TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

MOBİL ADLİ BİLİŞİMİNİN ÖNEMİ BAĞLAMINDA HUKUKİ SÜREÇ VE DELİL ZİNCİRİ KAVRAMI İLE YENİ NESİL MOBİL CİHAZLARIN İNCELENMESİNDE KARŞILAŞILAN GÜNCEL ZORLUKLARIN DEĞERLENDİRİLMESİ

Hamza Aytaç DOĞANAY

DİSİPLİNLERARASI ADLİ BİLİMLER ANA BİLİM DALI
ADLİ BİLİŞİM
YÜKSEK LİSANS TEZİ

DANIŞMAN
Prof. Dr. Hakkı Gökhan İLK

ANKARA
2019

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

MOBİL ADLİ BİLİŞİMİNİN ÖNEMİ BAĞLAMINDA HUKUKİ SÜREÇ VE DELİL ZİNCİRİ KAVRAMI İLE YENİ NESİL MOBİL CİHAZLARIN İNCELENMESİNDE KARŞILAŞILAN GÜNCEL ZORLUKLARIN DEĞERLENDİRİLMESİ

Hamza Aytaç DOĞANAY

DİSİPLİNLERARASI ADLİ BİLİMLER ANA BİLİM DALI
ADLİ BİLİŞİM
YÜKSEK LİSANS TEZİ

DANIŞMAN
Prof. Dr. Hakkı Gökhan İLK

ANKARA
2019

ETİK BEYAN

Ankara Üniversitesi

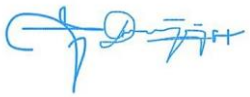
Sağlık Bilimleri Enstitüsü Müdürlüğü'ne

Yüksek Lisans tezi olarak hazırlayıp sunduğum "Mobil Adli Bilişiminin Önemi Bağlamında Hukuki Süreç ve Delil Zinciri Kavramı ile Yeni Nesil Mobil Cihazların İncelenmesinde Karşılaşılan Güncel Zorlukların Değerlendirilmesi" başlıklı tez; bilimsel ahlak ve değerlere uygun olarak tarafımdan yazılmıştır. Tezimin fikir/hipotezi tümüyle tez danışmanım ve bana aittir. Tezde yer alan araştırma tarafımdan yapılmış olup, tüm cümleler, yorumlar bana aittir.

Yukarıda belirtilen hususların doğruluğunu beyan ederim.

Öğrencinin Adı Soyadı: Hamza Aytaç DOĞANAY

Tarih: 10/06/2019

İmza: 

KABUL VE ONAY

Ankara Üniversitesi Sağlık Bilimleri Enstitüsü
Disiplinlerarası Adli Bilimler Anabilim Dalı
Adli Bilişim İkinci Öğretim Tezli Yüksek Lisans Programında

Hamza Aytaç DOĞANAY tarafından hazırlanan

"Mobil Adli Bilişimin Önemi Bağlamında Hukuki Süreç ve Delil Zinciri Kavramı ile Yeni Nesil Mobil Cihazların İncelenmesinde Karşılaşılan Güncel Zorlukların Değerlendirilmesi"

adlı tez çalışması

aşağıdaki jüri tarafından **YÜKSEK LİSANS TEZİ** olarak

OY BİRLİĞİ ile kabul edilmiştir.

10.06.2019

Prof.Dr. Hakkı Gökhan İLK
Ankara Ü. Mühendislik Fakültesi
Jüri Başkanı

Prof.Dr.Refik SAMET
Ankara Ü. Mühendislik Fakültesi
Üye

Dr.Öğr.Üyesi Hüseyin ÇAKIR
Gazi Ü. Gazi Eğitim Fakültesi
Üye

Tez hakkında alınan jüri kararı, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü Yönetim Kurulu tarafından onaylanmıştır.

Prof.Dr. Mehmet AKAN
Sağlık Bilimleri Enstitüsü Müdürü

İÇİNDEKİLER

Etik Beyan ii

Kabul ve Onay iii

İçindekiler iv

Önsöz vii

Simgeler ve Kısaltmalar viii

Şekiller xi

Çizelgeler xii

1. GİRİŞ 1

2. GEREÇ VE YÖNTEM 6

2.1. Kullanılan Malzeme, Cihaz ve Yazılımlar 6

2.2. Kullanılan Diğer Gereçler 6

3. BULGULAR 7

3.1. Adli Bilişimin Tanımı ve Kapsamı 7

3.2. Adli Bilişimin Safhaları 11

3.2.1. Adli Talimatın Alınması 11

3.2.1.1. CMK 134. Maddesinin Birinci Fıkrasının Değerlendirilmesi 15

3.2.1.2.Bilgisayar, Bilgisayar Programları, Bilgisayar Kütükleri Kayıtların Çözülerek Metin Haline Getirilmesi İbarelerinin Değerlendirilmesi 16

3.2.1.3. Dijital Veride Arama ve Rızaen Arama 17

3.2.1.4. CMK 134. Maddesinin İkinci Fıkrasının Değerlendirilmesi 18

3.2.1.5. CMK 134. Maddesinin Üçüncü Fıkrasının Değerlendirilmesi 20

3.2.1.6. CMK 134. Maddesinin Dördüncü Fıkrasının Değerlendirilmesi 21

3.2.1.7. CMK 134. Maddesinin Beşinci Fıkrasının Değerlendirilmesi 22

3.2.2. Bilişim Sisteminin Tespiti 23

3.2.3. Bulgunun Muhafaza Altına Alınması 24

3.2.4. İnceleme ve Analiz 26
3.2.5. Raporlama ve Adli Makamlara Sunum 28
3.3. Delil Zinciri 33
3.3.1. Laboratuvar Akreditasyonları Açısından Delil Zinciri ve Türkiye'deki Laboratuvarların Değerlendirilmesi 36
3.3.2. Mobil Cihaz Adli Bilişimi İçin Olay Yeri ve Laboratuvar Örnek İş Akış Görselleri 38
3.4. Mobil Cihaz Adli Bilişiminim Tanımı ve Önemi 41
3.5. İnternetin Kullanımı 43
3.5.1. Tarihçe 43
3.5.1.1. Dünyada İnternetin Tarihi 43
3.5.1.2. Türkiye'de İnternetin Tarihi 45
3.5.2. Türkiye'de ve Dünyada İnternet Kullanımının Mevcut Durumu 46
3.5.3. Mobil Cihazlar 51
3.5.3.1. Cep Telefonu 51
3.5.3.2. PDA (Personal Digital Assistant) 54
3.5.3.3. SIM Kart 54
3.5.3.4. Hafıza Kartları 55
3.5.3.5. GPS (The Global Positioning System) 56
3.5.3.6. Tablet PC 57
3.5.3.7. Akıllı Saatler ve Diğer Giyilebilir Teknolojiler 57
3.5.3.8. Drone 58
3.5.3.9. Kart Kopyalayıcılar ve ATM Skimmer 59
4. TARTIŞMA 61
4.1. CMK 134. Maddesi Kapsamı Dışında Kalan Adli Bilişim İncelemeleri, İleri Düzey Teknik Yöntemlerin Uygulanabilirliği ve Tartışmalı Konular 61
4.1.1. Müşteki, Mağdur ve Maktul Açısından CMK 134. Maddesi 61
4.1.2. İdari Soruşturmalarda CMK 134. Maddesi Uyarınca Karar Alınıp Alınamayacağı Hususunun Değerlendirilmesi 62
4.1.3. CMK 134. Maddesi ve İleri Düzey Teknik Yöntemlerin Kullanılabilme Durumu 63

4.1.4. Mahkeme Kararında Dijital Materyal Özelliklerinin Geçmemesi, Olay Yerinde Tutulmuş Tutanakların Değerlendirilmesi ve Bu Evraklarda Sehven Gerçekleştirilmiş Maddi Hatalar 65

4.1.5. CMK 134. Maddesi Doğrultusunda Alınan Hakim Kararında İncelemeci Birimin Belirtilmesi 66

4.1.6. Kovuşturma Aşamasında CMK 134. Maddesi Tedbirlerinin Uygulanabilirliği 69

4.1.7. PUK Bilgisinin Elde Edilmesi 70

4.1.8. Bilişim Sistemleri Açısından Müsadere 71

4.1.9. Tesadüfi Delillerin Değerlendirilmesi 73

4.1.10. Bölümün İrdelenmesi 73

4.1.11. Çözüm Değerlendirmesi 77

4.2. Almanya ve Amerika Ülkelerindeki Hukuki Durum 78

4.3. Budapeşte Sözleşmesi ve Değerlendirme 81

4.4. Teknik Boyutta Karşılaşılan Sorunlar ve Çözüm Tartışmaları 82

4.4.1. İmaj Alma Olgusu 83

4.4.2. Hash Olgusu 85

4.4.3. İleri Düzey Teknik Yöntemler ve Zorluklar 87

4.4.4. Apple ve Veri Güvenliği 89

4.4.4.1. iOS Veri Şifreleme Sistemi Direnci 89

4.4.4.2. iOS Veri Şifreleme Sistemi Zayıflığı 92

4.4.4.3. Apple Cihazlarda Parmak İzi Güvenliği (TouchID) Aşma Yöntemi 95

4.5. Android İşletim Sistemi ve Kullanan Cihazlar 99

5. SONUÇ VE ÖNERİLER 101

ÖZET 104

SUMMARY 105

KAYNAKLAR 106

ÖZGEÇMİŞ 116

ÖNSÖZ

Adli bilişim, çalışma boyunca irdelenecek olan teknik, hukuki ve bilimsel yönleriyle kritik ve gizli olabilecek dijital veri üzerinde gerçekleştirilmektedir. Hukuki süreçler, teknik işlemler ve delil bütünlüğünü, kişi hak ve hürriyetleri açısından doğrudan ilgilendirdiği için mutlaka belli prosedür ve standartlar çerçevesinde profesyonelce uygulanması gerekmektedir. Uygulayanların eğitimli, tecrübeli ve yetkin olmaları da önem arz etmektedir. Uygulamadaki bir eksiklikten dolayı bulgunun bozularak delil niteliğini kaybetmesi ciddi hukuki sonuçlar ve sorumluluklar doğurabilecektir. Bu çerçevede; bir çok disiplinin bir arada kullanıldığı adli bilişime dair iş ve işlemlerde, bilinmeyen uygulamalar hakkında uygulayıcıların malumat sahibi olabilmesi, en doğru prosedürün uygulanarak hukuki sürecin en iyi şekilde yürütülmesi ve teknolojik gelişmeler neticesinde karşılaşılan güncel zorluklarla başa çıkılmasını sağlamak amacıyla tezde ilgili konular irdelenmiş, tartışılmış ve eksiklik görülen kısımlara yönelik çözüm önerileri sunulmuştur. Bu yönleriyle çalışmanın özellikle hukuk, kolluk kuvveti ve adli bilişim uygulanan sivil alanda faydalı olmasını, yeni çalışmalara ilham vermesini temenni etmekteyim.

Tezim, yüksek lisans eğitimim devam ederken kaybettiğim değerli babam Timur DOĞANAY ve kıymetli annem Gülşen DOĞANAY'a saygı ve minnetle, tez çalışmasının her safhasında emeği ve el izi olan, çok bunaldığım anlarda moral motivasyon ile beni tekrar çalışmaya sevk eden, güler yüzüyle desteğini her daim aldığım, bilgi birikimi ve karakteriyle her zaman saygı duyduğum eğitmene en kalbi duygu ve teşekkürlerimle, kardeşlerim Elif, Emine ve Koray ile canımız Gökay Anıl'a sevgi ve muhabbetle ithaf olunur.

Yüksek lisans eğitimim ve tez yazım sürecim boyunca emek ve desteklerinden dolayı danışmanım Prof.Dr. Hakkı Gökhan İLK ve yardımlarını asla esirgemeyen Prof.Dr. Refik SAMET'e, derslerini aldığım ve akademik gelişimime büyük katkıları olan öğretim üyelerimize, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü çalışanlarına sonsuz teşekkürlerimi sunarım.

SİMGELER VE KISALTMALAR

ABD	Amerika Birleşik Devletleri
AK	Avrupa Konseyi
AMOLED	Active-Matrix Organic Light-Emitting Diode
ARPANET	Advanced Research Projects Agency Network -Gelişmiş Araştırma Projeleri Dairesi Ağı
CAS	Cellebrite Advanced Services
CF	Compact flash
CMK	Ceza Muhakemesi Kanunu
CMUK	Ceza Muhakemeleri Usulü Kanunu
DARPA	Savunma İleri Düzey Araştırma Projeleri Kurumu
EGM	Emniyet Genel Müdürlüğü
FTK	Forensic Toolkit
FTP	File Transfer Protocol
GPS	Global Positioning System (Küresel Konumlama Sistemi)
GSM	Global System for Mobile
HTTP	Hyper Text Transfer Protocol
IrDA	Infrared Data Association
ISP	In-system programming
İHA	İnsansız Hava Aracı
JKDB	Jandarma Kriminal Daire Başkanlığı (JKDB)
JUGHEAD	Jonzy's Universal Gopher Hierarchy Excavation And Display
KHK	Kanun Hükmünde Kararnamede
LCD	Liquid Crystal Display - sıvı kristal ekran
MMC	Multimedia card
MMS	Multimedia Messaging

NCCIS	Ulusal Sibersuç ve Haberleşme Entegrasyonu Merkezi
NCMEC	National Center for Missing and Exploited Children
NCP	Network Control Protocol
NCSA	National Center For Supercomputing Applications
NFC	Yakın Alan İletişimi – Near Field Communication
NIST	National Institute of Standards and Technology
NSFNet	National Science Foundation-Ulusal Bilim Vakfı
ODTÜ	Ortadoğu Teknik Üniversitesi
OECD	Ekonomik İşbirliği ve Kalkınma Örgütü
OHAL	Olağanüstü Hal
OLED	Organic Light Emitting Diode
P2P	Peer to Peer –Eşten eşe
PDA	Personal Digital Assistant
PEFC	Programme for the Endorsement of Forest Certification
PIN	Personal Identification Number
POP IMAP	Post Office Protocol
PUK	Personal Unblocking Key
PVSK	Polis Vazife Ve Salâhiyet Kanunu
RAM	Rasgele erişim belleği
RFID	Radio Frequency Identification
ROM	Okunur bellek
SD	Secure drive
SIM	Subscriber Identity Module
SSMDB	Siber Suçlarla Mücadele Daire Başkanlığı
TCP/IP	Transmission Control Protocol/İnternet Protocol
TELNET	Telecommunication Network – İletişim Ağı
TSH	Türk Standartları Enstitüsü

TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
TÜRKAK	Türk Akreditasyon Kurumu
US-CERT	United States Computer Emergency Rediness Team
VERONICA	Very Easy Rodent-Oriented Netwide Index to Computerized Archives
WAIS	Wide Area Information Server
WAP	Wireless Application Protocol
Wifi	Wireless Fidelity
WWW	World Wide Web

ŞEKİLLER

Şekil 3.1 Laboratuvar İçin Mobil Cihaz İnceleme İş Akış Şeması 39
Şekil 3.2 Şüpheli İçin Mobil Cihaz Adli Bilişimi Olay Yeri İş Akış Şeması 40
Şekil 3.3 Türkiye'de İnternet, Mobil Cihaz ve Sosyal Medya Kullanımı 48
Şekil 3.4 Dünyada İnternet, Mobil Cihaz ve Sosyal Medya Kullanımı 49
Şekil 4.1 Cumhuriyet Başsavcılığı Talep Örneği 64
Şekil 4.2 Uygun Bulunduğu Mahkeme Hükmü Örneği 64
Şekil 4.3 Uygun Bulunduğu Mahkeme Hükmü Örneği 65
Şekil 4.4 FTK 7.0.0.163 Hash Algoritmaları 86
Şekil 4.5 iOS Yazılımsal ve Donanımsal Şifreleme Üst Seviye Şeması 91
Şekil 4.6 iOS Yazılımsal Şifreleme Adımları 92
Şekil 4.7 Silikon Tabancası 97
Şekil 4.8 Beyaz Tutkal Ön 97
Şekil 4.9 Alüminyum Folyo 97
Şekil 4.10 Beyaz Tutkal Arka 97
Şekil 4.11 Silikon Parmak İzi Kalıbı 98

ÇİZELGELER

Çizelge 3.1 Araştırma sonuçlarına göre dosyalara ait belirtilmesi gereken bilgiler 29
Çizelge 3.2 Araştırma sonuçlarına göre bulgu adli kopyaya ait belirtilmesi gereken bilgiler 29
Çizelge 3.3 Araştırma sonuçlarına göre bulgu veriye ait bulunması gereken bilgiler30
Çizelge 3.4 Araştırma sonuçlarına göre delil zinciri açısından bulunması gereken bilgiler 31
Çizelge 3.5 JKDB MJKLA Adli Bilişim Laboratuvar Akreditasyonu 37
Çizelge 3.6 Türkiye'de İnternet Kullanımına İlişkin Veriler 48
Çizelge 3.7 OECD (Ekonomik İşbirliği ve Kalkınma Örgütü) Üye Ülkeleri Nüfusa Göre İnternet Kullanımları ve Facebook Kullanıcı Sayıları 50
Çizelge 3.8 Mobil Cihazların Yazılımsal Özellikleri 53
Çizelge 3.9 Mobil Cihazların Donanımsal Özellikleri 53
Çizelge 4.1 Başarılı Chip-Off Örnekleri 100

1. GİRİŞ

“The Truth, The Whole Truth, Nothing But The Truth”

Teknolojinin günümüzde vardığı noktada insanların azımsanmayacak bir çoğunluğu iş, okul, gizli ve özel kısımları da dâhil olmak üzere hayatlarına dair en önemli bilgileri akıllı cep telefonları başta olmak üzere taşınabilir iletişim cihazlarında barındırmaktadırlar. Bu açıdan mobil cihazlardan elde edilen veriler adli süreçlerde ve mahkeme önünde gerçekten önemli bulgular olabilmekte, suçun ve/veya suçsuzluğun delillendirilmesinde büyük rol oynayabilmektedir. Bu rolün merkezinde ise adli bilişim ve mobil cihaz adli bilişimi kavramları bulunmaktadır.

Bu çalışma ile bir çok disiplinin bir arada kullanıldığı adli bilişimin tüm aşamaları irdelenmiş olacaktır. Teknik ve hukuki alanda bilinmeyen adli bilişim uygulamaları bulgu olarak sunularak, pratikte en doğru prosedürün takip edilip hukuki sürecin en iyi şekilde yürütülmesi ve teknolojik gelişmeler neticesinde karşılaşılan güncel zorluklarla başa çıkılmasını sağlamaya yönelik tespitlere yer verilecektir. Tespitler alan tecrübesi ve uygulamalı çalışmalar ile desteklenecektir.

Yine çalışma ile adli bilişime yönelik tartışılan ve eksiklik görülen süreçlere yönelik çözüm önerileri de sunulmuştur. Bu özgün yönleriyle çalışmanın özellikle hukuk, kolluk kuvveti ve adli bilişim uygulanan sivil alanda faydalı olması amaçlanmıştır.

