SETSCI conference proceedings
SETSCI Conference Proceedings
9, 444-449, 2019

4th International Symposium on Innovative Approaches in Engineering and Natural Sciences
November 22-24, 2019, Samsun, Turkey

https://doi.org/10.36287/setsci.4.6.118
2687-5527/ © 2019 The Authors. Published by SETSCI

ISAS WINTER - 2019

Digital Evidences According to ISO/IEC 27035-2, ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042 and ISO/IEC 27043 Standards

Nursel Yalçın[1*] and Berker Kılıç[2+]

[1] Gazi University, Gazi Faculty of Educcation, Ankara/Türkiye
[2] Gazi University, Institution of Information Technologies Ankara/Türkiye
*Corresponding Author: nyalcin@gazi.edu.tr
+Speaker: berker.kilic@gmail.com
Sunum/Bildiri Türü: Sözlü/ Tam Metin

Abstract **–** Family of ISO/IEC 27K provides standards including processes from the preparation before the incident up to the closure of it, as well as warnings and general advices.
There are many types of investigation for digital evidences. For instance; device investigations such as desktop computers, laptops, servers, repositories, phones/mobile phones, investigations for live data (for example unstable data reviews) and DVRs, game consoles, controlling systems.
Standards, named as ISO/IEC 27035-2 Information technology - Security techniques - Information security incident management - Part 2: Guidelines to plan and prepare for incident response, ISO/IEC 27037 Information technology - Security techniques - Guidelines for identification, collection, acquisition, and preservation of digital evidence, ISO/IEC 27041 Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative method, ISO/IEC 27042 Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence ISO/IEC 27043 Information technology - Security techniques - Incident investigation principles and processes, are formulated by the operation of investigating digital evidences and rendered them applicable to the all kinds of digital evidences.
In this study, the working process beginning with organizing the expert report without the requisition of digital evidences and up to submitting it to the relevant forensic unit is examined and a generalizable model is suggested in terms of ISO/IEC 27035-2, ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042 ve ISO/IEC 27043 standards.
Keywords– *Computer Forensic, Digital Evidence, Security Techniques, Adequacy of Incident, ISO/IEC 27035-2, ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042, ISO/IEC 27043*

ISO/IEC 27035-2, ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042 ve ISO/IEC 27043 Standartlarına Göre Sayısal Kanıtlar

Özet **–** Sayısal kanıtların incelenmesinde ISO/IEC 27K ailesi, uyarılar ve genel tavsiyelerin yanı sıra, olay öncesi hazırlıktan olayın kapanışına kadar olan süreçleri içerir standartlar sağlamaktadır.
Sayısal kanıtlar için birçok inceleme türü vardır. Örneğin; masaüstü bilgisayarları, dizüstü bilgisayarları, sunucular, veri havuzları, el/cep telefonu gibi cihaz incelemeleri, canlı veri araştırmaları (örneğin ağ ve istikrarsız veri incelemeleri) ve DVR ler, oyun konsolları, kontrol sistemleri.
ISO/IEC 27035-2 Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği olay yönetimi - Bölüm 2: Olay tepkisi için planlama ve hazırlık ilkeleri, ISO/IEC 27037 Bilgi teknolojileri - Güvenlik teknikleri - Sayısal kanıtların belirlenmesi, edinimi, bir araya getirilmesi ve korunması hakkında kılavuz, ISO/IEC 27041 Bilgi teknolojisi - Güvenlik teknikleri - İhlal olayı inceleme yönteminin uygunluğu ve yeterliliğini sağlamak için kılavuz, ISO/IEC 27042 Bilgi teknolojisi - Güvenlik teknikleri - Sayısal kanıtların analizi ve yorumlanması için tavsiyeler, ISO/IEC 27043 Bilgi teknolojisi - Güvenlik teknikleri - İhlal olayı inceleme ilkeleri ve süreçler isimli standartlar, sayısal kanıtların inceleme işlemi formülleştirilmiş ve her türlü sayısal kanıta uygulanabilir hale getirilmiştir.
Bu çalışmada ISO/IEC 27035-2, ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042 ve ISO/IEC 27043 standartları açısıdan sayısal kanıtların el koymadan başlanarak bilirkişi raporunun düzenlenmesi ve ilgili adli birime teslimine kadar geçen iş süreci incelenmiş ve genellenebilir bir model önerilmiştir.
Anahtar Kelimeler- *Adli Bilişim, Sayısal Kanıt, Güvenlik Teknikleri, İhlal Olayı, ISO/IEC 27035-2, ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042, ISO/IEC 27043*

I. GIRIŞ

Günümüzün dijitalleşen dünyasında, suçlular da avantaj ve dezavantaj sağlamaktadırlar. Suça ilişkin deliller, çeşitli elektronik ortamlarda bulunabilmekte ve suça konu olayın aydınlatılabilmesi, şüphelinin suçlu veya suçsuz olduğunun belirlenebilmesinde önemli rol oynamaktadır.

