üniversitesi, Hukuk Fakültesi)
- Cumhuriyet Savcısı Mahmut Kaan YÜKSEL (Ankara Cumhuriyet Başsavcılığı)
- Cumhuriyet Savcısı Adem CAN (Ankara Cumhuriyet Başsavcılığı)
- Tetkik Hakimi Faruk KARCI (Adalet Bakanlığı Ceza İşleri Genel Müdürlüğü)