Çalışma yapılırken öncelikle bir literatür taraması yapılmış yerli ve yabancı güncel kaynaklardan faydalanılmaya çalışılmıştır. Malum bu alan hızlı teknolojik gelişmelere bağlı olarak güncel yenilikleri barındırmaktadır. Yenilikleri takip etmek amacıyla sadece bilimsel basılı eserler değil bunların yanında; açık İnternet kaynakları, bilişim şirketlerine ait İnternet sayfaları, Youtube’ta yayınlanan videolar vb. üzerinden kapsamlı taramalar yapılmıştır.

Çalışmanın bir diğer boyutu olan hukuki veçhe ile ilgili olarak ise resmi gazetede yayımlanan hukuki metinler gerek yayımlanma tarihi gerekse güncellenmiş son halleri ile değerlendirilmiştir. Mahkeme kararları ile gerçek vakalara dair uygulamalar araştırılmış, yayınlanmış tezlerin özellikle bulguları da göz ardı edilmemiştir.

Çalışma yapılırken yukarıda sıralanan kaynaklardan teorik boyutu kurgulanmış, bunun yanı sıra deneysel yöntem de kullanılmıştır. Çeşitli mobil cihazlar üzerinde yardımcı malzeme, donanım ve yazılımlar kullanarak testler yapılmış, adli bilişim inceleme yazılımlarından istifade edilmiştir.

Tezin konusunun önemini anlamak bakımından ise çeşitli istatistiklerden bahsetmek gerekmektedir. Zira Reuters haber ajansının Orbis araştırma firmasından aktardığı bilgiye göre 2017 yılında 3.09 milyar dolar olan adli bilişim pazarının 2023 yılında 6.83 milyar dolar olması beklenmektedir. Bu pazarı besleyen şey adli bilişim bilimi olacaktır. Bu tez çalışmasının amacını destekleyen önemli unsurlardan biri de adli bilişim ve özellikle mobil cihaz adli bilişimi alanındaki hukuki ve teknik boyuttaki birçok soru ve soruna cevap ve çözüm önerisi sunması olacaktır. Diğer bir dayanak olarak ülkemizin bu alanda söz sahibi olması için daha çok akademik çalışmaya ve bu alandaki yüksek lisans ve doktora çalışmalarının artırılmasına ihtiyaç olduğu düşünülmektedir. Mevcut çalışmamız da bu amaç ile gerçekleştirilmiştir.

Adli bilişimde incelenen dijital verilerin hassasiyeti Anayasamız tarafından güvence altına alınmış olan kişi özel hayatı, hak ve hürriyeti gibi vazgeçilmez haklar ile doğrudan bağıntılı olmasından kaynaklanmaktadır. Dijital veriler kasten veya sehven olacak şekilde kolaylıkla tahrif veya tahrip edilebilirler. Bu nedenle korunması gereken haklar mutlaka göz önünde bulundurularak, Anayasa ve uluslararası hukuk ihlalleri gerçekleştirilmemesi adına gerekli hukuki ve teknik alt yapı sağlanmalıdır. Bununla birlikte suçla mücadele açısından da birçok ülkede uygulandığı üzere suçun en etkin şekilde tespiti için ihtiyaç olunan bütün imkânlar, hukuken ve teknik açıdan sağlanmış olmalıdır. Bu nedenle güven unsuru kişi veya kurumlar üzerine değil kamu vicdanını rahatlatacak güvenilir ortak bir sistem üzerine kurulmalıdır.

Giriş başlıklı bu bölümdeki giriş cümlesi olan “The Truth, The Whole Truth, Nothing But The Truth” cümlesi bu hassasiyet açısından tercih edilmiştir. Gerçek, bir kısmıyla değil bütünüyle sunulmalıdır ve adli bilişim incelemelerinde de bu disiplin tercih edilmelidir. Bahse konu sistemin kurulmasının çıktıları arasında kamu vicdanını rahatlatacak olmasının yanında, ülke itibarının artması ve korunması, uluslararası alanda hukuk sistemimizin ve burada tespit edilen delillerin güvenilirliğinin artması ve milli servetin korunması gibi çok önemli çıktıları da olacaktır. Bu sistemde bulunması gereken özellikler tez çalışmasında irdelenecek ve ortaya konacaktır.

Adli bilişim işlemleri en temelde hem hukuki hem de teknik boyuta sahiptir. Dolayısıyla adli bilişim incelemeleri gerçekleştirilirken şahsi ve özel verilerin hassasiyeti açısından uyulması gereken hem hukuki adımlar, hem iş akış ve uygulama prosedürleri, hem de uygun teknik işlemler gerektiği gibi yürütülmelidir. Delil bütünlüğünün ve güvenilirliğinin göstergesi olan “delil zinciri” sisteminin sağlanması ve mümkün olduğunca azami ölçüde kırılmadan uygulanması gereklidir. Oluşturulacak sistematik prosedürler delil zincirinin en temel taşıdır. İncelenen verinin incelemeci tarafından uygun ve belli bir şablonda raporlanması da adli makamların işini kolaylaştıracak ve adaletin daha kısa sürede tesis edilmesine katkıda bulunulacaktır. Tez içerisinde, delil zincirinin güvencesi olacak olan günümüz adli süreci içerisindeki en güncel ve ideal iş akış şeması ortaya çıkarılacaktır. Adli sürecin hızlandırılması, adli bilişim incelemecileri için daha geniş bir vizyon sağlanması ve dijital delil güvenliğinin nasıl artırılabileceği hakkında çözümler üretilebilmesi adına bu alanda gerçekleştirilmiş çalışmaların ve oluşturulmuş uluslararası standartların irdelenmesi gereklidir. Bunun sonucunda elde edilecek bilgilerin somut yurt dışı örnekleri ile karşılaştırılması geliştirilebilir fikirler ve çözümler sağlayacaktır.

Kişilerin hak ve hukukları kolluk kuvvetleri tarafından bu prosedürler ile koruma altına alınmaya çalışılırken diğer taraftan gelişen teknolojiyi suçun gizlenmesi için kullanan suçlular ve suç örgütleri de mevcuttur. Şifreleme, ekran kodları, PIN (personal identification number) kodları, verinin kriptolanması gibi kişisel verilerin güvenliğini sağlayan ancak suç verisini de koruyor olabilecek birçok yöntem karşısında kolluk kuvvetleri ve incelemeciler bilgi eksikliği, bilginin değerli oluşundan

dolayı gizleniyor oluşu veya o konuda henüz bir çözüm bulunmuyor olmasından dolayı çaresiz kalabilmektedirler. Bu nedenle sürekli güncellenen yazılımların kullanılması, inceleme yapan görevlilerin mevcut bilgilerini güncel tutması ve dünyadaki diğer uygulama ve gelişmelerin takip edilmesi önemlidir.

Bu tez kapsamında yukarıdaki hususlar değerlendirilirken mobil cihaz adli bilişiminde en güncel sorunlar ortaya konacaktır. İşbu çalışma gelişim aşamasında iken ülkemizde adli bilişim iş ve işlemlerinin dayandırıldığı Ceza Muhakemesi Kanunu (CMK) 134. Maddesinde kanun koyucu tarafından değişiklikler de gerçekleştirilmiştir. Bu durum yeni olması sebebiyle uygulama ve kişinin kanuni hakları açısından da değerlendirmeye muhtaç bir durumdur ve çalışma içerisinde değerlendirmesi yapılarak sorun olarak görülen noktalara çözüm önerilerinde bulunulmuştur. Teknik sorunların teknolojik ve bilimsel çalışmalar ile çözülmesi beklenirken, delilin bütünlüğü ve güvenilirliği ile kişi hak ve hürriyetlerinin korunması bağlamında adli süreçte doğabilecek sorunların ise uygun iş akışı, prosedür ve standartları içeren bir sistemin takip edilmesi ile çözülmesi beklenmelidir. İlgili kanun maddesi genel hatları belirlemeli ve hukuki sınırları çizmeli, uygun şekilde oluşturulacak uluslararası standartlara uygun olarak kamu vicdanının kabul edeceği şekilde ilgili kurumlarca oluşturulmuş iş akışı ve prosedürler kanalıyla uygulanmalıdır. Hukuki ve teknik boyuttaki bu sorunlara karşı atılabilecek adımlar ve uygulanabilecek yeni teknik yöntemler, gerçek vakalar ve istatistiksel veriler kullanılarak çözüm önerileri şeklinde sunulacak ve irdelenecektir.

Özetle bu tez ile mobil cihaz adli bilişimi alanında yaşanan zorluklara önerilecek çözümlerin, özellikle adli süreçlerin doğru şekilde işlemesi adına faydalı olması, multidisipliner ve interdisipliner bir yapıya sahip olan adli bilişim alanının bir alt disiplini olan mobil cihaz adli bilişimi alanında getirilecek çözüm önerileri ile bu bilim alanında var olabilecek diğer sorunlara da ışık tutması amaçlanmaktadır. Amaca ilişkin çalışmalar sunulurken adli bilişim genelinde konular değerlendirilecek, mobil cihaz adli bilişimi özelinde ilintili hususlar derinleştirilecektir. Bunun yanında kapsama giren kişi ve kuruluşların referans alabileceği bir çalışma meydana getirilmesi hedeflenmektedir. Adli bilişim iş ve işlemleri için birçok farklı ilde farklı hakimler

karar vermekte, aynı şekilde farklı birçok görevli veya bilirkişi eli ile inceleme gerçekleştirilmektedir. Dijital verilerin incelenmesi sonucu oluşturulan teknik inceleme raporu ise yine bir başka birim veya görevli tarafından değerlendirilmektedir. Kısacası böyle farklı alanlarda yürütülen, adli süreçte çok büyük önemi olan ve hassasiyeti tartışılmayacak adli bilişim iş ve işlemlerinde ortak bir dile ve delil zincirinin bütünlüğünü sağlayacak adımlara ihtiyaç vardır. Ülkemizde kurumlar ve kişiler bu standartları uluslararası benzerlerini örnek alarak yürütmeye çalışmaktadır. Ancak bu durumda dahi farklı anlayışlar kabul edildiğinden veya bu kurallar yazılı olarak bulunmadığından uygulamada farklılıklar görülebilmektedir. CMK 134. Maddesi de hem uygulayanlar hem de muhataplar tarafından olumlu ve olumsuz yanları ile eleştirilmektedir. Bu eleştiriler akıllarda soru işareti bırakabilmektedir. Teknik açıdan ise hem kavramlar hem de gelişen teknoloji ile karşı karşıya kalınan zorluklar her geçen gün artmakta, bunun karşısında bu zorluklara yeni çözümler üretilebilmektedir. Yine çalışmada en güncel teknik sorunlara değinilerek mevcut çözüm önerileri irdelenmiş ve sunulmuştur.

Bu çalışmanın, hem bu alanda bilimsel çalışma yürütmek isteyen hem de mobil cihaz adli bilişimi icra etmek isteyen kişiler ve kurumların referans alacakları bir çalışma olmasının hedeflenmesinin en güçlü sebepleri yukarıda bahsedilen hususlardır. Ayrıca önemli bir alan olan mobil cihaz adli bilişiminde inceleme sürecine olumlu katkıda bulunarak ülkemize yarar sağlaması, bahse konu alan için çok fazla kaynak taraması ve deneme yanılma yönteminin yerine tez çalışmasının kullanılması sonucu zaman ve maddi kaynağın etkin kullanımı ile ülke ekonomisine katkıda bulunulması da ulaşılmak istenen hedefler arasındadır.

2. GEREÇ VE YÖNTEM

Mobil Adli Bilişiminin Önemi Bağlamında Delil Zinciri Kavramının ve Yeni Nesil Mobil Cihazların İncelenmesinde Karşılaşılan Güncel Zorlukların Değerlendirilmesi konusunun başarılı şekilde irdelenebilmesi için hem teknik hem de hukuki açıdan tetkik edilmesi gerekmektedir. Bu nedenle çalışma boyunca araştırma yöntemi, literatür tarama, İnternet kaynaklarından faydalanma, gerçek hukuki belge ve uygulamaları araştırma, adli bilişim inceleme yazılımlarını değerlendirme ve çeşitli mobil cihazlar üzerinde yardımcı malzeme, donanım ve yazılımlar kullanarak testler gerçekleştirme şeklinde uygulanmıştır.

2.1. Kullanılan Malzeme, Cihaz ve Yazılımlar

Muhtelif marka model akıllı cep telefonları, ısı tabancası, sıcak silikon barı, beyaz tutkal, i7 işlemcili dizüstü bilgisayar, MacOS işletim sistemli Apple marka bir dizüstü bilgisayar malzeme, havya ve ısı istasyonu malzeme ve cihaz olarak kullanılmıştır.

Forensic Toolkit (FTK), FTK Imager ve UFED 4PC yazılımları ise çalışma boyunca ağırlıklı olarak kullanılan inceleme yazılımlarıdır.

2.2. Kullanılan Diğer Gereçler

Çalışma boyunca adli bilişimin hukuk alanında uygulanan yöntemler, hukuki süreçteki belgeler, kanun metinleri ve akademik çalışmalar çalışmanın geliştirilmesinde kullanılmıştır.

3. BULGULAR

3.1. Adli Bilişimin Tanımı ve Kapsamı

Literatürde adli bilişim kavramının tanımı ve kapsamı ile ilgili olarak birçok farklı anlayış bulunmaktadır. Gerek bu tanımların eksikliği gerekse teknolojik ve uygulama bilgisi yetersizliğinden kaynaklı mevcut durum, bu alanda mevzuat ve düzenleme çalışmalarına da olumsuz olarak yansımaktadır. Örnek olarak Aydoğan çalışmasında adli bilişim ile ilgili birçok kaynaktan tanıma yer vermiş, tanımların eksikliği hakkında isabetli bir görüş belirtmiştir. Ancak bu kavram çokluğu içinde dahi belirtilen önceki tanımları kapsayan bir tanım verilemediği, özet bir tanımla yetinildiği görülmüştür (Aydoğan, 2009:8). Aynı çalışmada verilen literatürdeki bazı adli bilişim tanımları aşağıdaki gibidir:

"Adli Bilişim, bilgisayar biliminin yasal sürece katkıda bulunmak üzere uygulanması bilimi ve sanatıdır" (Brown, 2006: 3).

"Adli Bilişim bilgisayar datasının muhafazası, tanımlanması, elde edilmesi, dokümantasyonu ve yorumlanmasıdır" (Kruise ve Heiser, 2002: 2).

"Adli Bilişim en basit tanımıyla, bir yargılama esnasında kullanılabilecek potansiyel delillerin belirlenmesi için bilgisayar araştırma ve analiz tekniklerinin kullanılmasıdır. Bilgisayardaki verilerin korunması, tanılanması, çıkarılması, dökümü ve yorumunu içerir ancak bunun yanında hukuki kurallar, süreçler, delillerin bütünlüğü gibi konulara da riayet ederek bulunan veriler hakkında rapor yazılmasını da kapsar" (Aydoğan,2009:8)

"Adli Bilişim (Computer Forensics – Bilgisayar Kriminalistiği) bilimi; suçun aydınlatılabilmesi için bilimsel metotlar kullanılarak, çeşitli varyasyonlardaki dijital medyalar üzerinde bulunan, suçla ilgili dijital delillerin bozulmadan ve zarar görmeden anlaşılabilir bir şekilde adalet önüne sunulmaya hazır hale getirilmesini sağlayan ve

başlı başına bilimsel teknik prensiplerin uygulandığı bir delil inceleme sürecinin bütünüdür" (Ekizer, 2014)

Adli bilişimde bazı eksik tanım ve kapsam anlayışı ile oluşturulan mevzuat ve buna bağlı saha uygulamaları hem görevliler hem de materyali incelenecek olan kişiler açısından çeşitli problemlere yol açmaktadır. Örnek olarak CMK 134. Maddesinde tanımlanmış olan "bilgisayar ve bilgisayar kütükleri" ibaresi tanımı yapılmadığı zaman teknik bilgi eksikliğinden dolayı bir Cumhuriyet Savcısı veya kolluk kuvvetinden bir incelemeci tarafından USB flash bellek gibi bir veri depolama birimi bu madde kapsamı dışında olarak algılanabilmektedir. Hâlbuki USB flash bellek de ilerleyen bölümlerde ayrıntılarıyla anlatılacağı gibi bilgisayar kütüğü olarak tanımlanan verileri barındırmaktır. Bu sebeplerle öncelikli olarak adli bilişimin tanımı tüm evrelerini kapsayacak şekilde aşağıdaki gibi yapılabilecektir.

Adli bilişim, bilişim sistemlerinde iletilen, işlenen ve/veya depolanan dijital verinin adli talimat üzerine elde edilerek bulgu olarak tespit edilmesinden, raporlanarak delil olarak değerlendirilmesi amacıyla mahkemeye sunulmasına kadar geçen süreçte delil zinciri her aşamada uygulanarak gerçekleştirilen multidisipliner (çoklu disiplinli) ve interdisipliner (disiplinler arası) halde işletilen teknik ve hukuki adımlar ile işlemler bütünüdür.[1]

Burada karşımıza çıkan diğer bir kavram ise "bilişim sistemleri" kavramıdır. Bilişim sistemi; manyetik, optik veya elektriksel ortamlarda bulunan veriyi sayısal olarak işleyebilen, saklayabilen ve/veya iletebilen cihaz veya cihazlar bütününe verilen isimdir. Dijital veri; bilişim sistemlerinde manyetik, optik ve/veya elektriksel olarak saklanan, iletilen ve/veya işlenen verinin ikilik (binary) sistem kullanılarak anlamlandırılmış halidir. Türkçe'ye sayısal veri olarak çevrilmektedir. Ülkemiz adli bilişim literatüründe bilişim sistemleri çoğunlukla dijital materyal olarak adlandırılmaktadır. Bundan dolayı çalışma boyunca bilişim sistemleri kavramının karşılığı olarak dijital materyal kavramı da kullanılacaktır. Dijital materyallerin veya

[1] Söz konusu tanım literatürdeki tüm tanımlara vurgu yapmakla birlikte kapsayıcı ve özgündür. Hamza Aytaç DOĞANAY, Adli Bilişim Uzmanı

dijital verinin adli süreçte doğrulanabilir ve değiştirilmediği kanıtlanabilir halde alınan kopyalarına ise adli kopya (imaj) adı verilir. Manyetik veya enerji olarak saklanan veriler ise çeşitli dönüştürücüler ile sayısal veriye dönüştürülüp çeşitli yazılımlar ile tasnif edilebilir.