Pek çok durumda, suç konusu doğrudan elektronik sistemlerle ilişkili de olabilmektedir.

Ülkemizde de özellikle bilgi güvenliği ve bilişim suçları alanında gelişmeler son yıllarda hız kazanmıştır. 5651 Sayılı

Internet Ortaminda Yapilan Yayinlarin Düzenlenmesi ve Bu Yayinlar Yoluyla Işlenen Suçlarla Mücadele Edilmesi Hakkinda Kanun, 6698 Sayılı Kişisel Verilerin Korunması Kanunu gibi temel düzenlemeler kamu eli ile özel sektöre bir takım düzenlemeler getirmekle birlikte, 11' nci Kalkınma Planı' nda Siber Güvenlik konusuna geniş bir yer verilmiş olması ayrıca Cumhurbaşkanlığı tarafından yayınlanan 2019/12 Sayılı Bilgi ve İletişim Güvenliği konulu genelge ve Genelge' de ifade bulan Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı aracılığı ile yayınlanması beklenen Bilgi ve İletişim Güvenliği Rehberi ile bilgi güvenliği alanındaki gelişmelerin hızlanarak devam etmesi beklenmektedir [1-4].

Ancak bilginin korunmasına yönelik farklı açılardan çeşitli düzenlemeler yapılmaktayken, elektronik delillerin temini ve incelenmesi süreçleri ile ilgili düzenlemelerin yeterince hızlı ilerlemediği görülmektedir.

Bu çalışmada, elektronik delillerin temininden incelenmesi sürecine kadar gerçekleştirlen işlemler, literatür taraması ile incelenmiş, ISO standartları açısından genel bir değerlendirmeye tabi tutulmuştur.

II. MATERIALS AND METHOD

Elektronik delillerin soruşturma ve kovuşturma makamlarınca kullanılması süreci, tam bir standardizasyona sahip değildir. Fakat, ISO standartları bu standardizasyonu sağlama kapasitesine sahiptir.

A. ISO Standartları Ne Sunuyor?

ISI/IEC 27041 ve 27043 standartları, elektronik delillerin temin planlanmasından, delillerin raporlanması ve vakanın kapatılmasına kadar tüm sürecin kontrolü ve yeterliliği için tavsiyeler sunmaktadır. Sürecin alt adımları, 27035-2, 27037 ve 27042 standartlarında kılavuz ve tavsiyeler sunmaktadır. Elektronik delillerin incelenmesine ilişkin ISO/IEC standartları tam isimleri ile şunlardır [5-9]:

- 27035-2: Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği olay yönetimi - Bölüm 2: Olay tepkisi için planlama ve hazırlık ilkeleri.
- 27037: Bilgi teknolojisi - Güvenlik teknikleri - Sayısal kanıtlarin belirlenmesi, edinimi, bir araya getirilmesi ve korunması hakkında kılavuz.
- 27041: Bilgi teknolojisi - Güvenlik teknikleri - İhlal olayı inceleme yönteminin uygunluğu ve yeterliliğini sağlamak için kılavuz.
- 27042: Bilgi teknolojisi - Güvenlik teknikleri - Sayısal kanıtların analizi ve yorumlanması için tavsiyeler.
- 27043: Bilgi teknolojisi - Güvenlik teknikleri - İhlal olayı inceleme ilkeleri ve süreçleri.

ISO/IEC standartlarına göre elektronik delillerin temin ve inceleme süreci Şekil 1' de görülmektedir.

Şekil 1. Elektronik delillerin incelenmesinde ilgili ISO/IEC Standartları

Bir başka deyişle ISO/IEC 27043 standartdı ihlal olayı inceleme ilk ve süreçleri için bir referansken, ISO/IEC 27041 bu inceleme sürecinde kullanılan yöntemlerin uygunluğu ve yeterliliğini sağlamak üzere bir kılavuzdur.