Adli bilişimin vurgulanan bir diğer özelliği ise multidisipliner bir yapısı olmasıdır. Adli bilişim birçok akademisyen tarafından bir bilim olarak tanımlanır ve dijital delilin öneminin geniş kitlelerce kabul edilmesi ile büyük adımlar atıldığı ve adli bilişim bilimindeki bilim kelimesinin vurgulandığından emin olunmasının sağlandığı belirtilir. (Beebe, 2009:30). Bununla birlikte literatürde adli bilişim bazı ana alanlara ayrılır. Farklı sayıda başlıklar belirlenen bu alanlar için çoğu zaman dört ana başlık tanımlanır. Bunlar bilgisayar adli bilişimi, mobil cihaz adli bilişimi, ağ adli bilişimi ve bulut adli bilişimidir (Lutui, 2016: 594). Bu alanların hepsi teknik olarak benzerlik gösterse de farklı disiplin dalları sayılabilirler. Sayılan dalların altında işletim sistemi, veri tabanı, bunlardan veri kurtarma ve yazılım alanı gibi birçok alt uzmanlık alanı oluşturmak da mümkündür. Görüldüğü üzere teknik olarak birçok disiplin adli bilişim alanına girebilmektedir. Bununla birlikte adli boyutundan dolayı hukuk alanı da adli bilişim açısından önemi tartışılmaz disiplinlerdendir. İlgili bilgiler değerlendirildiğinde adli bilişimin multidisipliner özelliği açıkça görülmektedir. Bu yaklaşımda disiplinlerin koşut ve ardışık olarak yürütülmesi söz konusu iken adli bilişim incelemecilerinin multidisipliner bir anlayışa sahip olmaları gerektiği bununla birlikte dijital incelemenin interdisipliner doğasının mutlaka göz önünde bulundurulması gerektiği savunulur (Irons, 2009:84). Disiplinlerin birbiri ile uyum içinde çalıştıkları ve birbirlerinin alanlarını daraltmadıkları düşünüldüğü taktirde bu yaklaşımın da doğru olduğu düşünülebilir. Örneğin bir bilgisayar üzerinde adli bilişim incelemesi yapılacağı zaman hukuk ve bilgisayar bilimi aynı vakada işletilir. İki disiplin bu durumda birbirlerinin alanını kesinlikle daraltmamakta, birbirleri ile etkileşim içerisinde yürütülmektedir. Bu kadar disiplin arasında adli süreçte de en doğru tespitlerin gerçekleştirilmesi için adli bilişim incelemesi yapacak kişilerin gerekli eğitimleri almış ve tecrübe kazanmış olmaları gerekmektedir. Hatta adli sürecin ve adalet kavramının önemi ile dijital verinin hassasiyeti göz önünde bulundurularak uzman yardımcısı ve uzman gibi profesyonel sınıflandırmalara

gidilmesi gerçekleştirilen adli bilişim işlemlerinin kalitesini artıracak ve standartlara daha uygun hale getirecektir. Aksi taktirde tecrübesizlik ve bilgisizlik sonucu delil zincirinin bozulması ve bulgu verinin delil özelliğini kaybetmesi işten bile değildir. Bu durumda da adaletin tesis edilmesinden bahsedilemeyecektir.

Yine literatürdeki adli bilişim safhalarına bakıldığı zaman adli bilişim iş ve işlemlerinin akademik ve bilimsel çalışmalarda genellikle "toplama" işlemi ile başlatıldığı görülmektedir (Ukşal, 2015:25). Ancak yukarıdaki tanımda da geçen "bulgu" kelimesinden anlaşılacağı üzere adli bilişim iş ve işlemleri hukuki bir eylem ile başlamaktadır. Öyle ki; adli yönü olmayan bir dijital materyal incelemesi sadece teknik bir inceleme olmaktan öteye geçmeyecektir. Adli talimat alınmadan gerçekleştirilecek olan dijital bulgu incelemelerinde tespit edilen verilerin mahkemede delil olarak kullanılması da mümkün olmayacaktır. Burada "delil" kavramının kullanılmadığı bunun yerine "bulgu" kavramının kullanıldığı görülmektedir. Bunun nedeni her hangi bir verinin delil sayılması için mahkeme tarafından delil olarak kabul edilmesinin gerekli olduğunun düşünülmesidir. Delil sayılana kadar bu yönde değerlendirilecek her türlü verinin bulgu olarak nitelendirilmesi uygun olacaktır. Öyle ki Anayasamızın 38. Maddesinde 2001 yılında yapılan değişiklikle bu iki kavramın farkına vurgu yapıldığı görülmektedir. İlgili maddedeki "Kanuna aykırı olarak elde edilmiş bulgular, delil olarak kabul edilemez" fıkrası bulgu ve delil kavramlarının birbirinden farklı olduğunu göstermektedir. Ülkemizde halen bulgu yerine delil kavramı sıklıkla kullanılmaktadır. Bununla birlikte adli bilişim alanında ülkemizdeki kabiliyetli kurumlardan olan Emniyet Genel Müdürlüğü (EGM) Siber Suçlarla Mücadele Daire Başkanlığı'nın (SSMDB) dijital materyal için kullandıkları poşetlerin üzerine 2015 yılına kadar "delil torbası" yazarken 2015 yılı ve sonrasında "Bulgu Poşeti" yazması bu farkındalığı yansıtmaktadır. Ek olarak bu iki kavramın birbirlerinin yerlerine kullanılmasının ileri düzey bir sorun teşkil etmeyeceği düşünülse de literatürde kavramların yerinde ve ortak dille kullanılmasının bu alanda teknik, akademik veya hukuki boyutta çalışan görevli, araştırmacı ve incelemecilerin birbirlerini anlamalarını kolaylaştıracaktır.

Bölümdeki bilgiler ışığında ülkemizde de kolluk tarafından uygulanan adli bilişim genel safhalarını aşağıdaki gibi sıralayabiliriz:

1. Adli Talimatın Alınması
2. Bilişim Sisteminin Tespiti
3. Bulgunun Muhafaza Altına Alınması
4. İnceleme ve Analiz
5. Raporlama ve Adli Makamlara Sunum

Bunlardan 2 ve 3 numaralı safhalar dijital delillere ilk müdahale safhalarını oluştururlar.

3.2. Adli Bilişimin Safhaları

Adli bilişimin safhaları aşağıdaki şekli ile tasniflenebilir.

3.2.1. Adli Talimatın Alınması

Temel olarak adli bilişim iş ve işlemleri ülkemizde 5271 Sayılı Ceza Muhakemesi Kanunu 134. Maddesi uyarınca gerçekleştirilmektedir.[2] Aşağıdaki bölümlerde detayı verilecek olan kanun değişiklikleri neticesinde şüpheliye ait bilişim sistemleri hakkındaki adli bilişim iş ve işlemleri CMK 134. Maddesinde gerçekleştirilen değişiklik ile hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından verilecek olan adli talimatın alınması ile başlamaktadır. Cumhuriyet savcısı tarafından verilecek olan adli talimat 24 saat içerisinde hakim onayına sunulmak zorundadır. Bununla birlikte CMK 134. Maddesi sadece "şüpheli" için tasarrufta bulunmaktadır. Maktul veya müşteki için CMK 134. maddesinde herhangi bir düzenleme bulunmamaktadır. Kolluk kuvvetlerimizdeki uygulamada maktul ve müşteki dijital materyallerinin incelenmesi Cumhuriyet savcısının yazılı talimatı ile gerçekleştirilmektedir. Keyfi işlemlerin önlenmesi açısından şüpheli

[2] 04.12.2014 tarihli kanunun tam metni için bknz. http://www.resmigazete.gov.tr/eskiler/2004/12/20041217.htm#1 (Erişim Tarihi: 09.02.2019)

haricindeki taleplerin Cumhuriyet savcısı talimatı ile gelmesi uygun olacaktır. Bu kararlar ve talimatlar yazı boyunca adli talimat olarak adlandırılmaktadır. Bununla birlikte son birkaç yıl içerisinde ilerleyen bölümlerde detaylandırılacak olan bazı kanunlar ile CMK 134. Maddesi içeriğinde bazı değişiklikler gerçekleştirilmiştir.

Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Başlıklı CMK 134. Maddesinin 6526 Sayılı Terörle Mücadele Kanunu ve Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanunu sonrası ve ilerleyen bölümlerde irdelenecek olan bu tarihten sonraki değişikliklerden önceki hali aşağıdaki gibidir[3]:

Madde 134 - (1) Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli 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 çözülememesinden 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.

[3] 06.03.2014 tarihli kanunun tam metni için bknz.
http://www.resmigazete.gov.tr/eskiler/2014/03/20140306M1-1.htm

(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.

Genel olarak ilgili kanun maddesi incelendiğinde, dijital veri incelemesi için son değişikliklerden önce sadece hakim kararı alınmasının kanun koyucu tarafından şart koşulduğu görülmektedir. Eski halinde normal şartlarda gecikmesinde sakınca bulunan hal veya başka bir makama yetki tanınmamıştır. Bu açılardan kanun koyucunun bu konuda hassas olduğu anlaşılmaktadır. Ancak dünya standartları, uygulamadaki zorluklar ve teknolojik gelişmeler nedeniyle CMK 134. Maddesinin geliştirilerek değiştirilmesi gerektiği görülmektedir.

Uygulamadaki zorlukların hissedildiği düşünülen 21 Temmuz 2016 ve 19 Temmuz 2018 tarihleri arasında devam eden Olağanüstü Hal (OHAL) döneminde çıkarılan 668 Sayılı Kanun Hükmünde Kararnamede (KHK)) ve 6755 Sayılı Olağanüstü Hal Kapsamında Alınması Gereken Tedbirler İle Bazı Kurum Ve Kuruluşlara Dair Düzenleme Yapılması Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabul Edilmesine Dair Kanun adıyla kanunlaşan halinin 3. Maddesi J Fıkrası ile CMK 134. Maddesi uygulamasında bazı değişiklikler yapıldığı görülmektedir. Bu değişikliği gösteren ilgili fıkra aşağıdaki gibi olup, kanun koyucunun çeşitli zorlukları göz önünde bulundurarak süre ve ilk talimat açısından bazı değişiklikler gerçekleştirdiği ancak kanun maddesinin özündeki dijital veri hassasiyetini koruduğu değerlendirilmektedir:

“5271 sayılı Kanunun 134 üncü maddesi uyarınca bilgisayarlarda, bilgisayar programlarında ve kütüklerinde yapılacak arama, kopyalama ve el koyma işlemlerine, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da karar verilebilir. Bu karar, beş gün içinde görevli hâkimin onayına sunulur. Hâkim, kararını elkoymadan itibaren on gün içinde açıklar; aksi halde el koyma kendiliğinden kalkar. Kopyalama ve yedekleme işleminin uzun sürecek olması halinde bu araç ve gereçlere el konulabilir. İşlemlerin tamamlanması üzerine el konulan cihazlar gecikme olmaksızın iade edilir.”

İrdelenen değişiklikler son olarak 25/07/2018 tarih ve 7145 Sayılı "Bazı Kanun Ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanunun" 16. Maddesinde aşağıdaki şekilde düzenlenmiş ve kanun olarak uygulanmaya konmuştur:

"5271 sayılı Kanunun 134 üncü maddesinin birinci fıkrasında yer alan "Cumhuriyet savcısının istemi üzerine" ibaresi "hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından" şeklinde değiştirilmiş, fıkrada yer alan "hâkim tarafından" ibaresi madde metninden çıkarılmış, fıkraya aşağıdaki cümleler eklenmiş ve ikinci fıkrasına "bilgilere ulaşılamaması" ibaresinden sonra gelmek üzere "ya da işlemin uzun sürecek olması" ibaresi eklenmiştir.

"Cumhuriyet savcısı tarafından verilen kararlar yirmi dört saat içinde hâkim onayına sunulur. Hâkim kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde çıkarılan kopyalar ve çözümü yapılan metinler derhâl imha edilir."

İşbu tez tarihi itibari ile CMK 134. Maddesi 7145 Sayılı kanunda belirtilen değişiklikle birlikte yürürlükte olan hali aşağıdaki gibi olup son değişiklik ile ilgili olarak bölüm sonunda ayrıca değerlendirme sunulacaktır:

(1) Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine karar verilir. Cumhuriyet savcısı tarafından verilen kararlar yirmi dört saat içinde hâkim onayına sunulur. Hâkim kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde çıkarılan kopyalar ve çözümü yapılan metinler derhâl imha edilir

(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.

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

3.2.1.1. CMK 134. Maddesinin Birinci Fıkrasının Değerlendirilmesi

CMK 134. Maddesinin birinci fıkrasında bir suç dolayısıyla suç soruşturmasının yürütülüyor olması, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması, şüpheliye ait bir bilişim sisteminin incelenebilmesi için ön şartlar olarak görülmektedir. Bu ibareler dijital materyal incelenmesi gerektiğinde kişilerin hak ve hukuklarına hassasiyet gösterilmesi ve dijital verinin hassasiyetinden dolayı karar verilmesinin katı kurallara bağlanması olarak yorumlanabilir. Bu hassasiyete hukuken önem verilmesi gerektiği düşünüldüğünden bu ibarelerin ek olarak detaylandırılmasına ihtiyaç duyulmamıştır.

3.2.1.2. Bilgisayar, Bilgisayar Programları, Bilgisayar Kütükleri Kayıtların Çözülerek Metin Haline Getirilmesi İbarelerinin Değerlendirilmesi

Aynı fıkrada adli bilişim konusu olarak "bilgisayar ve bilgisayar programları ile bilgisayar kütükleri" ibareleri bulunmaktadır. Teknik açıdan bakıldığında bu ibareler, incelenecek olan dijital materyalleri tam anlamıyla karşılamaktadır. Bunun göstergesi olarak teknik bilgi yetersiz olduğu durumlarda yorumlandığında bu kavramların karşılık geldiği cihazlar hakkında yanlış değerlendirmeler yapılabildiği görülmektedir. Tanım eksikliğinden dolayı teknik bilgisi eksik bir kişi tarafından bir cep telefonunun bilgisayar olmadığı söylenerek CMK 134. Maddesi dışında değerlendirilmesi gerektiği iddia edilebilir. Hâlbuki hem dijital verinin hassasiyeti, hem kişilerin özel hayat gizliliğine riayet, hem de teknik açıdan cep telefonları için bu kanun maddesinin işletilmesi gerekir. Teknik anlam olarak bilgisayar; kısaca aritmetik ve mantıksal işlemler yapabilen programlanabilir cihazlar olarak tanımlanır. Örnek olarak, bahsi geçen "cep telefonları" bu tanıma uymaktadır. Bilgisayar kütükleri ifadesinde geçen "kütük" kelimesi ise ingilizce "log" kelimesinden gelmektedir. Log kavramı bilişim alanında "kayıt" kelimesinin karşılığıdır. Bu açıdan kanunda geçen bilgisayar kütükleri ibaresi bilgisayar dosya ve dizinlerini ifade etmektedir. Fakat yine de ilgili kanunda, bilişim sistemleri ve dijital veri kavramlarının tanımları yapıldıktan sonra tanımı yapılan bu güncel kavramların kullanılmasının daha isabetli olacağı değerlendirilmektedir.

Ayrıca kayıtların çözülerek metin haline getirilmesi teknik ve reel açıdan garipsenecek bir durumdur. Örnek olarak Microsoft Office Word yazılımı kullanılarak bu yazılıma ait türde bir metin dosyası oluşturulduğu varsayılırsa, 4 GB'lık bir flash belleğin ortalama hesapla 200'er sayfalık 1700'den fazla kitap alabileceği söylenebilir. Bu duruma ek olarak, metin haline getirme işinin, ekranda gördüğümüz dosya, yazı vb. verinin teknik açıdan değerlendirilerek disk üzerindeki 0 ve 1 sayısal halini metin haline getirmek olarak algılanırsa, ilgili örnekten bile daha fazla sayfa ortaya çıkacaktır. "Metin haline getirilmesi" ifadesinin yerine "tespit edilen bulgu verinin raporlanmasına" ifadesinin kullanılmasının daha uygun olacağı değerlendirilmektedir.

3.2.1.3. Dijital Veride Arama ve Rızaen Arama

CMK 134. Maddesinde kastedilen arama ve el koyma bilişim sistemleri ve içerdikleri veriler üzerinde gerçekleştirilecek arama ve el koymadır. Bu durumun CMK 116 ve devam eden maddelerinde geçen arama ve el koyma ile zaman zaman karıştırıldığı görülmektedir. Bilişim sistemleri ve dijital veriler hakkındaki el koyma, arama ve kopya çıkarılması gibi adli işlemlerin kesinlikle diğer eşya ve materyallerden ayrılacak şekilde farklı bir kanuni düzenleme ile gerçekleştirilmesinin dijital verilerin hassasiyeti göz önüne alınarak kişisel verilerin ve hakların korunması bağlamında önemli olduğu düşünülmektedir. Bu nedenle bilişim sistemleri için arama ve el koyma işlemleri CMK 116 ve devam eden maddelerdeki şekilde değil CMK 134. Maddesinde bu alanda çıkarılabilecek özel ve yeni düzenlemelerdeki şekliyle uygulanmalıdır. Örnek olarak CMK 120. Maddesinde aramada hazır bulunabilecekler belirtilmektedir. Ancak CMK 134. Maddesi uyarınca gerçekleştirilecek aramada CMK 120. Maddesinde sayılan fazla hazirunun olay yerinde bulunması işlemleri yavaşlatan ve çoğu zaman gereksiz bir durum olacaktır. Çünkü dijital veri üzerinde gerçekleştirilen aramalar çoğunlukla laboratuvar ortamında ve ev araması gibi aramalara nazaran daha uzun süreler içerisinde gerçekleştirilmektedir. Ayrıca dijital veri üzerinde yapılacak aramalar ve elde edilen bulgular, ne kadar süre geçerse geçsin aynı yöntem ve aynı versiyon yazılım ve donanımlar kullanıldığı taktirde aynı sonucu verecek şekilde doğrulanabilir olmalıdır. Bu nedenle bilişim sistemi üzerindeki aramada ilerleyen bölümlerde detaylandırılacak olan delil zincirinin takip edildiği ve ilerisi bir adım olarak gerekli düzenlemeler ile sağlandığı taktirde böyle bir hazır bulunma durumuna gerek yoktur.

Birinci fıkra kapsamında irdelenebilecek bir diğer hukuki kavram ise “rıza” kavramıdır. Bu madde özellikle dijital materyallerin incelenmesi için düzenlenmiştir. Dijital materyallere özel olarak kanun koyucunun bu maddeyi ortaya koyduğu görülmesine karşın, bahsi geçen hukuki adımlar diğer kanun maddelerine benzetilerek esnetilmeye veya katılaştırılmaya çalışılmaktadır. Örneğin el koyma durumu CMK 127 maddesinde de geçmesinin yanında daha önce de bahsedilen dijital verilerin

hassasiyetinden dolayı arama, el koyma ve ilgili diğer işlemler başka bir kanun maddesine atıfta bulunmaksızın dijital veriye özel olarak CMK 134. Maddesinde düzenlenmiştir. Burada sakıncalı durum esnetilme durumudur. Bu bağlamda dijital verilerde de "rızaen arama" ve "ilgilinin rızası" kavramı zaman içerisinde gündeme getirilmiştir. Bilindiği üzere Adli ve Önleme Aramaları Yönetmeliği'nin 8 inci maddesinin (a) ve (c) bentleri ile (f) bendindeki "ilgilinin rızası ile" ibaresi kuvvetli gerekçelerle kişilerin ve haklarının korunması yönünde Danıştay 10. Dairesinin 13.03.2007 tarih, 2005/6392 Esas ve 2007/948 Karar sayılı kararı ile iptal edilmiştir. Aynı şekilde dijital veri incelemesinde müşteki başvurusu olması, soruşturma ve kovuşturma durumlarında adli talimat olmaması, idari soruşturma ile idarenin kendi bilişim sistemlerini inceletmek istemesi durumlarında gerekli prosedür yerine getirilmeden şüpheli veya müşteki kişilerin salt rızası adli bilişim inceleme işleri için kesinlikle kabul edilmemelidir. EGM SSMDB hukuk kurallarını bu yönde uygulamaktadır.

6526 Sayılı kanun ile birinci fıkraya "somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve" ibaresinin eklenmesinin dijital verinin hassasiyeti, kişilerin anayasal haklarının ihlal edilmemesi ve keyfiyetin önlenmesi açılarından yerinde bir ekleme olduğu değerlendirilmektedir. Bunun yanında 7145 Sayılı kanun ile birinci fıkrada gerçekleştirilen değişiklik Anayasa'ya uygunluk ve uygulamadaki yansıması açısından bölüm sonunda irdelenecektir.

3.2.1.4. CMK 134. Maddesinin İkinci Fıkrasının Değerlendirilmesi

İkinci fıkrada dijital materyale el konulma şartı olarak 7145 Sayılı kanunun kabul edilmesine kadar şifrenin çözülememesi veya gizlenmiş bilgiye ulaşılamaması gösterilmiştir. 7145 Sayılı Kanunun kabul edilmesi ile el koymaya dayanak olarak işlemin uzun sürecek olması eklenmiştir. Bir sonraki bölümde bahsedileceği üzere CMK 134. Maddesi üçüncü fıkrasında el koyma esnasında verilerin yedeğinin alınması hükmü bulunmaktadır. İkinci fıkrada bahsedildiği şekilde şifreli veya gizlenmiş dahi olsa verilerin yedekleme imkânı bulunabilecekken el koymaya işlemin

uzun sürmesinden dolayı karar verildiyse yedek almaya çalışmak mantık hatası olacaktır. Bununla birlikte olay yerinde adli kopya alma işlemi teknik imkânsızlık ve güvenlik gibi sebeplerle her zaman gerçekleştirilemeyebilir.

Şifrenin çözülememesi veya gizlenmiş bilgiye ulaşılamadığı tespiti ise canlı inceleme yapıldığı durumda ortaya çıkacaktır. Ancak ülkemizde genel uygulamada canlı incelemeden ziyade alınan imaj (adli kopya) üzerinden inceleme yapmak esastır. Fakat çoğu zaman dijital materyaldeki verinin tamamının çıkarımının yapılması ile sonuçlandırılan bu yöntem ile zaman ve para kaybı yaşanmakta, kolluk ve adli süreç bu durumdan olumsuz etkilenmektedir. Aynı zamanda örneğin kelime listesi araması gibi bir süzgeçten geçirilmeden gerekli gereksiz tüm verinin çıkartılması (export edilmesi) yaklaşımı artık dünya standartlarında da geçerliliğini yitirmeye başlayan bir yöntemdir. Zira canlı inceleme genellikle sistem açıkken gerçekleştirilen inceleme olması nedeniyle yeterince uzman olmayan kişilerce uygulandığı takdirde yazma koruma kullanılmaması, hatalı şekilde dosyalara ya da materyale erişim sağlanması gibi nedenlerden dolayı dosyaların tarih saat değişimleri, uçucu verinin kaybı, materyallerin çalışmaz hale gelmesi gibi önemli sıkıntılara sebebiyet verebilecektir.

Yine sistem kapalı olsa dahi olay yerindeki bilişim sistemi üzerinde yedeği ilk etapta alınmaksızın yazma koruma gibi gerekli önlemler alınmak suretiyle inceleme yapmak da canlı inceleme olarak değerlendirilebilir. Bununla birlikte örneğin devasa sistemlerde adli kopya alma işleminin maliyet ve zaman açısından efektif olmayacağı, bulut ve sanal sistemlerde verilerin dağınık olmasının ek zorluklar getirebileceği veya sistem kapandığında güçlü şifreleme ile karşılaşılabileceği gibi durumlar göz önünde bulundurularak canlı incelemeye de imkân tanınmalıdır. Ancak ehil olmayan, yeterli eğitimi almamış ve tecrübesi olmayan kişilerin kesinlikle canlı inceleme yapmaması delil güvenilirliği ve bütünlüğü açısından önemlidir.

Ek olarak el konulma şartları arasına sayılan kriterlerin tekrar değerlendirilmesinin gerekli olduğu görülmekle beraber işlemin yapıldığı ortamın güvenliği ve isnat edilen suçun ağırlığı gibi kriterlerin de eklenmesinin daha uygun olacağı değerlendirilmektedir. Örnek olarak hali hazırda ilgili kanun maddesine göre

terör ve çocuk istismarı suçlarında dahi el konulan dijital materyal adli kopyası alınır alınmaz bu adli kopya ile birlikte gecikmeksizin şüpheliye veya vekiline iade edilmek durumundadır. Muhtemel suç verisi bu durumda çoğaltılarak suç şüphelisine verilmektedir. Kişilerin günlük hayatlarını devam ettirmeleri ve kurum veya şirketlerin faaliyetlerini sürdürmeleri açısından bu iade işlemi faydalı olabilir. İade işlemine karar verilmesi için dijital materyal ve barındırdığı verinin derhal sınıflandırılması önemlidir. Bunu en etkin şekilde sağlamak için de ileride daha ayrıntılı olarak bahsedilecek olan "dijital triage" ya da kısaca triage adı verilen ve zaman kritik konularda soruşturma konusu ile en çok ilgili olan dijital verinin ve materyalin önceliklendirilmesi şeklinde tanımlanabilecek adli bilişim işlemi için hukuki zemin hazırlanabilir (Marturana, 2014). Örneğin "Çocukların Kullanıldığı Müstehcen Ürünleri Ülkeye Sokma, Çoğaltma, Satma, Depolama, Bulundurma ve Kullanıma Sunma Suçu (TCK 226/3-ikinci cümle)" adlı suçun tespiti çoğunlukla resim ve video gibi görsellerin bulundurulmasının ya da gönderilmesinin ispatlanması ile gerçekleştirilmektedir. Bu olayda triage işlemi uygulanarak bahse konu görsellerin bulunabileceği dizinler öncelikli olarak aranarak ilgili dosyalar toplanmak suretiyle değerlendirilebilir.

3.2.1.5. CMK 134. Maddesinin Üçüncü Fıkrasının Değerlendirilmesi

Üçüncü fıkrada el koyma işlemi sırasında verilerin bir yedeğinin alınacağı söylenmektedir. Verilerin yedekleri kısmen veya tamamen adli kopyasının alınması sureti ile elde edilmektedir. Ancak teknik imkanlar açısından adli kopyanın laboratuvarda alınması daha sağlıklı olmaktadır. Bunun yanında bir yandan zaten el koyma yapılacağından diğer yandan da olay yerinde geçirilen sürenin kısaltılması açısından işlem yapılacak bilişim sisteminin uygun şekilde muhafaza edilmesiyle laboratuvarda gerekli işlemlerin yapılması daha pratik ve uygun olacaktır. İkinci fıkrada işlemin uzun sürmesinden dolayı bir el koyma durumunda dahi daha önce belirtildiği gibi yedek alınması zorunlu olarak anlaşılmaktadır. Burada bir düzeltme yapmak gerektiği görülmektedir. Bununla birlikte daha önce bahsedildiği üzere büyük veri, bulut veri, kişilerin konutlarındaki diğer kişilerin günlük yaşantılarını sekteye

uğratma veya şirketin ticari faaliyetlerinin devam etmesi gerekliği gibi durumlar söz konusu olduğunda belirli bölümlere el koyma veya uygun görülen belirli bölümlerin yedeklerinin alınması için bir takdir yetkisi makamı belirlenmesi uygun olacaktır.

3.2.1.6. CMK 134. Maddesinin Dördüncü Fıkrasının Değerlendirilmesi

Dördüncü fıkrada ise öncesinde istemesi halinde verilmesi söz konusu iken 21.2.2014 tarihli 6526 Sayılı Kanunun 11 maddesi doğrultusunda gerçekleştirilen değişiklik ile alınan adli kopyanın bir suretinin şüpheliye veya vekiline verilmesi şart koşulmuştur. Bunun yanında adli kopyası alınan bilişim sistemi de gecikmeksizin şüpheliye iade edilmektedir. Bu durum çocuk istismarı, terör, kredi kartı kopyalma ve organize suç gibi çok ciddi konularda suç unsuru verinin çoğaltılması ve şüphelide kalması durumuna yol açmaktadır. Örneğin çocuk istismarı soruşturmasında suç konusu bilişim sistemine el konulmayıp bir kopyasının da şüpheliye verilmesi durumunda içerisindeki hassas çocuk görselleri yayılmaya devam edebilecektir. Uygulama bu şekilde yapıldığında suçla mücadelenin önleme amacının sakatlandığı değerlendirilmektedir. Özellikle şüphelinin veya vekilinin huzurunda alınan adli kopyanın bir kopyasının verilmesi yerine alınan adli kopyanın hash bilgisini de içeren imaj alma tutanağının verilmesi yeterli olacaktır. Gerçekleştirilen yurtdışı ziyaretlerinde alınan bilgiler doğrultusunda Amerika Birleşik Devletleri (ABD), Almanya ve İngiltere gibi gelişmiş ülkelerde gerçekleştirilen adli bilişim işlemlerinde mahkemeler daha çok prosedürlerin nasıl uygulandığına, mevcut adımların doğru uygulanıp uygulanmadığına ve delil zincirinin bozulup bozulmadığına resmi evrakları ve inceleme raporlarını inceleyerek kanaat getirdikleri söylenebilir. Doğaldır ki öngörülemeyen ancak adli bilişim işlemleri esnasında ilk defa veya normalden farklı olarak uygulanacak olan teknik işlemler olabilir. Bunun gerekliliğinin raporlanması ve bulgu verinin güvenilirliğini ve bütünlüğünü koruyarak gerçekleştirilen işlemlerin ayrıntılı olarak dokümante edilmesi durumunda mahkeme bu işlemleri olumlu yönde kabul etmektedir. Sayılan ülkelere ek olarak kolluk kuvvetlerine yönelik Polonya'da gerçekleştirilen uluslararası bir eğitimde alınan bilgiler doğrultusunda, el konulan

dijital materyalin özellikle suç hakkında kuvvetli şüphe olduğu durumlarda şüpheliye veya vekiline verilmesi söz konusu olmadığı görülmüştür (CEPOL, 2016).

Adli bilişim inceleme konusu olmuş dijital verinin bütünlüğünü, değiştirilmediğini ve güvenilirliğini göstermekte kullanılan en yaygın ve önemli yöntem ise hash adı verilen algoritmaların kullanılmasıdır. Hash bilgisi Türkçe'de "veri özeti" olarak tanımlanabilir. Hash, belli bir verinin tanımlanmış algoritmalar ile tek yönlü olarak matematiksel işleme sokulması sonucu elde edilen özet veridir. MD5, SHA1 ve SHA256 çeşitli hash algoritmalarıdır. Hash'leme işleminin tek yönlü olması demek özet veriden özeti alınan veriye ulaşılamaması anlamına gelmektedir ve bu yönden içerik veriye ulaşılmaması sağlanmış olur. Örnek olarak MD5 algoritması kullanılarak elde edilen hash verisi 32 karakterlidir. A dijital verisinin MD5 hash'i de alınsa, yüzlerce A dijital verisinin yan yana geldiği veri topluluğunun MD5 hash'i alınsa da özet veri olarak 32 karakterli bir sonuç elde edilir. Bu veri içerisinde, en küçük veri birimi olan 1 bit veri bile değiştirilse elde edilen hash değeri değişecektir. Sonuç olarak hash bilgisi; incelenen veri veya adli kopyanın içerisinde veri değişip değişmediğinin kanıtı olacaktır. Hash olgusu ilerleyen bölümlerde daha detaylı olarak irdelenecek olup, mobil cihaz adli bilişimi yönünden de değerlendirilecektir. Bu fıkranın, şahısların günlük yaşamlarının sağlıklı olarak devam edebilmesi, ticari işlemlerin devam edebilmesi gibi konular değerlendirilerek Cumhuriyet savcılarının inisiyatifine bırakılması yönünde düzenlenmesinin daha uygun olacağı değerlendirilmektedir. Örneğin şüphelinin adli kopya içerisinde tez çalışmasının bulunduğu bir durumda talep etmesi halinde Cumhuriyet Savcısı talimatı ile bu veriler kendisine tutanakla verilebilir. Burada kolluk kuvvetinin yoğunluğunun da dikkate alınması ve talebe ilişkin talimatın adli süreci etkilemeyecek şekilde uygulanmasının faydalı olacağı değerlendirilmektedir.

3.2.1.7. CMK 134. Maddesinin Beşinci Fıkrasının Değerlendirilmesi

Beşinci fıkrada ilgili bilişim sistemindeki verinin el koymaksızın da tamamının veya bir kısmının yedeğinin alınabileceği belirtilmiştir. Uygulamada genellikle bu

madde işletilmektedir ve sistemin tamamının adli kopyası olay yerinde alınmaktadır. "*Kopyası alınan verilerin kağıda yazdırılması"* ifadesinin yerine ise *"adli kopya alma işlemi tutanağa yazılır"* ifadesinin kullanılmasının uygun olacağı değerlendirilmektedir. Alınan veriler içerisinde yüzlerce dosya olma ihtimali mevcuttur ve bu dosyaların sadece isimlerini bile kağıda yazdırmak faydasız olduğu kadar zaman kaybı da olacaktır. Bunun yerine tanımlayıcı teknik detayları, işlem zamanı, mekanı ve hash bilgisi gibi bilgileri içeren "imaj alma tutanağı" yeterli olmalıdır.

3.2.2. Bilişim Sisteminin Tespiti

Adli bilişim yöntemleriyle incelemesi yapılacak olan bilişim sisteminin tespiti işlemi dijital materyallere ilk müdahale işlemlerinin başlangıcıdır. Uygulanan adımları, olay yerinin durumunu, tespit edilen cihazları, gerekli özelliklerini ve özellikle normalin dışında gelişen hususları kayıt altına almak yani dokümante etmek önceki bölümde değinildiği gibi çok önemlidir. Dokümante işlemi ülkemizde tutanak ve rapor halinde gerçekleştirilmektedir. Bununla birlikte olay yeri fotoğrafları ve işlemin video olarak kayıt alınması ile dokümante işleminin kuvvetlendirilmesi adli süreç açısından faydalı olacaktır. Öyle ki; dünya genelinde mahkemelerdeki hakimler teknik olarak anlamadıkları hususlarda dahi iyi dokümante edilmiş bir adli bilişim incelemesini bu sağlıklı dokümanları inceleyerek isabetli kanaatler getirebilmektedirler.

Adli talimat alındıktan sonra eğitimi ve tecrübesi olmasının önemi daha önce vurgulanan yetkili ve uzman personel tarafından veri içerebilecek bilişim sistemlerinin tespiti yapılır. Bu işlemin yetkili ve uzman personel veya kişilerce yapılmaması durumunda sistemin zarar görmesi, verinin kaybedilmesi veya teknik bilgi yetersizliğinden alakasız cihazların muhafaza edilerek gereksiz işleme sebebiyet verilmesi gibi durumlarla (seyyar şarj aletine (powerbank) el konulması) karşılaşılmaktadır. National Institute of Standards and Technology (NIST) adı verilen ve fiziksel bilim laboratuvarı niteliğinde olup laboratuvarlar için standartları tespit

eden bir kuruluşun yayınladığı belgeye göre, el koyma esnasındaki yanlış prosedürler ve uygun olmayan bulgu elde etme adımları, dijital verinin kaybına yol açabilmektedir (Ayers ve ark, 2014:27). Hukuki sorumluluk getirecek bu olumsuz durumlar yine iş akışı ve standartların uygulanması ile önlenmiş olacaktır.

Tespit edilen bilişim sistemleri mümkünse seri numarası ve "International Mobile Equipment Identity" (IMEI) numarası gibi belirleyici ve benzersiz özellikler ile birlikte kayıt altına alınmalıdır. Benzersiz tanımlayıcısı bulunmayan bilişim sistemleri kaydı için görüntüleme ve üzerindeki diğer yazı ve şekilleri kayıt altına alma işlemi uygulanabilir.

Tespit işlemi sırasında bilişim sistemleri üzerinden diğer vücut ve adli manadaki kalıntılar (parmak izi, kan, vücut sıvısı vb.) elde edilebileceğinden bu hususlar hakkında da eğitimli olunması ve eldiven giyme gibi gerekli tedbirlerin alınması sağlıklı bir adli süreç açısından uygun olacaktır.

3.2.3. Bulgunun Muhafaza Altına Alınması

Başlıktan anlaşılması gereken, gerekli işlemin gerçekleştirilmesi adına saklanmak veya taşınmak amaçlı olarak bilişim sisteminin uygun şekilde koruma altına alınması, el konulması ya da adli kopyasının çıkarılarak tespit edilmesidir. O CMK 123. Maddesinde “İspat aracı olarak yararlı görülen malvarlığı değerleri, muhafaza altına alınır” hükmü bulunmaktadır. Olay yerinde bilişim sistemlerinin tespiti yapıldıktan sonra işlemin uzun sürüp sürmeyeceği veya şifre bulunup bulunmaması gibi durumlar bu aşamada bilinmediğinden el koyma işlemi başlamamış ancak bilişim sistemi ve dijital veri üzerinde kolluğun veya görevlinin tasarrufu başlamıştır. Bu nedenle bu safha muhafaza altına alma olarak isimlendirilmiştir.

Olay yerine gidilmeden önce mümkün olan bütün araç, gereç ve yazılımlar hazır edilmelidir. Bu araç gereç ve yazılımlardan özellikle mobil cihazlar için

kullanılabilecek olanlar ilerleyen bölümlerde anlatılacaktır. Ek olarak mümkünse taşınabilir bir yazıcı bulundurulması faydalı olacaktır.

Olay yerine gidildiğinde öncelikli olarak sigortaların indirilmesi suretiyle kasten elektriğin kesilmesine karşı önlem alınmalıdır. Açık olan bir bilgisayar tespit edilirse bazı bilgilerin kontrol edilmesi ve canlı olarak uçucu verilerin alınması gerekir. Bilgisayar o anda bir silme işlemi yürütüyor olabilir, bulgu veri olarak değerlendirilebilecek başka bir ağa bağlı olabilir veya kapattıktan sonra şifreli olarak incelemecinin karşısına çıkabilecek bir sürücüye ya da veriye sahip olabilir. Bu nedenle kapatılmadan önce bahse konu uçucu verilerin uygun şekilde ve dokümante edilerek kaydı yapılmalıdır. Bu konu ile ilgili ek detay bilgiler ilerleyen safhalarda verilecektir.

Bununla birlikte şifrenin çözülememesi durumunda ya da işlemin uzun sürecek olması durumu tespit edildiğinde kanun gereği el koyma işlemi uygulanır ve bilişim sistemleri zarar görmeyecek şekilde bulgu poşetlerine veya korumalı ve mühürlü kutulara konur.