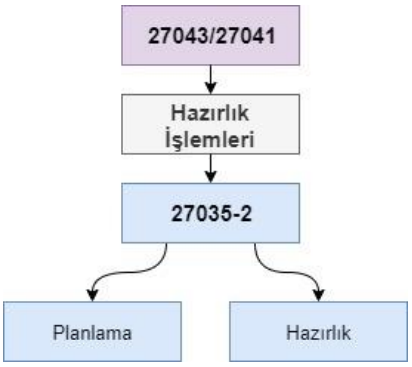
İhlal olayı inceleme sürecinde ISO/IEC 27035-2 standardı vakaya müdahale öncesi planlama ve hazırlık ilkeleri, ISO/IEC 27037 standardı olay yerinde sayısal kanıtların belirlenmesi, edinimi, bir araya getirilmesi ve korunması, ISO/IEC 27041 standardı ise sayısal kanıtların yorumlanması, raporlaması ve vakanın sonlandırılması kılavuz ve tavsiyeler içermektedir.

B. ISO/IEC 27043 Standardı

Bu standart bir vaka ile ilişkili, ihlal olayı için inceleme ilkeleri ve süreçlerini 4 ana süreç olarak tanımlamaktadır:

1. Hazırlık İşlemleri
2. Başlatma İşlemleri
3. Edinim İşlemleri
4. İnceleme İşlemleri

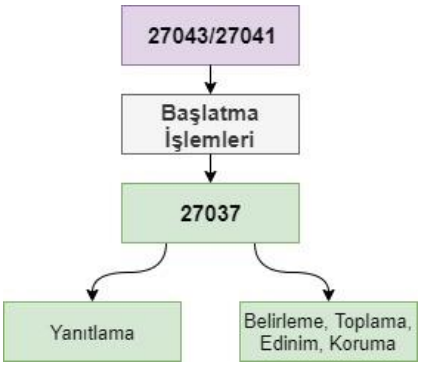
Hazırlık İşlemleri kapsamında, ISO/IEC 27035-2 standardında tanımlanan planlama ve hazırlık işlemleri, inceleme zaman ve maliyetinin en aza indirilmesini ve buna parallel olarak elde edilen bulguların da kullanılabilirliğini en üst seviyeye taşımayı amaçlamaktadır [5]. ISO/IEC 27035-2 standardında hazırlık işlemleri Şekil 2.' de görülmektedir.



Şekil 2. Hazırlık İşlemleri

Başlatma İşlemleri kapsamında, ISO/IEC 27037 standardında tanımlanan yanıtlama, belirleme, toplama, edinim ve koruma işlemleri, elektronik delillere ilk müdahaleden edinilen delillerin korunmasına kadar süreç için

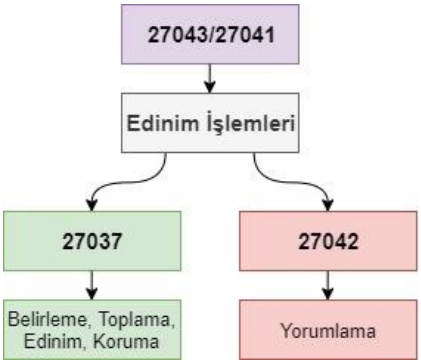
kılavuz ve tavsiyeler içermektedir [6]. ISO/IEC 27037 standardında başlatma işlemleri Şekil 3.' de görülmektedir.



Şekil 3. Başlatma İşlemleri

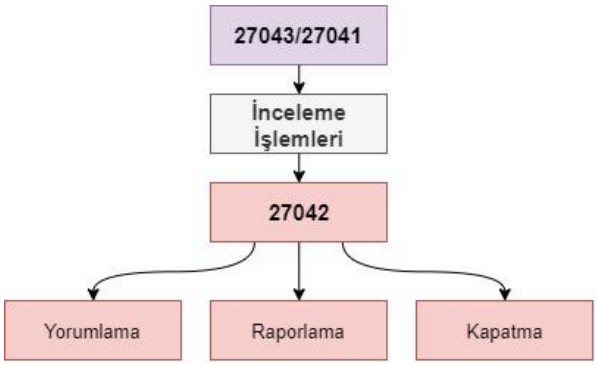
Edinim İşlemleri kapsamında, ISO/IEC 27037 standardında edinim işlemleri ile ISO/IEC 27042 standardında delillerin yorumlanması işlemleri için kılavuz ve tavsiyeler içermektedir. ISO/IEC 27037 standardında yer alan edinim işlemi, elektronik delilin türüne göre inceleme işlemlerinde de farklılıklar içereceği için ISO/IEC 27042 standardının yorumlama işlemleri ile birlikte değerlendirilmektedir [6, 8]. ISO/IEC 27037 ve ISO/IEC 27042 standardında edinim işlemleri Şekil 4.' de görülmektedir.