Olay yerinden laboratuvara veya laboratuvardan ilgili birimlere bilişim sistemlerinin taşınması esnasında hem zarar görmemesi hem de taşıma esnasında müdahale edilmediğinin gösterilmesi için ağzı kapatıldıktan sonra tekrar açıldığı belli olacak bulgu poşetlerine konmalıdır. Bulgu poşetlerinin içerisinde bilişim sistemini belli darbelere karşı koruyabilecek koruyucu materyal bulunmalıdır. Bu materyal mümkünse anti-statik özelliği olan bir maddeden üretilmiş olmalıdır. Ek güvenlik önlemi olarak ağzı kapanan bulgu poşetlerinin kapanma kısımlarına üzerlerinde başka bir kurumda ya da ilde bulunmasının mümkün olmadığı seri numarası yazılı olan mühür bantları kullanılmalıdır. Bilişim sisteminin güvenli taşınması ve saklanması için Radio Frequency Identification (RFID, Radyo Frekansı ile Tanımlama)**,** sert ve şifreli kutularda taşıma vb. birçok yöntem ve materyal kullanılabilir. Ancak bahsedilen bulgu poşeti ve mühür bandı kullanımı maaliyet-fayda açısından kurumlar için en uygun olanı olarak gösterilebilir. Kimi zaman ise bilişim sistemlerinin, adli kopyalarının veya export edildiği depolama birimlerinin kargo ile gönderilmesi gerekebilmektedir. Bu durumda sarsılma ve darbeler ile güvenlik hususları hesaba

katılarak uygun şekilde kapatılması ve paketlenmesi gerekmektedir. Kargo firmasında böyle bir imkân olması durumunda hassas taşıma olduğunun bildirilmesi uygun olacaktır.

3.2.4. İnceleme ve Analiz

Adli bilişim incelemelerinde en sık görülen durum Cumhuriyet başsavcılığının bizzat atadığı veya belirlediği kurumun görevlendirdiği uzman personel tarafından gerçekleştirilmesidir. Bu işlemler ayrıca mahkemenin belirleyeceği ya da şüphelinin ticari olarak kiralayabileceği bilirkişiler tarafından da yerine getirilebilir. Önemli olan gerçekleştirilen işlemlerin ve hazırlanan raporun mahkeme veya hakim tarafından kabul görmesidir. Adli bilişim bahsedilen multidisipliner özelliğinden dolayı sadece teknik konulara hakim olmak yeterli değildir. Bunun bir diğer sebebi de doğası gereği adli bilişim incelemelerinde sadece hackleme, zararlı yazılım tespiti gibi siber suçların araştırılmaması, teknik yönü olmayan birçok farklı suçun da bu incelemelerde tespit edilmeye çalışılmasıdır. Diğer bir deyişle dünya literatüründeki tanımlama kullanılırsa hem siber suç hem de siber etkin suçlar da adli bilişim konusudur. Siber suç siber ortam kullanılmadan işlenemeyecek suçlar olarak tanımlanırken, siber etkin suç ise siber ortamın (bilişim sistemi, İnternet vb.) aracı olarak kullanıldığı suçlar olarak tanımlanmaktadır.

İncelemecinin adli bilişim alanında gerekli eğitimleri almış olması yetkinliği açısından önemlidir (Jones and Valli, 2008). Yetkinlik, sertifika ve alandaki tecrübe önemlidir. Öyle ki Hukuk İşleri Genel Müdürlüğü Bilirkişilik Daire Başkanlığı'nın 6754 Sayılı Bilirkişilik Kanunu 10. Maddesi doğrultusunda bilirkişi olabilmek için duyurmuş olduğu şartlar arasına hukuk ve prosedür temel bilgisinin verildiği bilirkişilik temel eğitimini tamamlamak ve bilirkişilik yapacağı uzmanlık alanında en az beş yıl fiilen çalışmış olmak şartlarının getirildiği görülmektedir. Kanun düzenlemesi ile adli bilişimde yetkinlik, eğitim ve alan tecrübesinin gerekliliği vurgulanmıştır.

İnceleme yapacak uzman personelin aynı zamanda hukuk bilgisine ve isnat edilen suç hakkında bu suça ilişkin bulguları tespit edebilecek kadar adli bilgiye sahip

olması beklenmelidir. Ayrıca bir HDD (harddisk) incelemesi ile cep telefonu incelemesi hususu ile bozuk bilişim sisteminden veri kurtarılarak incelenmesi hususları birbirinden ayrı uzmanlık alanlarıdır. Bu nedenle bilirkişi veya adli bilişim uzmanı olarak dosyalara atanacak görevlilerin yeterli eğitim ve tecrübeye sahip olup olmadığı da Cumhuriyet başsavcılıkları tarafından göz önünde bulundurulmalıdır.

Ayrıca inceleme ve analiz kelimeleri adli bilişim ve suç tespiti açısından farklı anlamları ve alanları karşılamaktadır. Adli bilişimde inceleme tabiri, veriye ulaşılarak bu dijital verinin okunabilir hale getirilmesi, şifrenin kırılması, teknik yöntemler kullanılarak verilerin kurtarılması ve gerekli teknik aramaların yapılması gibi yöntemleri karşılamaktadır. Analiz ise tespit edilmiş verilerin ilişkilendirilerek suç ve suçlu ile olan bağlarının ortaya çıkarılması işlemidir. Bu açıdan ayrı bir uzmanlık alanı olması sebebiyle analiz konusu adli bilişimin dışında görülmeli ve uzmanları tarafından gerçekleştirilmelidir.

İnceleme raporları ve adli bilişimden elde edilecek suç verilerinin ülke genelinde korelasyon yöntemi kullanılarak analiz edilmesi suçla mücadele açısından elzemdir. Ancak bu ihtiyaç beyan edilirken, elde edilen verilerin bu çalışma ile belirtilmiş kriter ilkelere uygun şekilde elde edilmiş olması ve mahkeme tarafından bu analize izin verilmiş olması gerektiği düşünülmektedir. Bununla birlikte burada verilmesi gereken izin bahsinden, CMK 134. Maddesi tedbiri uygulanan kişinin 3. şahıslarla ilgili içerik verisi içermeyen eposta adresi, rehberi, sosyal medya hesapları vb. verilerin analizi için verilen izin telakki edilmelidir. Bu raporlar hem şüpheliye hem de üçüncü kişilere ait özel ve kişisel veriler içerebileceğinden mümkün olduğu kadar iyi korunmalı, ilgisiz ve yetkisiz erişime kapalı olmalı ve adli özelliği olmayan sorgular dışında tutulmalıdır. Bu hususlara dikkat edilmediği taktirde Anayasa ihlalleri ile karşılaşma durumu olabilecektir.

3.2.5. Raporlama ve Adli Makamlara Sunum

Bahse konu safhalardaki raporlama aşaması adli bilişimin önemli safhalarından birisidir. Adli bilişim inceleme işlemleri için belirlenmiş ve delil zincirini destekleyen bir raporlama formatı, özellikle incelemecilerin bir davada uzman tanık olması gerektiğinde çok kritik olabilir. (Hewling, 2013:106) EGM SSMDB başta olmak üzere EGM Kaçakçılık ve Organize Suçlarla Mücadele Dairesi Başkanlığı, Kriminal Dairesi Başkanlığı, Jandarma Genel Komutanlığı KOM Daire Başkanlığı ve Adli Tıp Adli Bilişim İhtisas Dairelerinde adli bilişim incelemeleri gerçekleştirilmektedir. Basına yansıyan ve daha önce bazı tez çalışmalarında da sunulmuş olan bilgiler doğrultusunda rapor isimlerinin kurum bazlı olarak bilirkişi raporu, inceleme raporu, teknik çıkarım raporu gibi başlıklarla adlandırıldığı görülmektedir. Çalışma devamında verilen bilgiler daha çok delil zincirine destek olacak bir rapor içeriğinde bulunması gereken bilgiler olarak sunulmuştur.

Bilişim incelemeleri sonucunda bir "inceleme raporu" oluşturulur. İnceleme raporundan farklı olarak verilerin tespit edilerek okunabilir hale getirildiği, analiz işlemlerinden ziyade teknik aramaların yapıldığı ve değerlendirmenin başka bir uzmana, bilirkişiye ve/veya soruşturmacı birim veya makama bırakıldığı, işlem tarihi, hash bilgisi, izlenen süreç, tespit edilen veriler, rapor tarihi vb. genel bilgileri içeren ev inceleme raporuna kıyasla daha yüzeysel fakat pratik denebilecek Teknik Çıkarım (Export) Raporu isimli bir rapor hazırlamak da mümkündür. Bu nedenle rapor özelinde teknik çıkarım raporunda inceleme raporuna göre bulgu veriye ait daha az veri belirtilir.

139 katılımcısının 135'nin adli bilişim araçları ile aşina olduğu ve 104'ünün adli bilişim alanında 5 yıldan fazla deneyimi bulunduğu bir anket çalışmasında incelemeye konu olan dosyaya (vaka, inceleme) ait bilgiler, bulgu kaynak bilgisi (adli kopya), bulgu veri ve delil zincirine ait verilerden hangilerinin mutlaka belirtilmesi gerektiği araştırılmıştır (Bariki ve ark, 2010). Araştırma sonuçlarına göre bu 4 bölümün içermesi gereken bilgiler Çizelge 3.1, 3.2, 3.3 ve 3.4'te verilmiştir.

Çizelge 3.1 Araştırma sonuçlarına göre dosyalara ait belirtilmesi gereken bilgiler (Bariki ve ark, 2010)

	A. Dosya Bilgisi
1	Dosya numarası
2	Dosya ismi
3	Dosya tanımı
4	Rapor oluşturma tarihi
5	Adli bilişim aracı ismi ve versiyonu
6	Adli bilişim görevlisi (bilirkişi, uzman vb.) bilgisi (isim, kurum, adres, telefon, fax, eposta, yorumlar)
7	Adli soruşturmacı bilgisi (isim, kurum, adres, telefon, fax, eposta, yorumlar)

Çizelge 3.2 Araştırma sonuçlarına göre bulgu adli kopyaya ait belirtilmesi gereken bilgiler (Bariki ve ark, 2010)

	B. Bulgu Kaynak Bilgisi (Adli kopya)
1	Bulgu dosya ismi
2	Bulgu dosya yolu
3	Bulgu dosya çeşidi
4	Bulgu dosya boyutu
5	Bulgu dosya hash (checksum)
6	Sistem zamanı
7	Bulgu kaynağı ile kullanılan yazma-koruma metodu
8	Kullanıcı bilgileri
9	İşletim sistemi versiyonu
10	Dosya sistemi
11	Bölümlerin (Partition)bilgisi
12	Kullanımdaki şifreleme

Çizelge 3.3 Araştırma sonuçlarına göre bulgu veriye ait bulunması gereken bilgiler (Bariki ve ark, 2010)

C. Bulgu (veri)	
1	Dosya ismi
2	Dosya yolu
3	Dosya çeşidi
4	Dosya mantıksal boyutu
5	Dosya fiziksel boyutu
6	Hash (Checksum)
7	Oluşturulma tarihi
8	Değiştirilme tarihi
9	Erişim tarihi
10	Sektör bilgisi
11	Cluster bilgisi
12	Silinmiş mi?
13	Gizlenmiş mi?
14	Ayrılmamış alanda mı?
15	Offset bilgisi
16	Notlar

Çizelge 3.4 Araştırma sonuçlarına göre delil zinciri açısından bulunması gereken bilgiler (Bariki ve ark, 2010)

	D. Delil Zinciri
1	Tarih
2	Nereden alındı / el konuldu
3	Kim tarafından alındı / el konuldu
4	Edinme sebebi
5	Alındığı yerin lokasyonu
6	Bulgunun tanımı
7	Zincirdeki değişim kaydı (değişimin sebebi, transfer metodu, kim tarafından gerçekleştirildiği, tarih, kim tarafından alındı, alınma tarihi, hash bilgisi)

Çizelge 3.1, 3.2, 3.3 ve 3.4 incelendiğinde bir adli bilişim inceleme raporunda bulunması gereken temel bilgiler görülmektedir. Özetlemek gerekirse inceleme raporu asgari olarak adli talimat bilgilerini, incelenen bilişim sisteminin teknik özelliklerini, hash bilgisini, kullanılan yöntemleri, kullanılan araçların versiyon bilgilerini, değerlendirilen verilerin kaynak değerlendirmesini, üst verileri, veri yollarını, şüpheli bilgisini, incelemeyi talep eden makamı, inceleme sürecini, tarihi, sonuç ve değerlendirme kısmını ve inceleyen uzman bilgilerini içermelidir. Bu bilgilerin bulundurulması incelemenin mahkeme önünde güvenilirliğini artırmaktadır ve delil zincirini destekleyici niteliktedir. Örnek olarak EGM SSMDB inceleme ve teknik çıkarım raporları asgari bu bilgileri içermektedir.

Raporun dili kesinlikle mümkün olduğu kadar açıklayıcı olmalı, incelemeci tarafından ihtiyaç duyulacağı hissediliyor ise giriş kısmına rapor içeriğindeki teknik terimleri ve ifadeleri anlaşılır hale getirebilecek bir sözlük konmalıdır. Tespit edilen bulgu veriler dışında kişisel yorumlara yer verilmemelidir ve somut ifadeler kullanılmalıdır. Kullanılan yazılım ve donanımlar ile bunların sürümlerini inceleme süreci kısmında belirtmek de ayrıca bulgunun güvenilirliği ve doğrulanabilirliği

açısından da önemlidir. Öyle ki dijital dünyada gerçekleştirilen teknik işlemlerin doğası gereği bir yazılım dünya standartlarında olsa dahi teknolojik gelişmeler veya geliştirici hatalarından dolayı bir sürümünde tespit ettiği veriyi diğer sürümünde edemeyebilmektedir. Diğer yandan ticari olarak lisans süresi dâhilinde satılan bazı yazılım ve donanımlar lisans süreleri bitse de güncelleme almamak koşuluyla lisans süresinin dolduğu tarih veya önceki sürümlerinde çalışabilmektedir. Avrupa Birliği ve bağlı ülke kolluk kuvvetlerinde genel görüş, açık kaynak dahi olsa güncelleme alan inceleme yazılımının incelemelerde kullanılmasının yeğlenmesi gerektiği yönündedir. Fakat yazılım güncelleme almasa dahi bir veri açıklanabilecek şekilde tespit edebiliyor ve doğrulanabiliyor ise herhangi bir sorun çıkması beklenmemelidir. Sorun çıkma durumu tespit edilemeyen veriler için söz konusu olabilecektir. Bu durumda da adli bilişimin temel mantıklarından olan tek yazılım veya donanıma bağımlı kalmama, mümkünse muadilini de doğrulama amaçlı olarak bulundurma ilkesi işletilebilir. İkinci bir yazılım veya donanım ile inceleme işleminin tekrarlanması sonucu işlem doğrulaması gerçekleştirilmiş ve mahkeme önündeki güvenilirlik artırılmış olacaktır. Doğaldır ki her olay için iki araçla birden doğrulama yapmak efektif değildir. Bu seçenek teknik ve adli tecrübe açısından ihtiyaç duyulduğunda işletilmelidir. Ancak, teknik olarak tam karar verilemeyen durumlar raporda belirtilerek soruşturmacı makam veya birimin değerlendirmesine bırakılır. Soruşturmacı makam veya birim bu durumu farklı bir bilirkişiye veya uzmana değerlendirmesi için havale edebilir.

Teknik zorluklar veya detaylı inceleme ihtiyacından dolayı adli bilişim inceleme süreci zaman zaman uzayabilir. Bununla birlikte süreç esnasında herhangi bir inceleme safhasında incelemeci tarafından soruşturmada veya kovuşturmada faydalı olabilecek ve acilen ilgili makama iletilmesi gereken tespitler gerçekleştirilmiş olabilir. Diğer bulguların da tespit edilmesi açısından adli bilişim incelemesine devam edilmesi gereken bu durumda ara rapor mahiyetinde bir rapor hazırlanır ve bu rapora "Ön İnceleme Raporu" adı verilir. Ön İnceleme Raporunda mevcut durum ve tespitler belirtilerek işlemin devam ettiği vurgulanır.

Doğal olarak bu raporlarda da maddi hatalar veya sehven sebep olunmuş hatalar görülebilir. Bilirkişinin Hukuki Sorumluluğu başlıklı Hukuk Muhakemeleri Kanunu

(HMK) 285. Maddesi değerlendirilirse gerçeğe aykırılık bilirkişinin kasti veya ağır ihmalinden kaynaklanmıyorsa cezai sorumluluğu olmayacaktır. Adli bilişim incelemesi bilirkişi sıfatı ile atanmamış olsa bile adli bilişim uzmanları veya adli bilişim görevlisi gibi benzer isimlerle anılan kişiler ya da görevlilerce de gerçekleştirilmektedir. Örneğin kolluk kuvvetlerinde görev yapan adli bilişim incelemecileri birçok olayda bu sınıftadır. Bu bilgiden hareketle adli talimat ile görevlendirilmiş incelemeci uzmanlardan hukuka uygun şekilde inceleme yapmaları beklenmekle birlikte bu kanun maddesi çerçevesinde değerlendirilmelidir. Adli bilişim incelemesi gerçekleştirilirken raporda bir yanlışlık yapıldığı taktirde adli süreç içerisinde bu raporun düzeltilmesi talep edilmektedir. Bu durumda ilk hazırlanmış rapor üzerinde değişiklik yapılıp gönderilme işlemi kesinlikle uygulanmamalı, hatayı da belirtecek şekilde bir "ek rapor" düzenlenmelidir. Raporun her sayfası paraflanır ve son sayfası inceleyen uzmanın bilgisi bulunmak suretiyle imza altına alınır. İmzalanmış ve adli sürece dahil edilmiş bir raporun orijinali kesinlikle değiştirilmemelidir. Bu durum tespit edilmiş bulgulara gölde düşürebileceğinden delil niteliklerini kaybetmelerine sebep olabilecektir. Özellikle adli bilişim incelemesinde suç verisinin tespiti için incelemecinin hukuk ve suçla ilgili bilgisinin de olması beklense de bulgunun ve raporun değerlendirilmesi adli ve/veya soruşturmacı birim veya kurumlarca yapılmak üzere kendilerine bırakılır. Bununla birlikte doğrudan uzmanlık alanlarına giren konularda, örneğin siber suç olup teknik hususlar içeren suç verilerinin raporlanması aşamasında adli bilişim uzmanları tespit ettikleri teknik konularda daha kesin ifade kullanmalıdırlar. Bilişim dünyasının doğası gereği pozitif veya negatif şeklinde kesin olarak belirtilemeyecek durumlarla karşılaşmak olasıdır. Bu durumlar da göz önünde bulundurularak, aleyhte ve lehte olan bütün bulguların belirtilmesi kanun ve hukuk vicdanı gereğidir.

3.3. Delil Zinciri

Adli bilişim alanında dünya litaratüründe geçen önemli bir diğer tanım ise delil zinciri (Chain of Custody)'dir. "Chain of custody" kavramı farklı alanlarda da kullanılabilmektedir. Örneğin "Programme for the Endorsement of Forest

Certification" (PEFC) isimli kuruluş sürdürülebilir orman yönetimi alanında sertifikasyon gerçekleştirmektedir.[4] Ana sertifikalarından biri ise "chain of custody" adı verdikleri gözetim zinciri olarak adlandırılabilecek sertifikasyon çeşididir. Gözetim zinciri sertifikasyonunun amacı sürdürülebilir orman yönetimindeki ormanlardan elde edilen ürünün elde edilmesinden son kullanıcıya ulaşmasına kadar geçen sürede orijinallik de sayılabilecek belirlenmiş bazı özelliklerin değişmediğinin garanti altına alınmasıdır. Standart dokümanında ise "chain of custody" kavramını, organizasyona sertifikalandırılmış ürün hakkında isabetli ve doğrulanabilir hak talebi yapma izni veren orman kaynaklı ürünlerin materyal kategorisi hakkındaki bilginin işlenme süreci olarak tanımlanmaktadır.[5] Görüldüğü üzere bu kavramla kastedilen işlem konusu materyal hakkındaki belli bir orijinalliğin ve tutarlılığın işlem başından sonuna kadar korunmasıdır.

Adli süreçte ve adli bilişimde de delilin bütünlüğü ve orijinalliği, delilin güvenilirliği açısından çok önemlidir. Ve hatta bütünlük ve orijinallik mahkeme önünde delilin sahip olması gereken hayati 2 unsurdur (Gordon, 2015:798). Uygun bir delil zinciri verinin nasıl elde edildiği, nakledildiği, analiz edildiği, korunduğu ve taşındığı bilgilerini içermelidir (Cosic ve Baca, 2010).

Dünya genelinde hem özel sektör hem de kolluk kuvvetleri tarafından, delil zincirinin öneminden dolayı bütünlüğünün sağlanması için çeşitli prosedürler işletilmekte ve önlemler alınmaktadır. Bu önlemlerden ilki muhtemel her durum için bir çatı iş akış şeması çıkarmak olmalıdır. İş akış şemasının ortaya çıkarılabilmesi için adli bilişim açısından oluşturulmuş standartların incelenmesi faydalı olacaktır. Çünkü bu alanda belirlenmiş bir standart bütünün birçok maddesi işin teknik doğası gereği benzerlik gösterdiğinden farklı ülkelerde de kullanılabilir durumdadır. Uluslararası standartların dikkate alınmasının bir diğer faydası ise yeri geldiğinde yabancı ülke konulu veya bağlantılı bir adli bilişim incelemesinde iki ülkenin bulguların delil olarak kabul edilmesinde fikir birliğine varmaları açısından büyük kolaylık sağlayacaktır.

[4] Kuruluş ile ilgili bilgi için bknz. https://www.pefc.org/standards/chain-of-custody (Et.18/02/2019)
[5] Ayrıntılar için bknz. https://consultations.pefc.org/consult.ti/PEFCsChainOfCustody/viewCompoundDoc?docid=7826164&partId=7826324&sessionid=&voteid (Et. 09/02/2019)

Standartlar uygulanarak oluşturulan iş akışları ve prosedürlerin yanında el konulan bilişim sistemlerinin ve alınan adli kopyaların da taşınması, korunması ve nakledilmesi esnasında uygulanması gereken kurallar olmalıdır. Zaman damgası, hash algoritması kullanılması ve watermark (filigran) kullanımı gibi yazılmsal olarak verinin bütünlüğü ve güvenilirliği ortaya konabilmektedir. Ancak fiziki şartlara ve maddi imkanlara bağlı olarak bu yöntemlerle güvenliği alınmış dijital bulgunun taşıma ve nakil esnasında doğabilecek zararlara karşı sert ve antistatik kutularda taşınması veya adli emanet gibi uzun süreli bekleyeceği ortamlarda nem ve sıcaklık dengesinin sağlanması gibi bazı standartların getirilmesi bilişim sistemlerinin ve adli kopyaların ömürlerini uzatacaktır. Aksi taktirde henüz adli bilişim incelemesine geçilmeden bir mobil telefonun bataryasının şişerek hafıza çipine zarar vermesi ve muhtemel delilleri karartması söz konusu olabilecektir.

Adli bilişimde birçok farklı alt alan bulunduğu daha önceki verilerden anlaşılmaktadır. Bu nedenle oluşturulacak delil zinciri prosedürlerinde bu alan farklılıkları da gözetilmelidir. Örneğin bulut bilişim alanında teknik olarak veriyi elde etme imkanı bulunsa da bazı durumlarda kolluk kuvvetleri ile incelemeciler hukuk ve delil zinciri açısından bir takım sorunlarla karşılaşabileceklerdir (Piwari, 2016:67). Mobil cihaz adli bilişimi bu hassasiyetin arttığı alanlardan bir tanesidir. Bu nedenle çalışma sonunda uygun ve sağlam bir delil zinciri uygulamasının hem görevlilerin korunması hem de şüpheli, mağdur, müşteki vb. şahısların haklarının korunması açısından mobil cihaz adli bilişiminde ayrı bir önem arz etmekte olduğunun anlaşılması ayrıca amaçlanmaktadır.

Dikkat edilmesi ve uygulanması gereken bir diğer önemli husus ise olması muhtemel, açıklanabilir ve görev gereği olarak zincirde meydana gelmiş değişikliklerin mutlaka belirtilmesidir. Gerçekleştirilen işlemler istenilen sonuçları vermese de mutlaka bu haliyle dokümante edilmeli ve işlemlerdeki şeffaflık sağlanmalıdır. Delil zincirindeki değişiklikler verinin ciddi şekilde bozulmasına ve delil niteliğini kaybetmesine sebep olmamış ise hakim tarafından kabul görmesi beklenir.

3.3.1. Laboratuvar Akreditasyonları Açısından Delil Zinciri ve Türkiye'deki Laboratuvarların Değerlendirilmesi

Çözüm Önerisi başlıklı bölümde tavsiye edilen modelin oluşturulması ile ülkedeki delil zinciri süreci de pekiştirilecek ve daha güvenilir hale getirilebilecektir. Özellikle teknik boyutta irdelenecek olan dijital verinin hassasiyetinin mobil cihaz adli bilişiminde bu bilişim sistemlerinin doğası gereği olarak çok daha hassas adli bilişim uygulamaları gerektirdiği görülecektir. Belli modellemeler ve standardizasyon yöntemleri takip edilerek bu hassasiyetin gerektirdiği daha sağlam zeminli inceleme ortamları oluşturulmalıdır.

Aynı bölümde vurgulanmış olan laboratuvarların akredite edilmesi hususunda ülkemizde harekete geçilmesi gerektiği görülmektedir. Gerçekleştirilen bir çalışmada Jandarma Kriminal Daire Başkanlığı (JKDB) altındaki Bilişim Teknolojileri İnceleme Şube Müdürlükleri, EGM Kriminal Dairesi Başkanlığındaki Ses, Görüntü ve Data İnceleme Şube Müdürlüğü ve Adli Tıp Kurumu Fizik İhtisas Dairesi altındaki Bilişim ve Teknoloji Suçları Şubelerinin laboratuvarlarının, ISO/IEC 17025 Deney ve Kalibrasyon Laboratuvarlarının Yeterliliği kalite standardına göre TÜRKAK tarafından akredite edilmeye başlandığı bilgisi verilmiştir (Barbaros, 2016:28). İlgili bilgiler TÜRKAK İnternet sitesinden kontrol edildiğinde TS EN ISO/IEC 17025:2012 standardına göre JKDB Merkez Jandarma Kriminal Laboratuvar Amirliği'nin (MJKLA) Çizelge 3.5'te belirtildiği şekilde ses, görüntü ve data (veri) inceleme işlemlerini akredite ettiği (TÜRKAK, 2018), EGM Kriminal Dairesi Başkanlığı'nda ise adli bilişim açısından sadece görüntü inceleme işlemlerinin akredite edildiği görülmüştür (TÜRKAK, 2017). Delil zincirini güvenilir hale getirecek şekilde laboratuvarında Class-100 standartlarında bir temiz odaya sahip olduğu, uluslararası kabul görmüş lisanslı ve açık kaynak birçok yazılım-donanımı kullandığı, personelini yurtiçi ve uluslararası birçok eğitimle güncel tuttuğu bilinen EGM SSMDB'nin ise akredite çalışmalarına 2014 yılı ortalarında başladığı, ancak yoğun iş yükü nedeniyle ara verilen akreditasyon ve standardizasyon işlemlerini tekrar başlattığı bilgisi, kurum tarafından 2018 yılı 10-13 Aralık günleri arasında düzenlenen 5. Uluslarası Siber Suçlar Çalıştayı'nda verilmiştir. Adli bilişim incelemesi gerçekleştiren diğer kurum ve

kuruluşların da bahse konu akreditasyon ve standardizasyon işlemlerini uygulamalarında fayda olacağı değerlendirilmektedir.

Çizelge 3.5 JKDB MJKLA Adli Bilişim Laboratuvar Akreditasyonu (TÜRKAK, 2018)

Adli Bilimler - Görüntü İnceleme	Görüntü İyileştirme
	Yüz Karşılaştırması
	Görüntü / Fotoğraf Medyaları Üzerinde Kurgu ve Manipülasyon İncelemesi
	Görüntü / Fotoğraf Karşılaştırma
Adli Bilimler - Ses İnceleme	Ses İyileştirme
	Konuşmacı Tanıma
	Ses Kayıtları Üzerinde Kurgu ve Manipülasyon İncelemesi
Adli Bilimler - Veri İnceleme	Sim Kart İncelemesi
	Anahtar Kelime Arama
	Dosya Türüne Göre İnceleme Metodu

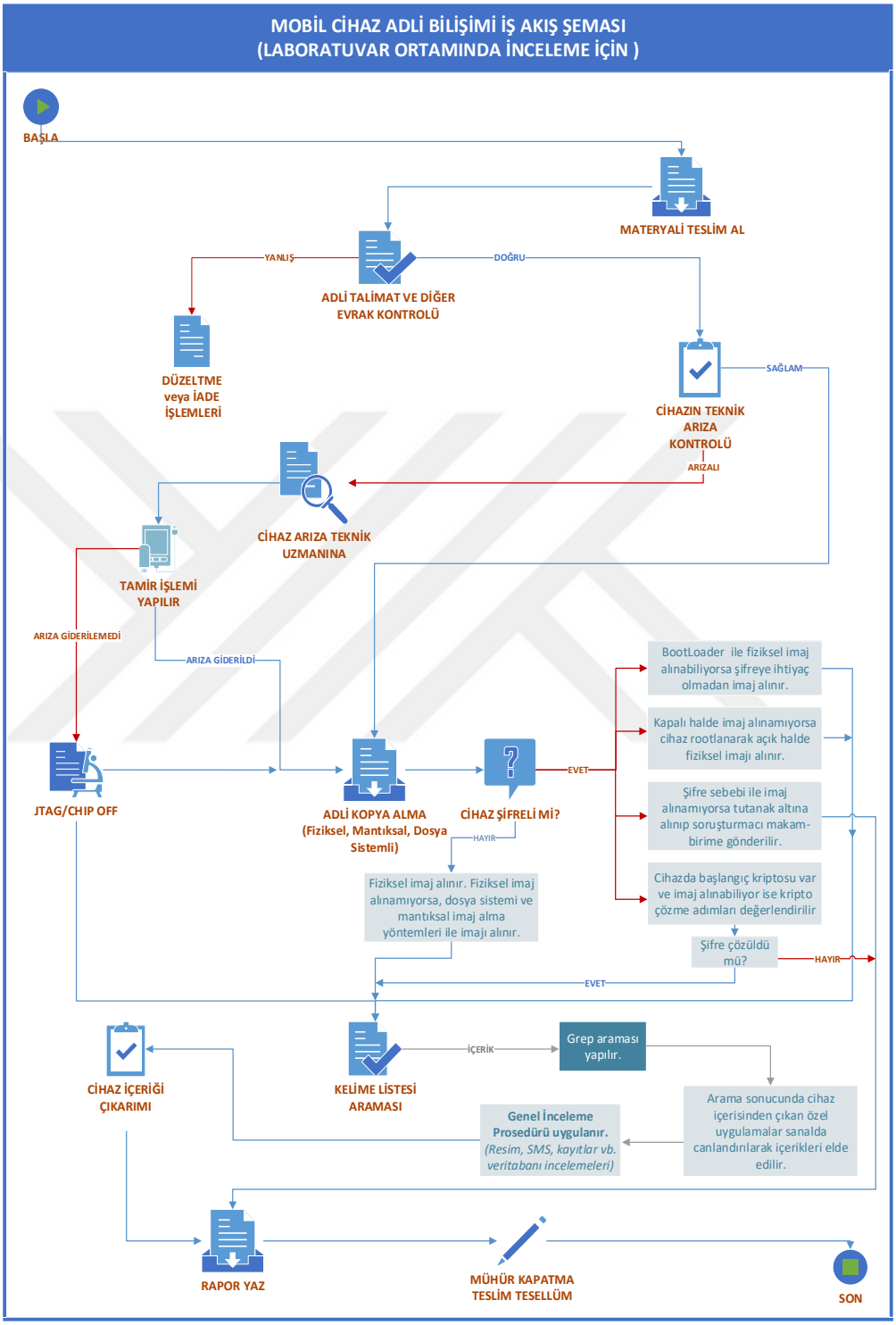
Adli bilişim incelemesi gerçekleştirilen laboratuvarların akredite olmamış olması burada gerçekleştirilen incelemelerin sağlıklı olmadığı anlamına gelmemektedir. Zaman ve imkânlar kapsamında akredite işlemlerinin gerçekleştirilmesi tabi ki işlemlerin daha sağlam zeminlerde gerçekleştirilmesini sağlayacaktır. Bununla birlikte adli bilişimde kullanılan yazılım ve donanımların dünya genelinde mahkemelerde kabul görüyor olması (Kahiye, 2014:1) ile kurum içi iş akışlarının oluşturulmuş ve uygulanıyor olması da delil zincirini sağlayabilecek yöntemlerdir. Ancak laboratuvar akreditasyonu ile birlikte delil niteliği taşıyan bulgu ve hakkındaki işlemler aynı zamanda uluslararası kabul edilen bir geçerliliğe de sahip olacaktır. Daha önce de bahsedildiği gibi bu akreditasyona sahip olunduğu taktirde karşı ülke mahkeme ve hakimlerinin, delil zincirini ve uluslararası standartlar ile

akredite edilmiş usulleri değerlendirerek daha çok bulgunun delil olarak kabul edilmesi yönünde karar verebilecekleri düşünülmektedir. Akredite olmuş bir laboratuvarda incelenmiş bulgular hakkında böyle bir kararı vermek hakim açısından daha kolay olacaktır.

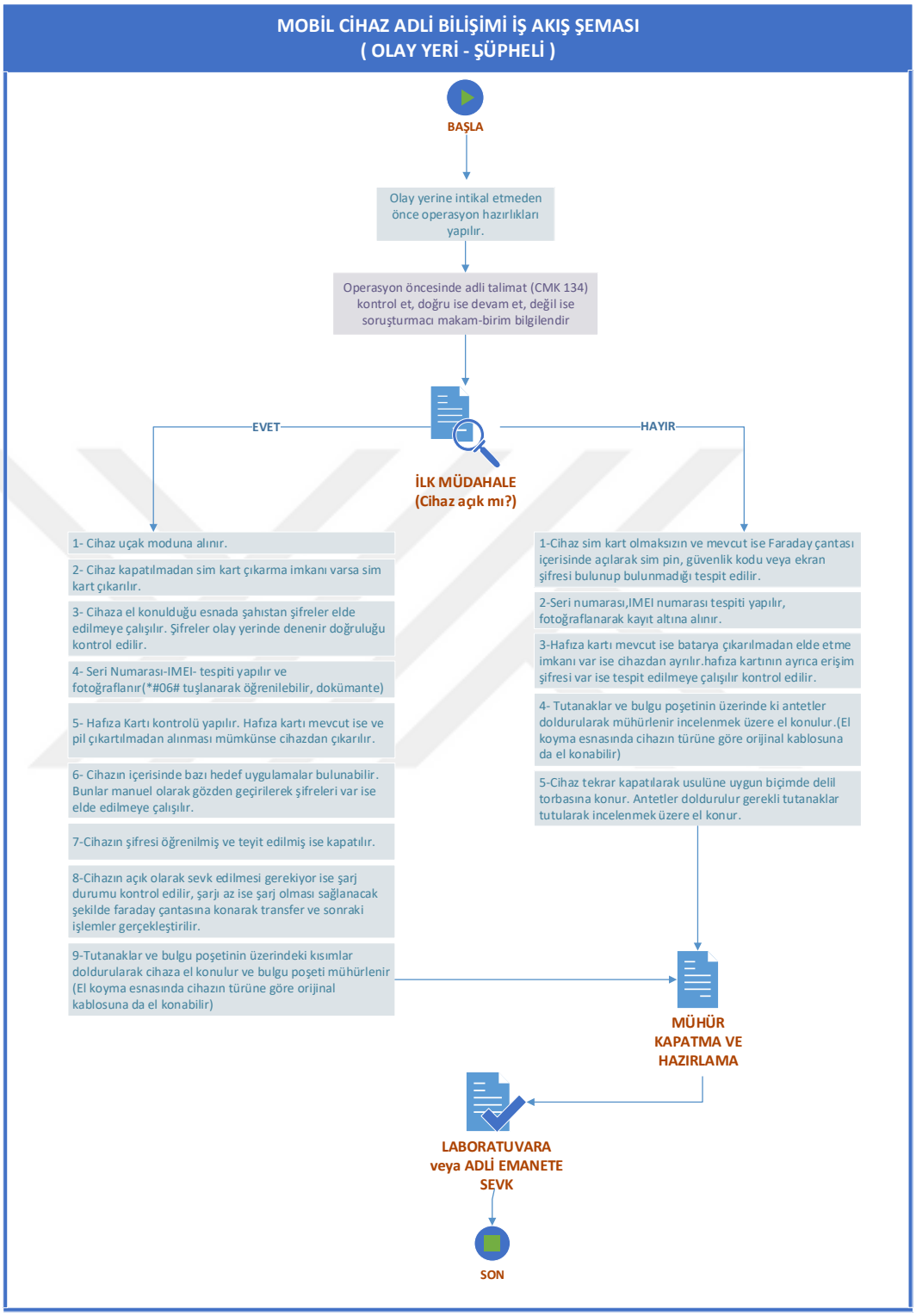
3.3.2. Mobil Cihaz Adli Bilişimi İçin Olay Yeri ve Laboratuvar Örnek İş Akış Görselleri

Takip eden akış şemaları da Şekil 3.1 ve Şekil 3.2 olarak örnek şema olarak çizilmiştir ve bu süreçteki çalışmalarda ilgili kurum veya birimlerce kullanılabileceği değerlendirilmektedir. Adli bilişim alanında birçok firma, resmi görevli veya bilirkişi kendi prosedürlerini uygulamaktadırlar. İşlemlerde yeknesaklığın sağlanması ve delil zincirinin korunması için en temel prosedürleri içeren akış şemaları bu tez kapsamında incelenen literatür ve uygulamadaki gereklilikler göz önüne alınarak oluşturulmuştur. oluşturulmuştur. Akış şemaları çalışmanın diğer bölümlerinde anlatılan adımları da içeriyor olmasının yanında özellikle delil zincirinin önemli bir dayanağı olması nedeniyle çalışmada delil zinciri bölümünün içerisinde sunulmuştur.

Şekil 3.1 Laboratuvar İçin Mobil Cihaz İnceleme İş Akış Şeması



Şekil 3.2 Şüpheli İçin Mobil Cihaz Adli Bilişimi Olay Yeri İş Akış Şeması



Bu bölümle birlikte hukuki boyutun bulgular açısından irdelemesi sonlandırılmış olup sonraki bölümlerde mobil cihaz adli bilişimi ve teknik boyut hususları çalışılacaktır.