Örneği, bir cep telefonunun edinimi ve incelenmesi ile bir güvenlik kamera sisteminden alınacak kayıtların edinimi ve incelenmesi birlikte değerlendirilmesi gerekmektedir.



Şekil 4. Edinim İşlemleri

İnceleme İşlemleri kapsamında, ISO/IEC 27042 standardında tanımlanan yorumlama, raporlama ve kapatma, incelemeye konu olan vakanın aydınlatılmasında, elde edilen elektronik delillerin analizi ile elde edilen bulguların doğru şekilde yorumlanması ve raporlanması ile ilgililerine sunulup inceleme sürecinin sonlandırılması kapsamaktadır [9]. ISO/IEC 27042 standardında hazırlık işlemleri Şekil 5.' de görülmektedir.



Şekil 5. İnceleme İşlemleri

C. ISO/IEC 27041 Standardı

Bu standart diğer standarların tamamlayıcısı olarak ihlal olayı sürecinin uygunluğunu ve yeterliliğini sağlamayı amaçlayan bir kılavuz niteliğindedir.

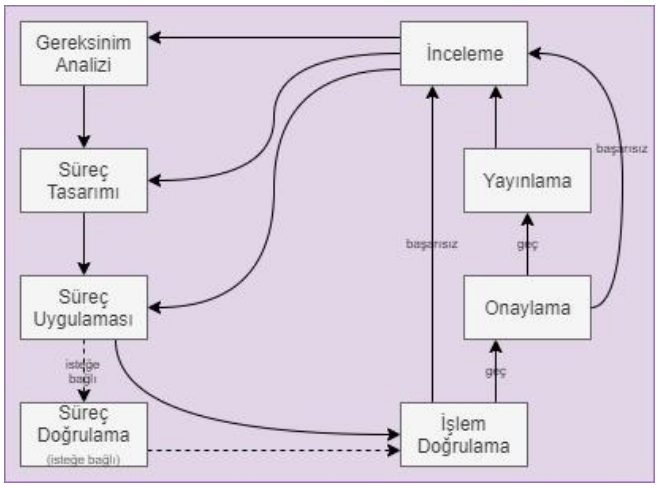
Her ne kadar diğer standartlar, sürecin uygulanması için yeterli görünse de, uygulamada her bir standardın farklı yargı ve kolluk birimlerince uygulanıyor olması, uygulayıcı birbirine denk birimlerin varlığı, aynı birim içerisinde dahi olsa uygulayıcı personelin farklılaşabilmesi gibi nedenlerden dolayı, sürecin bütünsel olarak yeterliliğinin ve elde edilen sonuçların güvenilirliğinin de sağlanabilmesi önem arz etmektedir.

Diğer bir açıdan bakıldığında, uygulamada benzer vakalar karşısında farklı uygulamaların gerçekleştirilmesi, ihlal olayının ilişkili olduğu soruşturma veya kovuşturma süreçlerinde, sanıkların adil yargılanması açısından da sorgulanabilir bir boşluk oluşmasına neden olabilmektedir.

İhlal olayının incelenmesi sürecinde tipik olarak aşağıdaki gibi uygun bir süreç kontrol planlanması gerekmektedir.

- Gereksinim analizi
- Süreç tasarımı
- Süreç uygulaması
- Süreç doğrulama (isteğe bağlı ve zorunlu olmayan)
- İşlem doğrulama
- Onaylama
- Yayınlama
- İnceleme

Şekil 6.' da ihlal olayı incelem süreci uygunluk ve yeterliliğini sağlamak üzere ISO/IEC 27041 Standardına kontrol planı görülmektedir.



Şekil 6. ISO/IEC 27041 İhlal olayı uygunluk ve yeterlilik planı

D. ISO/IEC 27035-2

ISO/IEC 27035-2 standardında ihlal olayı inceleme yöntemlerinin uygunluğu planlama ve hazırlık olmak üzere iki aşamadan oluşmaktadır.

Bu aşamalar, yetkili mercilerin kurumsal taahhütü ile birlikte, olay müdahale ekibinin kuruluşu, iç ve dış kuruluşlarla ilişkiler ve bağlantılar, teknik ve operasyonel destek, bilgi güvenliği eğitimleri ve olay müdahale testlerini kapsamaktadır. Ayrıca, olay müdahalelerinden edinilen deneyimlerin iyileştirme amaçlı kullanılmak üzere kayıt altına alınması da aşamaların bir parçasıdır [5].