3.4. Mobil Cihaz Adli Bilişiminim Tanımı ve Önemi

Mobil yani hareketli ve taşınabilir olarak adlandırabileceğimiz cep telefonları, akıllı cep telefonları, akıllı saatler, PDA, GPS cihazları ve drone gibi cihazlar mobil cihaz adli bilişimin alanına girmektedir. Bu cihazların özelliklerine bakıldığında günlük eposta gönderip alma, mesajlaşma, sosyal ağları kullanma, fotoğraf çekme, konum bildirme, konum öğrenme, ses kaydetme, video kaydetme, sağlık bilgisi takip etme, yön bulma, zamanlayıcı olarak kullanma gibi birçok günlük işi avuç içimize sığan tek bir cihaz aracılığı ile yapabildiğimizi görmekteyiz. Tabi ki bu işlemlerde cihazların bir ağa ve özellikle İnternete bağlı olmaları da çok büyük etkendir. Bu şu anlama gelmektedir ki günlük yaşantımıza ait birçok iz artık bu cihazlar üzerinde barındırılmaktadır.

Hal böyle iken bir suç soruşturmasında veya bir suçun tespiti ile ilgili yürütülen çalışmalarda akıllı telefonlar başta olmak üzere mobil bilişim sistemlerinin önemi en üst seviyeye çıkmıştır. Mobil bilişim sistemlerini bu kadar önemli kılan en büyük etken görüldüğü üzere içerdiği verinin hassasiyeti ve kritikliğidir. Bu veriler bir suçun ispatı için ulaşılmaya çalışılan veriler olduğu gibi, hackleme olayı sonrası sızdırılmış olan ve bir kişinin sağlığına ilişkin çok hassas ve kritik veriler de olabilir. İşte tüm bu hassas veriler mobil cihaz adli bilişiminin konusu olabilmektedir. Mobil cihaz adli bilişimi için literatürde birçok tanım yapılmaktadır. Tanımlardan biri, bir mobil cihazdan, kabul edilmiş yöntemler kullanarak adli kurallara uygun koşullar altında dijital delilin kurtarılması bilimi şeklindedir (Ayers ve ark, 2014). Mobile kelimesi İngilizcede hareketli, yer değiştirebilen ve portatif kelimelerinin karşılığı olarak kullanılmaktadır ve Türkçe'de de mobil kelimesi olarak hareketli, taşınabilir kelimelerinin karşılığı olarak kullanılır. Mobil kelimesi İngilizce ve Türkçe'de de taşınabilir cihazları ifade etmek için tek başına kullanılabilmektedir. Bu anlamlardan hareketle İngilizce'de "mobile forensics" (mobil adli bilişimi) olarak kullanımlarına rastlansa da, teknik ve akademik literatürde daha çok "mobile device forensics" (mobil cihaz adli bilişimi) tabirinin kullanıldığı görülmektedir. İncelenen literatürdeki bilgiler de göz önüne alındığında, bu çalışmada yapılmış olan adli bilişim tanımındaki uygulamaların mobil

cihazlar olarak irdelenecek olan cihazların tümü üzerinde uygulanması mobil cihaz adli bilişimini tarif eder.

Bahsedilen boyutta önemli olan verilere ulaşmak için kullanılan bilim olarak tarif edilebilecek bilim olan mobil cihaz adli bilişimi de bu boyutu ile ayrıca önem taşımaktadır. Dünyada bu alanın ne kadar önemli olduğu sahip olduğu pazar payına bakılarak anlaşılabilir. IndustryARC isimli pazar araştırma raporları, genel danışma, veri analitikleri ve endüstri analizi servisi sağlayan bir firmanın web sitesinden alınan bilgiye göre % 14.2 Yıllık Bileşik Büyüme Oranı çerçevesinde 2023 yılı itibari ile 6.83 milyar dolar olacağı tahmin edilmektedir. Pazarın büyük bir bölümünü elinde bulunduran Amerika'da bu rakamın 3.6 milyar dolar olması beklenmektedir. Yine Amerika'da 2017 yılında 241.3 milyon dolar olan mobil cihaz adli bilişim pazar payının ise 2020 yılında 346.8 milyon dolara yükselmesi beklenmektedir. Mobil cihaz adli bilişimi alanındaki toplam pazar payının ise 2020 yılı itibarıyla 612.8 milyon dolar olması ön görülmektedir. Aynı araştırmada adli bilişim pazarı için Avrupa bölgesinde en çok büyümenin mobil cihaz adli bilişimi ve veritabanı adli bilişimi alanında olacağı belirtilmektedir. Böylesine büyük pazar payına sahip bir alanda dünyadaki trend ve mobil cihazlardaki verilerin suç tespiti ve kişisel verilerin korunmasındaki önemi bağlamında ülkemizde de bu alanda gerçekleştirilen çalışmaların artırılması ve zenginleştirilmesi gelecek adına olumlu olacaktır.

Mobil cihazlardaki verilerin kıymetli olmasının arkasındaki en büyük etken olarak İnternet kavramını söylersek hiç de yanlış olmaz. İnsanların mobil cihazlardaki verilerini depolama, sosyal çevresiyle paylaşma, iletişimlerini gerçekleştirme, araştırma ve geliştirme gibi ihtiyaçları doğrultusunda en çok kullanılan iletişim modelidir İnternet. Bu önemi daha iyi kavrayabilmek için mobil cihazların ve İnternetin birbirlerini etkileyen gelişimine göz atmak da faydalı olacaktır.

3.5. İnternetin Kullanımı

3.5.1. Tarihçe

Mobil cihazların tarihçesi gerek İnternet gerekse telefon teknolojisinin gelişimine bağlı olarak seyir göstermektedir. Bu süreç sebebiyle öncelikle İnternetin kullanımı seyri sonrasında ise mobil cihazlar hakkında temel bilgiler verilecektir.

3.5.1.1. Dünyada İnternetin Tarihi

II. Dünya Savaşı'nın bitimi ile başlayan Soğuk Savaş ve oluşan iki kutuplu dünyada özellikle bilgiyi üretme, ulaşma, saklama gibi süreçler stratejik bir önem kazanmıştır. Bu amaç doğrultusunda süper güç olarak adlandırılan devletler bilgi üretimi yolunda yatırımlar yaparak önemli teknolojik yeniliklere imza atmışlardır. Özellikle savaş esnasında yaşanacak iletişim bozuklukları Amerikan hükümeti tarafından değerlendirilmiş ve klasik iletişim araçları dışında (telefon, telgraf vb.) daha kapsayıcı, hızlı ve alternatif olabilecek teknolojik yenilikler için araştırmalar ve yatırımlar yapılmaya başlanmıştır. Tamamı ile savunma ihtiyacı ile ortaya çıkan en önemli yenilik bu minvalde İnternettir.

İnterneti ilk bulanlar Amerikan Federal Hükümeti Savunma Bakanlığı'nın araştırmadan sorumlu kuruluşu olan "Savunma İleri Düzey Araştırma Projeleri Kurumu" (DARPA-Defence Advanced Research Project Agency)'dur. Amerikan Savunma Bakanlığı İnternet ile birlikte bilgisayar bilimlerini ve bunlara bağlı militer projeleri desteklemek için ARPANET (Advanced Research Projects Agency Network -Gelişmiş Araştırma Projeleri Dairesi Ağı) adında bir ağ oluşturmuş ve bu ağı ABD'deki yükseköğretim ve Ar-Ge kuruluşlarının bilgisayarlarını da dahil ederek genişletmiştir. Bugünkü manada ilk İnternet ağının kurulması ise 1986 yılında NSFNet (National Science Foundation-Ulusal Bilim Vakfı) tarafından hayata geçirilmiştir.

Yerel alan ağı protokolü olan Ethernet ise ilk kez 1974 yılında Harvard Üniversitesindeki Robert Metcalfe isimli bir öğrenci tarafından ortaya konulmuştur. Metcalfe 1975'te buluşunun patentini almış ve 1980'de açık Ethernet standardı tamamlanmıştır.[6] 1977-1978 yıllarında Ethernet ve TCP/IP (Transmission Control Protocol/İnternet Protocol) üzerinde yapılan çalışmalar sonrasında geliştirilen protokol 1980 yılında ARPANet üzerinde kullanılmaya başlanmış ve bu sayede aynı ağa bağlı bilgisayarlar arasındaki iletişim gerçekleşmiştir.

1983 yılında ise tüm ARPANET ağı üzerinde kullanılmakta olan NCP (Network Control Protocol)'den TCP/IP'ye geçilmiş ve aynı yıl TCP/IP, ARPANET'i de içeren Savunma Bakanlığı İnternet'inde kullanılmak üzere standardizasyonu sağlanmıştır. 1984 yılında Unix işletim sistemi ticari olarak kullanılmaya başlanmasıyla birlikte, aynı yıl TCP/IP Unix üzerinde çalışır duruma gelmiş, Unix üzerinde DNS ile ilgili çalışmalara start verilmiştir. DNS çalışmalarının tamamlanması ise yaklaşık 4 yıl gibi bir sürece yayılmıştır.

1986 yılında İnternet erişimi için 56 Kbps omurga üzerinde NSFNet kurulmuş, ticari kullanımlar dışındaki tüm kullanıcıların (araştırmacılar, hükümet, vb.) kullanımına açılmıştır.[7] E-posta, FTP (File Transfer Protocol- Dosya Transfer Protokolü) ve TELNET (Telecommunication Network – İletişim Ağı) protokollerinin standartları oluşturulmuş, teknik olmayan kişiler tarafından kolay kullanılır şekle dönüştürülmüştür. İnternet'in ilk kullanıcıları üniversiteler, araştırma kurumları ve kütüphanelerdir. Kurulan ağ üzerinde bilgi/dosya/arşiv paylaşımına yönelik çalışmalar 1989 yılında başlamıştır.

FTP sitelerinin arşivlerinin oluşturulmasına ve bilginin İnternet üzerinde paylaşılmasına olanak sağlayan Archie sistemi, 1989 yılında Montreal McGill Üniversitesinde geliştirilmiş ancak ABD ve Kanada arasındaki trafiğin yarısını Archie'nin oluşturması nedeniyle üniversitedeki sistemin yükü artınca üniversite

[6]Ayrıntılar için bknz. https://www.networkworld.com/article/2202019/lan-wan/living-legends--ethernet-inventor-bob-metcalfe.html (Erişim Tarihi: 09/02/2019)

[7] Ayrıntılar için bknz. https://www.livingİnternet.com/doc/merit.edu/phenom.html (Erişim Tarihi:18/02/2019)

Archie'yi dış erişime kapatmıştır. Aynı yıllarda Thinking Machines Corp. tarafından veri tabanlarındaki full text dosyaların indekslenmesine ve İnternet üzerinden tarama yapılabilmesine olanak sağlayan WAIS (Wide Area Information Server) geliştirilmiştir. Daha sonra, 1991 yılında Minnesota Üniversitesi'nde İnternet üzerindeki bilgilere ve dosyalara bir menü sistemi aracılığıyla erişilmesini sağlayan ve istemci/sunucu (client/server) mimarisi üzerinde çalışan gopher sistemi geliştirilmiş, bunu sırasıyla VERONICA (Very Easy Rodent-Oriented Netwide Index to Computerized Archives), JUGHEAD (Jonzy's Universal Gopher Hierarchy Excavation And Display) sistemleri izlemiştir.

Öte yandan, İnternet üzerindeki bilgi/dosya ve arşivlere kolay ve hızlı erişimin sağlanabilmesi amacıyla 1989 yılında CERN'de (European Laboratory for Particle Physics) bir başka çalışma başlatılmıştır. Bu çalışma daha sonra 1991 yılında WWW (World Wide Web) protokolü adı altında kullanılmaya başlanmıştır. 1993 yılında National Center For Supercomputing Applications (NCSA) tarafından bu protokol üzerinde çalışan grafik arayüzlü bir yazılım olan Mosaic geliştirilmiş; bu tarayıcıyı daha sonra Netscape, vb. gibi tarayıcılar izlemiştir. [8]

3.5.1.2. Türkiye'de İnternetin Tarihi

Bütün bu süreç Türkiye'ye 1986 yılında tesis edilen EARN (European Academic and Research Network)/BITNET (Because It's Time Network) bağlantılı TÜVEKA (Türkiye Üniversiteler ve Araştırma Kurumları Ağı) ile gelmiştir. İlerleyen yıllarda bu ağın hat kapasitesinin yetersiz kalması ve teknolojik açıdan ihtiyaçlara cevap verememeye başlaması üzerine, 1991 yılı sonlarına doğru Ortadoğu Teknik Üniversitesi (ODTÜ) ve Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK), İnternet teknolojilerini kullanan yeni bir ağın tesis edilmesi yönünde bir proje başlatmışlardır. Bu çerçevede ilk deneysel bağlantı 1992 yılının Ekim ayında

[8] Sözkonusu bilgiler Orta Doğu Teknik Üniversitesi'nin sayfasından alınmıştır. Dünyada İnternetin tarihi ve Türkiye'ye İnternetin gelişi ve Üniversitelerin, TUBİTAK'ın ve ULAKBİM'in sürece katkıları hakkında ayrıntılı bilgi ve belgeler için bknz. http://www.İnternetarsivi.metu.edu.tr/tarihce.php (Erişim Tarihi:18/02/2018)

X.25 üzerinden Hollanda'ya yapılmış; PTT'ye 1992 yılında yapılan başvurunun sonuçlanmasını takiben, 12 Nisan 1993'de de 64 Kbps kapasiteli kiralık hat ile ODTÜ Bilgi İşlem Daire Başkanlığı sistem salonundaki yönlendiriciler kullanılarak, ABD'de NSFNet'e TCP/IP protokolu üzerinden Türkiye'nin ilk İnternet bağlantısı gerçekleştirilmiştir (Özgit, Çağıltay, 2018).

1994 yılında da kurumlara ve firmalara İnternet hesapları verilmeye başlandı. Bu arada ilk İnternet servis sağlayıcı "tr.net" de hizmete girmiştir. Ardından sırayla, Bilkent Üniversitesi (1995 Eylül), Boğaziçi Üniversitesi (1995 Kasım) ve İstanbul Teknik Üniversitesi (1996 Şubat) bağlantıları sağlandı. 2000'li yıllarda ise özel sektörün İnternet'e gösterdiği ilgi ve yatırımlar hızla artmış ve İnternet kullanımı yaygınlaşmıştır. Bu arada İnternet kullanımı ile ilgili olarak ilk kurumsallaşma çalışması 1998 yılında yapılmış ve Ulaştırma Bakanlığı bünyesinde İnternet Üst Kurulu oluşturulmuştur.

3.5.2. Türkiye'de ve Dünyada İnternet Kullanımının Mevcut Durumu

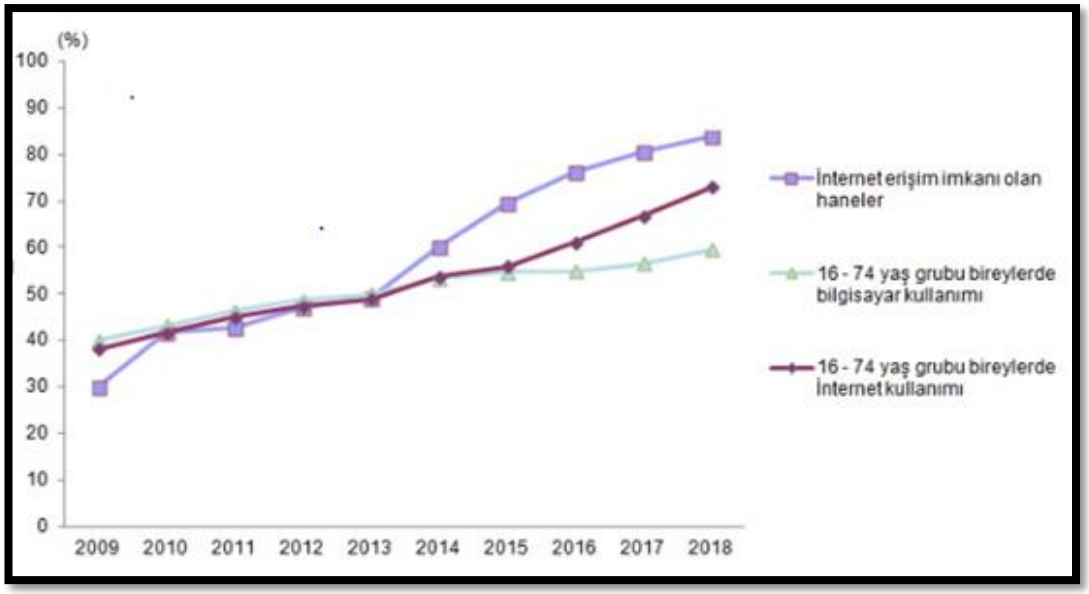
İnternet tabanlı çevrimiçi teknolojiler kısa bir zaman içinde büyük değişime girmiştir. İlk defa 2004 yılında isminden bahsedilmeye başlayan web 2.0 teknolojileri ile İnternet teknolojileri kendi içinde dönemlere ayrılmaya başlamıştır. 90'lı yıllarda sadece durağan İnternet siteleri ile tek taraflı bilgi akışı sunulurken; 2000'li yıllarla birlikte etkileşimli ve herkesin içerik oluşturabildiği web 2.0 teknolojileri ortaya çıkmaya başlamıştır. 2000'li yıllar ile birlikte İnternet kullanıcıları Web 2.0 teknolojisi ile tanışmaya başlamıştır. Web 2.0 teknolojisi ile web platformunda sadece içeriklere ulaşmak değil o içerikleri yönetmek, değiştirmek, ekleme yapmak veya silmek gibi aktivitelerin yanında tamamen yeni içerikler geliştirme imkanı da kullanıcılara sunulmaya başlamıştır. Kişisel web sayfalarında oluşan bloglar, içerik yönetimi sistemi sağlayan wiki'ler, kullanıcıların fotoğraflarını milyonlarca kullanıcı ile buluşturan Flickr, yine kullanıcıların başka kullanıcıların bilgisayarlarındaki içerikleri indirmelerine olanak tanıyan P2P (Peer to Peer –Eşten eşe) programları gibi servisler web 2.0 teknolojilerine geçişi hızlandırmıştır.

Web 2.0 teknolojileri sosyal ağlar ile daha da boyut değiştirmeye başlamıştır. 1997 yılında Six.Degrees.com sosyal ağının kurulmasının ardından bunu Livejournal, Friendster, Myspace gibi popüler sosyal ağlar izlemiştir ve son olarak 2004 yılında kurulan Facebook çok kısa zamanda büyük bir kullanıcı kitlesine ulaşmıştır. Web 2.0 teknolojileri özellikle sosyal iletişim olarak adlandırılan MySpace ve Facebook gibi daha çok arkadaş ve akraba arama ve onlarla iletişim kurma platformlarının doğmasına sebep olmuştur. 2000'li yıllardan 2010'lu yıllara geçerken sosyal iletişim mantığı ile kurulan sosyal ağlar, sosyal medya platformlarına kaymaya başlamıştır. Böylece kapalı gruplar arasındaki iletişim birden hiç tanımadığımız bir insanın bile paylaşımını görebilme imkânını doğuran sosyal medya platformlarına evrilmeye başlamıştır (Bilgi Teknolojileri ve İletişim Kurumu, 2018:2).