Uygulamada bu konu, ülkemizde yargı mercilerinin kararı ve kolluk kuvvetleri marifeti ile işletilmektedir. Yargı merciinin bir soruşturma veya kovuşturma süreci içerisinde elektronik ortamlardan delil elde edilebilir olduğuna karar vermesi yahut suçun niteliği itibariyle delillerin elektronik ortamlarda bulunduğunun belli olması durumunda, ilgili kanunların verdiği yetki ile kolluk kuvvetlerinden şüpheli veya sanığa ait elektronik cihazların incelenmesini talep etmektedir.

Ancak, kolluk tarafından elektronik cihazların bulunduğu ortamda cihazlar üzerinde inceleme ve/veya imaj alma işlemlerinden ziyade cihazlara doğrudan el koyma ve incelenmek üzere ilgili birimlere sevki sağlanmaktadır.

Her ne kadar bu husus, yargı merciilerince gerekli ise el koyma tedbirinin uygulanmasının rutin hale getirilmesi olarak değerlendirilebilir olsa da, kolluk kuvvetleri kapsamında yeterli teknik eleman olmaması seçimlik olan el koyma tedbirinin kolaylık sağladığı için tercih edilmesine neden olmaktadır.

Bu nokta literatürde de işlenmiş, delillerin toplanmasında, delil bütünlüğünü korumak amacıyla dikkat edilmesi gereken teknik hususların yanı sıra, ceza muhakemesi hukuku bakımından korunan kurallara uygun hareket edilmesi de büyük önem arzettiği defaatle vurgulanmıştır [10].

Şüphelinin veya sanığın kullandığı bilişim sistemlerinde arama yapılması, sistemdeki verilerin kopyasının çıkarılması ve kayıtların çözümünün yapılarak metin haline getirilmesini içermektedir. Yani kural olan arama tedbiridir; şüphelinin kullandığı bilişim sistemi olduğu yerde bırakılacak ve kopyalama işlemi sistemin bulunduğu yerde yapılacaktır. Ayrıca kolluk güçleri sistemin ya da veri taşıma aracının aslını almayacaktır [11].

E. ISO/IEC 27037

Literatürde delillerin elde edilmesinde kullanılan yöntemlerin bilim tarafından kabul edilebilir standartlara sahip olması gerektiği ifade edilmektedir [12].

Olay yerinde elektronik ortamlardan delillerin elde edilmesi süreci ISO/IEC 27037 standardında kılavuz olarak sunulmaktadır.

Standardın üzerinde durduğu ve tanımını yaptığı iki göre, sayısal kanıt ilk müdahale uzmanı ve sayısal kanıt uzmanı olarak tanımlanmıştır [6].

Bu görev tanımı vurgusu, ISO/IEC 27035-2 standardı ile ilgili olarak açıklanan ve literatürde de kendisine en sık yer bulan yargı ve kolluk birimlerince yapılan arama ve el koyma işlemlerinde, elektronik cihazların yerinde imajlarının (kopyalarının) alınmasındansa el konularak ilgili birimlere götürülmesi konusuna açıklık getirmektedir. Diğer taraftan bu ayrım, ISO/IEC 27042 standardında da değinilen raporlama süreci ile edinim sürecinin birbirinden ayrı ve aynı kişi tarafından gerçekleştirme zorunluluğu olmayan süreçler olduğunu ortaya koymaktadır.

İlgili kanunlarda da belirtilen öncelikli olanın elektronik cihazlara el koymak değil, olay yerinde imajlarının (kopyalarının) alınması gerektiğidir.

Standart ayrıca, elektronik delillerin elde edilmesinde kullanılan yöntemlerin bilimsel olarak kabul edilebilir olması konusunda, denetlenebilirlik, tekrarlanabilirlik, tekrar üretilebilirlik ve savunulabilirlik ilkelerini vurgulamaktadır [6].

Yargı merciilerinden gelen talep üzerine standart bu talebin yanıtlanmasını, yani elektronik delillerin edinimini gerçekleştirecek personelin belirlenmesinde yetkin personelin seçimini öngörmektedir.

Sayısal kanıtın belirlenmesi, toplanması, edinimi ve korunmasının sayısal kanıt ilk müdahale uzmanı kontrolünde gerçekleştirilecek ana bileşenleri şunlardır [6]:

Kanıt Koruma Zinciri: Kanıt koruma zinciri kaydı, sayısal veri veya diğer biçimlerden oluşan (kağıda alınan notlar gibi), sayısal kanıtın incelemesinden kimin sorumlu olduğunu kayıt altına alan ve kanıt korunma zincirini detaylandıran belge veya ilgili doküman serisidir. Kanıt koruma zinciri kaydı tutmanın amacı, belirtilen herhangi bir zamanda sayısal kanıta erişimin ve hareketlerinin belirlenmesine imkan tanımaktır.

Olay Yerindeki Önlemler: olay mahalline ulaşır ulaşmaz olası sayısal kanıtın yerini güvenceye almak ve korumak için eylemler gerçekleştirmelidir. Süreçte yer alan personelin güvenliği hayati önem taşıdığından, süreci başlatmadan önce personel güvenliği konusunda risk değerlendirmesi yapılmalıdır. Olası sayısal kanıtı bir araya getirirken veya edinirken, özel cihazların kullanımında dikkatli olunmalıdır.

Roller ve Sorumluluklar: Hareket etmeden önce riskleri hesaplamamak, bir araya getirme veya edinimde kullanılan teknolojiden dolayı olası sayısal kanıtın bir kısmının veya tamamının kaybolmasına neden olabilir.

Yeterlilik: Sayısal kanıt uzmanı veya uzmanları sayısal kanıt ilk müdahale uzmanı koordinesinde çalışmalı gerekli ise özel uzmanlık alanı gereken durumlara ilgili sayısal kanıt uzmanları müdahale etmelidir. Standart sayısal kanıt ilk müdahale uzmanı ve sayısal kanıt uzmanı için yeterlilik tabloları sunmaktadır.

Uygun Özen Gösterilmesi: Sürecin tamamında, delillerin kısmen veya tamamen kaybolmasına neden olabilecek riskli eylemlere karşı gereken özen gösterilmelidir.

Belgeleme: Müdahale edilen her elektronik cihaz ile ilgili gerekli belgeleme işlemleri yapılmalıdır.

Kısa Bilgilendirme: Uzmanlar, ilgili yasalar çerçevesinde, kendilerindne beklenen görevi anlamış olmalı ve gerekiyorsa sayısal kanıtlara özel ilgili merciiler için bilgilendirme yapmalı, olay yeri görev paylaşımı yapmalı ve gerçek zamanlı müdahale gereken durumları göz ardı etmemelidir.

Bir Araya Getirme ve Edinimde Önceliklendirme: Delil içerebilecek elektronik cihazların geçiciliğine ve/veya ilişkili/olası kanıtsal değerine göre önceliklendirmek gerekebilir. İlişkili/olası kanıtsal değeri yüksek olan ögeler, soruşturulan olayla doğrudan ilişkili veri içerme ihtimali yüksek olan ögelerdir.

Olası Sayısal Kanıtın Korunması: Tüm toplanan cihazlar ve edinilen olası sayısal kanıtlar, kayıptan, kurcalamadan ve bozulmadan mümkün olduğunca korunmalıdır. Koruma sürecindeki en önemli faaliyet olası sayısal kanıtın bütünlüğünü, özgünlüğünü ve kanıt koruma zincirini muhafaza etmektir. Toplanan sayısal cihaz(lar) ve edinilen olası sayısal kanıtlar, erişim kontrol sistemi, gözetleme sistemleri veya saldırı tespit sistemleri gibi fiziksel güvenlik kontrolleri olan kanıt koruma tesisinde veya sayısal kanıt koruması için başka kontrollü bir ortamda korunmalıdır.

F. ISO/IEC 27042

ISO/IEC 27042 standardı, edinilen sayısal kanıtların analizi ve yorumlanması için tavsiye niteliğindedir. Ancak bu tavsiyelerin genişletilerek uygulanması ve vakaya özel inceleme süreçlerinin geliştirilmesi, benzer vakaların incelenmesinde, benzer işlemlerin yapılmasında da standart oluşturabilmeyi sağlayacağı için öneri olmaktan daha önemli bir niteliğe sahiptir.

Özellikle edinilen sayısal kanıtların, farklı kolluk birimlerinde görevli personel veya bilirkişiler tarafından incelenmesinde, aynı nitelikteki sayısal kanıtlar için birbirine taban tabana zıt raporların hazırlanması durumu ile karşılaşılabilmektedir.

Yahut, raporlamanın yapıldığı yargı birimi açısından teknik olarak değerlendirilmesi mükün olmayan bulguların, doğru şekilde yorumlanamaması durumu ile de sık sık karşılaşılabilmektedir.

Uygulamada karşılaşılan bir diğer sorun ise, aslen soruşturulan veya kovuşturulan konu ile doğrudan bir bulgu niteliği taşımamasına ragmen, incelemecinin yanlış yorumu yahut yalnızca temel kelime benzerliklerinin dahi tespit olarak yargı merccine sunulması, yargı merciinin bu tespiti yanlış değerlendirebilmesine ve sanıkların adil yargılanmasının engellenmesine neden olabilecek sonuçlar ortaya çıkabilmektedir.

ISO/IEC 27042 standardı tipik bir inceleme sürecini açıklarken, potansiyel delil kaynaklarının incelenerek raporlanmasına kadar geçen süreci ele almaktadır. Bu süreç içerisinde inceleme kendi içerisinde sorgulama ve yorumlama alt basamaklarına ayrılmakta, her bir yorumlama için gerekli analiz ve her bir analiz için de alt süreçlerin ele alınması gerektiğini tavsiye eden bir model önermektedir.

Standart süreç içerisinde aşağıdaki başlıkları ele almaktadır [8]:

Soruşturma: Bir soruşturmanın birincil amacı, bir olay hakkındaki anlayışı geliştirmektir.

Analiz: Anlamlı dijital delillerin birçoğu, kendi ana formlarında gizli kaldığı için analiz gereklidir (ör. silinmiş dosyalar, disk boş alanları). İşlemlerin tamamı yetkin personel tarafından gerçekleştirilmeli ve bilgi için izlenebilir ve savunulabilir bir kanıt oluşturmak için titizlikle belgelendirilmelidir.

Analitik Modeller: Analizin türü çalışma kapsamı dışında olmakla birlikte temelde 2 tür analizden bahsedebilmek mümkündür (Statik Analiz, Canlı Analiz).

Yorumlama: Yorumlamanın amacı, verilerin değerlendirmesini yaparak ve durumu bağlamında analiz ederek dijital kanıtlardan anlam çıkarmaktır. Yorumlama, inceleme ve analiz süreçleriyle yorumlama, gerçekleri bulmayı ve bazı durumlarda gerçekleri fikirlerle güçlendirmeyi içerir. Yorumlama sonuçlarına bağlı olarak analizin tekrarlanmasını veya dijital kanıtların toplanmasını gerektirebilir.

Raporlama: Soruşturmaya başlamadan önce, nihai raporun niteliği ve amacı tespit edilmelidir. Bu, soruşturma sürecine rehberlik etmek için kullanılmalıdır ve cevaplanması gereken bir dizi soru, raporun muhtemel okuyucularının bir göstergesi mevcut olabilir.

Yetenek: Bir olayın soruşturmasında yer alan tüm adımlar, kendilerine verilen görevleri tamamlamada açıkça yetkin kişiler tarafından gerçekleştirilmelidir. Minimal gözetim ile gerçekleştirebilmek için kullanacakları araç, yöntem ve teknikleri yeterince bilmeli ve bu konuda deneyimli olmalı ve kendi yeteneklerinin sınırlarını tanıyabilmelidir. Bir araştırmacının kendi sınırlamalarını tanıması durumunda, yapılması gereken işlem için mesele daha kıdemli veya yetkili bir kişiye yönlendirilmelidir.

Yeterlik: Potansiyel bir dijital kanıt örneği verildiğinde, analizi benzer bir analiz kullanarak başka bir yetkili araştırmacı ekip tarafından üretilenlere eşdeğer sonuçlar ürettiğinde, yetkin bir araştırmacı ekip yeterli sayılabilir.

III. SONUÇ

ISO/IEC standartları, bir ihlal olayının başlatılması aşamasından sonlandırılmasına kadar süreç için tavsiyeler ve kılavuzlar yardımı ile süreç yönetimini ve çıktıların güvenilirliğini sağlama niteliğine sahiptir.

Uygulamadaki farklılıklar için şüpheli ve sanıkların aleyhine sonuçlanabilecek el koyma ve yorumlama hatalarını engelleyebilir niteliktedir.

IV. ÖNERILER

Uygulamada her ne kadar ilgili kanunlar yargı ve kolluk merciileri tarafından azami suretle uygulanmaya çalışılıyor olsa da, özellikle arama ve el koyma aşaması ile elektronik delillerin yorumlanması ve raporlanması noktalarında şüpheli ve sanıkların haksız yere aleyhine ortaya çıkabilecek sonuçlar ortaya çıkabilmektedir. Standartların bütününün tüm yargı ve kolluk birimlerinde eş zamanlı olarak uygulamaya geçirilmesi mümkün olmasa da merkezi olarak en aza indirgenebilmesi için, ilgili kanunlar paralelinde uygulamanın da standartlara uygun hale getirilmesi mümkündür.

Özellikle 27035-2 standardı, ilgili kanun hükümleri ile birlikte uygulanarak, yargı ve kolluk birimlerinin işlerini

kolaylaştıracak bir niteliktedir. Ancak, yargı ve kolluk birimlerin elektronik delillerin türleri ve gerçekleştirilmesi gereken inceleme yöntemleri konularında bilgilendirilmeleri gerekmektedir.

ISO/IEC 27037 standardı açısından, olay yerinde delillere müdahale eden kolluk personelinin, inceleme ve raporlama personelinden farklı olması mümkün olmakla, müdahale personelinin tam detaylı bir yetkinliğe sahip olması gerekmemekte, ancak el koyma tedbirinin ikincil uygulama olabilmesi için bir takım temel yeterliliklere sahip olması gerekmektedir.

ISO/IEC 27042 standardı açısından, özellikle elektronik delillerin raporlanması sürecinde, incelenen olayla ilişkili bir şekilde, yargı merciilerine yanlış yoruma neden olmayacak derecede kesin tespitler içeren raporlar düzenleyebilmeleri için vaka örnekleri için standart inceleme süreçleri belirlenmeli ve hem kolluk birimlerinde görevli uzmanlar hem de bilirkişiler tarafından bu süreçlerde belirtilen inceleme tekniklerine ve rapor standartlarına uymaları sağlanmalıdır.

KAYNAKLAR

[1] Resmi Gazete, (04/05/2007), 5651 Sayılı Internet Ortaminda Yapilan Yayinlarin Düzenlenmesi ve Bu Yayinlar Yoluyla Işlenen Suçlarla Mücadele Edilmesi Hakkinda Kanun, (Sayı: 26530).

[2] Resmi Gazete, (07/04/2016), 6698 Sayılı Internet Ortaminda Yapilan Yayinlarin Düzenlenmesi ve Bu Yayinlar Yoluyla Işlenen Suçlarla Mücadele Edilmesi Hakkinda Kanun, (Sayı: 29677).

[3] Resmi Gazete, (06/07/2019), 2019/12 Sayılı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi, (Sayı: 30823).

[4] Resmi Gazete, (23/07/2019), On Birinci Kalkinma Planinin (2019-2023) Onaylandiğina Ilişkin Karar, (30840 Mükerrer).

[5] International Organization for Standardization and the International Electrotechnical Commission, (2016), TS ISO/IEC 27035-2 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Olay Yönetimi - Bölüm 2: Olay Tepkisi İçin Planlama ve Hazırlık İlkeleri.

[6] International Organization for Standardization and the International Electrotechnical Commission, (2016), TS ISO/IEC 27037 Bilgi Teknolojisi - Güvenlik Teknikleri - Sayısal Kanıtların Belirlenmesi, Edinimi, Bir Araya Getirilmesi ve Korunması Hakkında Kılavuz, Ankara.

[7] International Organization for Standardization and the International Electrotechnical Commission, (2016), TS ISO/IEC 27041 Bilgi Teknolojisi - Güvenlik Teknikleri - İhlal Olayı İnceleme Yönteminin Uygunluğu ve Yeterliliğini Sağlamak İçin Kılavuz, Ankara.

[8] International Organization for Standardization and the International Electrotechnical Commission, (2016), TS ISO/IEC 27042 Bilgi Teknolojisi - Güvenlik Teknikleri - Sayısal Kanıtların Analizi ve Yorumlanması İçin Tavsiyeler, Ankara.

[9] International Organization for Standardization and the International Electrotechnical Commission, (2016), TS ISO/IEC 27043 Bilgi Teknolojisi - Güvenlik Teknikleri - İhlal Olayı İnceleme İlkeleri ve Süreçleri, Ankara.

[10] Özen, M. and Özocak G., (2015), Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M.134), Ankara Barosu Dergisi, s41-77.

[11] Dülger M.V., (2015), Bilişim Sistemleri Üzerinde Arama, Kopyalama ve El Koyma Tedbiri, Yayınlanmamış makale.

[12] Sarsıkoğlu, Ş., (2015), Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı, Türkiye Adalet Akademisi Dergisi, s507-534.