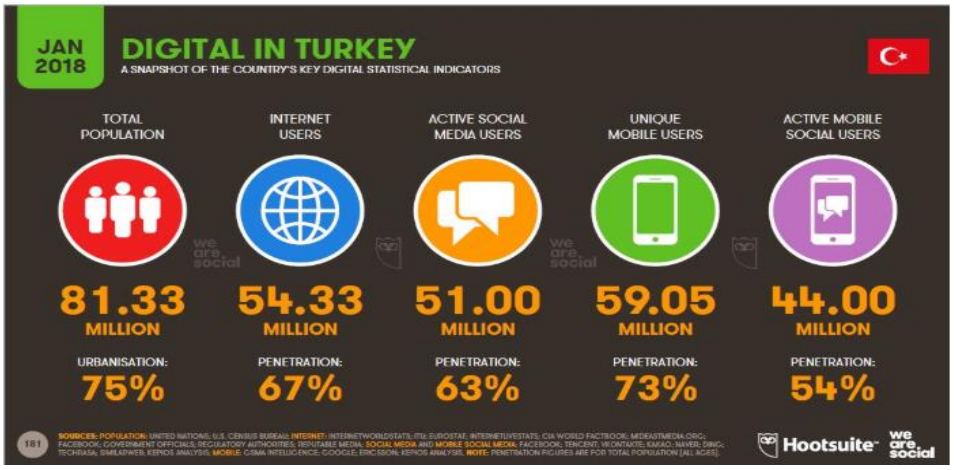
Türkiye'de İnternet kullanımına ilişkin veriler 08.08.2018 tarihinde kamuoyu ile paylaşılmıştır ve Çizelge 3-1'de gösterildiği gibidir.[9] Buna göre; bilgisayar ve İnternet kullanımı 2018 yılında 16-74 yaş grubundaki bireylerde sırasıyla yüzde 59,6 ve yüzde 72,9'dur. Bu oranlar 2017 yılında sırasıyla yüzde 56,6 ve yüzde 66,8 olarak kaydedilmiştir. Bilgisayar ve İnternet kullanım oranları 16-74 yaş grubundaki erkeklerde yüzde 68,6 ve yüzde 80,4 iken, kadınlarda yüzde 50,6 ve yüzde 65,5'tir. Hane halkı bilişim teknolojileri kullanım araştırması sonuçlarına göre 2018 yılı Nisan ayında hanelerin yüzde 83,8'i evden İnternete erişmiştir. Bu oran 2017 yılının aynı ayında yüzde 80,7'dir.

[9] "Bilgi Teknolojileri ve İnternetin Bilinçli, Güvenli Kullanımı", Bilgi Teknolojileri ve İletişim Kurumu İnternet Daire Başkanlığı Yayınları, 2018, s.2-5.
http://www.guvenliweb.org.tr/haber-detay/turkiyenin-İnternet-kullanim-aliskanliklari-tuik-2018
http://www.tuik.gov.tr/PreHaberBultenleri.do?id=27819 (Erişim Tarihi: 18/02/2019)

Çizelge 3.6 Türkiye'de İnternet Kullanımına İlişkin Veriler[10]



We Are Social ve Hootsuit isimli şirketlerce her yıl hazırlanan sosyal medya istatistikleri ise "**Digital in 2018 in Western Asia"** ismiyle yayınlanmıştır (Kamp, 2018).[11] Türkiye'nin İnternet kullanımına ilişkin bulgular Şekil 3.3'de gösterildiği gibidir. [12]



Şekil 3.3 Türkiye'de İnternet, Mobil Cihaz ve Sosyal Medya Kullanımı
(Kamp, 2018)

[10] 2018 yılına ait istatistikler için bknz. https://dijilopedi.com/tuik-turkiyenin-İnternet-kullanim-aliskanliklari-raporu/ (Erişim Tarihi: 09/02/2019)
[11] Ayrıntılar için bknz. https://wearesocial.com/blog/2018/01/global-digital-report-2018 (Erişim Tarihi: 18/02/2019)
[12] Ayrıntılar için bknz https://dijilopedi.com/2018-turkiye-İnternet-kullanim-ve-sosyal-medya-istatistikleri/ (Erişim Tarihi: 09/02/2019)

Nüfusun %67'sini oluşturan 54.3 milyon İnternet kullanıcısı, nüfusun %51'ini oluşturan 51 milyon aktif sosyal medya kullanıcısı, nüfusun %54'ünü oluşturan 44 milyon aktif mobil sosyal medya kullanıcısı olduğu bildirilmiştir. Aynı kuruluş tarafından çalışılmış olan dünyadaki mevcut durum ise Şekil 3.4'te yer almaktadır.

Şekil 3.4 Dünyada İnternet, Mobil Cihaz ve Sosyal Medya Kullanımı

(Kamp, 2018)

Çizelge 3.7 OECD (Ekonomik İşbirliği ve Kalkınma Örgütü) Üye Ülkeleri Nüfusa Göre İnternet Kullanımları ve Facebook Kullanıcı Sayıları

(İnternet World Stats, Mayıs 2018)

	ÜYE ÜLKE	TAHMİNİ NÜFUS 2018	INTERNET KULLANICILARI 31/12/2017	INTERNET KULLANIMI	FACEBOOK ÜYELİĞİ
1	Almanya	82,293,457	79,127,551	96.20%	31,000,000
2	Amerika	326,766,748	312,322,257	95.60%	240,000,000
3	Avusturalya	24,772,247	21,743,803	87.80%	15,000,000
4	Avusturya	8,751,820	7,695,168	87.90%	3,700,000
5	Belçika	11,498,519	10,857,126	94.40%	6,500,000
6	Birleşik Krallık	66,573,504	63,061,419	94.70%	44,000,000
7	Çek Cum.	10,625,250	9,323,428	87.70%	4,600,000
8	Danimarka	5,711,837	5,754,356	96.90%	3,700,000
9	Estonya	1,306,788	1,276,521	97.70%	620,000
10	Finlandiya	5,542,517	5,225,678	94.30%	2,700,000
11	Fransa	65,233,271	60,421,689	92.60%	33,000,000
12	Güney Kore	51,164,435	47,353,649	92.60%	43,000,000
13	Hollanda	17,084,459	16,383,879	95.90%	9,800,000
14	İrlanda	4,803,748	4,453,436	92.70%	2,700,000
15	İspanya	46,397,452	42,961,230	92.60%	23,000,000
16	İsrail	8,452,841	6,740,287	79.70%	5,800,000
17	İsveç	9,982,709	9,653,776	96.70%	6,300,000
18	İsviçre	8,544,034	7,776,749	91.00%	3,700,000
19	İtalya	59,290,969	54,798,299	92.40%	30,000,000
20	İzlanda	337,780	334,303	99.00%	250,000
21	Japonya	127,185,332	118,626,672	93.30%	71,000,000
22	Kanada	36,953,765	33,221,435	89.90%	23,000,000
23	Kolombiya	49,464,683	31,275,567	63.20%	29,000,000
24	Latviya	1,929,938	1,663,739	86.20%	740,000
25	Litvanya	2,876,475	2,599,678	90.40%	1,400,000
26	Lüksemburg	590,321	572,242	96.90%	320,000
27	Macaristan	9,688,847	8,588,776	88.60%	5,300,000
28	Meksika	130,759,074	85,000,000	65.00%	78,000,000
29	Norveç	5,353,363	5,311,892	99.20%	3,400,000
30	Polonya	38,563,573	28,267,099	73.30%	14,000,000
31	Portekiz	10,291,196	8,015,519	77.90%	5,800,000
32	Slovakya	5,449,816	4,629,641	85.00%	3,200,000
33	Slovenya	2,081,260	1,663,795	79.90%	910,000
34	Şili	18,197,209	14,108,392	77.50%	13,000,000
35	Türkiye	81,916,871	56000000.00	68.40%	44,000,000
36	Yeni Zelanda	4,749,598	4184520.00	88.10%	3,100,000
37	Yunanistan	10,892,931	7525926.00	69.10%	5,000,000
OECD ÜYESİ TOPLAM		1,351,911,645	1,180,119,911	87.30%	810,540,000

Çizelge 3-7'ye göre de Türkiye'nin OECD (Ekonomik İşbirliği ve Kalkınma Örügütü) üyesi ülkeler arasında İnternet kullanıcı sayısı ve Facebook kullanıcısı sayısı gösterilmiş olup sayının oldukça yüksek olduğu görünmektedir.[13]

[13] https://www.İnternetworldstats.com/stats16.htm, (Et. 09/02/2019)

3.5.3. Mobil Cihazlar

Mobil cihazlar, hücresel bağlantı ve diğer kablosuz bağlantı elemanlarını kullanarak verileri işlemek, iletmek ve depolamak için dizayn edilmişlerdir. İş ve sosyal hayatta zaman kazanma ve daha verimli çalışma olanağı sağlayan mobil cihazlar kapsamına laptop tabir edilen dizüstü bilgisayarlar girmemektedir. Ancak dizüstü bilgisayar gibi kullanabilen tabletler bu sınıfa girmekle beraber, akıllı veya klasik cep telefonları, akıllı saatler, SIM kartlar, PDA (Personal Digital Assistant) , GPS cihazları ve hatta drone adı verilen insansız hava araçları bu başlık altında ele alınmaktadırlar.

3.5.3.1. Cep Telefonu

1876 tarihinde Alexander Grahem Bell tarafından icat edilen ilk telefonun ardından taşınabilir ilk cep telefonu Motorola şirketinde mühendis olarak çalışan Martin Cooper tarafından 1973 yılında icat edilmiştir. Ürettiği kablosuz cep telefonuyla ilk görüşmeyi 3 Nisan 1973 tarihinde yaparak tarihe geçen Cooper'in ilk Motorola cep telefonu 850 gram ağırlığında, 25 cm yüksekliğinde, 8 cm derinliğinde ve 4 cm genişliğindeydi. Telefonun ekranı hesap makinalarının ekranı ile aynıydı ve 15 cm'lik anteni yanında telefonun fiyatı 4000 dolardı.[14]

1990'larda ise Nokia'nın ilk telefonu piyasaya çıkmıştır. Telefonda 99 kişilik hafıza ve 2 satırlık ekranın yanı sıra konuşma yapılacağı zaman çekilerek uzatılan bir de anten bulunmaktaydı. 1990'larda Nokia, Motorola ve IBM'in ürettiği telefonlar hızla tüm dünyaya yayıldı.

[14] Cep telefonunun tarihsel gelişimi hakkında ayrıntıya https://www.teknonce.com/cep-telefonunun-tarihsel-gelisimi.html adresinden ulaşılabilecektir. (Erişim Tarihi:18/02/2019)

2000'li yıllarda klavyesi, dokunmatik ekranı, kalemi, müzik çalma kapasitesi olan yeni tip telefonlar ile birlikte Samsung'un cep telefonu piyasasına girdiği görülmektedir. İlk kameralı telefon ise Japonlar tarafından geliştirilmiş, Apple da 2007 yılında ilk iPhone'u piyasaya sürmüştür. Bu cep telefonları açısından çığırdır çünkü telefon tamamen dokunmatiktir ve yüksek çözünürlüklü kameraya sahiptir, İnternet tarayıcısı ve multi-touch özelliği bulunan bu telefonlar günümüz cep telefonu anlayışını yansıtır. Bununla birlikte günümüzde mobil cihaz adli bilişiminde en çok akıllı tabir edilen cep telefonları ile karşılaşılmaktadır. Kimi verilere göre ilk akıllı telefon 1992 yılında sürülen IBM firmasına ait SIMON isimli telefon kimilerine göre ise 1996 yılında Nokia tarafından piyasaya sürülen Nokia 900 Communicator model PDA tarzı telefon gösterilmektedir. Ancak günümüz akıllı telefon anlayışı açısından ilk olarak tanımlanabilecek akıllı telefon, ilk çıkarılan Apple marka Iphone model telefondur.

Cep telefonları, basit bir çağrıdan kişisel bir bilgisayar gibi verilerin saklanmasına ve korunmasına kadar çeşitli görevleri gerçekleştirebilmektedir. Taşınabilir, kompakt, büyük güçte bataryaya sahip ve hafiftirler. Bu özellikleri sayesinde bahsedilen günlük teknolojik ihtiyaçlar için ayrıca yaygın olarak tercih edilme sebebi olabilmektedir. Temel olarak, mikroişlemci, salt okunur bellek (ROM), rasgele erişim belleği (RAM), mikrofon, hoparlör, dijital sinyal işlemcisi, bir dizi donanım tuşu ya da dokunmatik ekran ve arabirimi, teknolojinin gelişimine göre Organic Light Emitting Diode (OLED), Active-Matrix Organic Light-Emitting Diode (AMOLED) veya sıvı kristal ekran (LCD) içerir. SSMDB adına da görev yapmış olan mobil cihaz inceleme eğitimcilerinin katkısıyla hazırladığım ders müfredatında bulunan eski model cep telefonları ile akıllı cep telefonları arasındaki yazılımsal ve donanımsal farklar Çizelge 3.8 ve Çizelge 3.9 olarak sunulmuştur (Bireysel ders müfredatı, 2019) . Bu çizelgeler aynı zamanda cep telefonlarının günlük hayatımızın merkezine yerleşmelerinin sebeplerini gösteren bir farklar çizelgesi olarak değerlendirilebilir.

Çizelge 3.8 Mobil Cihazların Yazılımsal Özellikleri
(Bireysel ders müfredatı, 2019)

Kategori	**Eski Model Telefonlar**	**Akıllı Telefonlar**
İşletim Sistemi	Kapalı	Android, iOS, Windows, Blackberry
Aramalar	Ses	Ses Ve Video
Mesajlaşma	Metin	Multimedya
E-Posta	Metin Mesajı Yoluyla	POP IMAP Sağlayıcı Üzerinden
Web	WAP Gateway	Direkt HTTP

Çizelge 3.9 Mobil Cihazların Donanımsal Özellikleri
(Bireysel ders müfredatı, 2019)

Kategori	**Eski Model Telefonlar**	**Akıllı Telefonlar**
İşlemci Hızı	Sınırlı	Hızlı
Hafıza	Sınırlı	Geniş
Ekran	Küçük boyutlu renk ekran (12 bit-18 bit)	Büyük boy renk ekran (yaklaşık 24 bit)
Kamera	Yok	Var
Metin Girişi	Sayısal Tuş Takımı	Dokunmatik Ekran, QWERTY tuş takımı
Ses Girişi	Yok	Ses Tanıma
Konum Bilgisi	Yok	GPS verisi
Wireless	IrDA, Bluetooth	Bluethooth, Wifi, NFC

3.5.3.2. PDA (Personal Digital Assistant)

PDA ismi ilk defa Apple firmasının 1992'de tanıtmış olduğu zamanının yeni ürünü "Newton" cihazını tanıtmak için firmanın CEO'su J.Sculley tarafından kullanılmıştır. PDA cihazları avuç içine sığabilen boyutlarda, tuşlarla ya da kalem ile girdi yapılabilen, cep telefonu özelliği yanında faks gönderebilen, İnternet tarayıcısı olarak kullanılabilen ve kullanıcısına bireysel işlerini organize etme imkanı sağlayabilen ürünlerdir. Günümüzde yerlerini kullanımı çok daha kolay olan ve çok daha fazla özellik sunan akıllı cep telefonlarına ve diğer mobil cihazlara bırakmışlardır. Hatta PDA üretimi yapan firmalar bu değişimle birlikte üretimlerini tablet ve diğer mobil cihazların üretimi yönünde değiştirmişlerdir. [15]

3.5.3.3. SIM Kart

SIM kart, başta cep telefonları olmak üzere uygun özellikteki mobil cihazların bu servisin sağlayışı tarafından sunulan ses ve/veya data transferinden faydalanmasını sağlayan ve karta ait benzersiz kimlik verilerini içeren mikroçiptir. SIM kart tabiri, İngilizce'deki *Subscriber Identity Module* (Abone Kimlik Modülü) sözcüklerinin baş harfleri ile kart kelimesinin birleşiminden oluşmaktadır. Uygun özellikteki mobil cihazın içine yerleştirilen SIM kart GSM ağı ile irtibatlanır ve iletişim bu kart üzerinden gerçekleştirilir.[16]

SIM kartların ilk etapta 4-8 arası sayıdaki rakamlardan oluşan ve PIN numarası adı verilen bir kod ile güvenlikleri sağlanır. Mevcuttaki SIM kartların PIN şifreleri kırılamamaktadır ve unutulduğu taktirde kart imkanlarına yeniden erişim sağlamak

[15] Ayrıntılar için bknz. https://wmaraci.com/nedir/pda (Erişim Tarihi:09/02/2019)
[16] https://www.difose.com.tr/cep-telefonu-sim-kartlarinin-adli-incelenmesi/ (Erişim Tarihi:18/02/2019)

için PUK adı verilen ve servis sağlayıcı tarafından belirlenmiş bir koda ihtiyaç duyulur.

SIM kart hem işlemci hem de veri depolama birimi barındıran özel bir dizayna sahiptir. Depolama birimindeki dosya sistemi hiyerarşik bir yapıdadır. Standart bir SIM kart içerisinden rehber, gelen giden aramalar, kısa mesajlar ve kimi zaman da lokasyon bilgileri elde edilebilir.

SIM kart mobil cihazdan çıkarıldığında GSM üzerinden gerçekleştirilen iletişim yapılamaz ve SIM kart olmayan bir telefon sadece acil çağrı aramaları gerçekleştirebilir.

3.5.3.4. Hafıza Kartları

Bilişim sistemlerinde veri depolama kapasitesini artırmaya yaran veri depolama birimleridir. Cep telefonu, MP3 çalar, fotoğraf makinesi, tablet bilgisayar gibi birçok bilişim sisteminde ek veri depolama ünitesi olarak kullanılan hafıza kartları, adli bilişim açısından da çok önemli ve değerli veriler barındırabilmektedir.

Bahse konu hafıza kartlarının birçok farklı veri depolama kapasitesine sahip olmaları yanında şekil açısından da çok sayıda çeşidi bulunmaktadır. Compact flash kart (CF), smart media (SM) kart, secure drive/digital (SD) kart, multimedia card (MMC), microdrive, xD, memory stick, smart media ve memory stick pro duo gibi çeşidine ve kapasitesine göre birçok modeli ve markası üretilmiştir.

Birçok çeşidi bulunan hafıza kartlarının kullanıldıkları donanım ve bulunan ihtiyaca göre değişken kapasiteleri mevcuttur. Bir veri depolama ve veri yedekleme birimi olduğundan kapasitesi oranında mümkün olan her veriyi barındırabilir.[17]

[17] https://hukuksokagi.com/kaynak/adli-bilisim-computer-forensic/ (Erişim Tarihi: 09/02/2019)

Aynı şekilde cep telefonu cihazlarında da telefon marka modeline göre birçok farklı kapasite ve şekilde hafıza kartı kullanıldığı görülmektedir. Bu cihazların birçoğunda resim, video, diğer kullanıcı dosyaları, mesajlaşma veri tabanları ve işletim sistemi dosyaları gibi verileri tutmaktayken bir kısmında da daha hızlı erişim için rehber ve kısa mesajlar da yedeklenmektedir. Hafıza kartlarında da harddisklerde olduğu gibi yazılımsal olarak benzer, bununla birlikte donanımsal olarak bazı yönleriyle farklı yöntemler kullanılarak silinmiş verileri profesyonel olarak kurtarmak mümkündür.

3.5.3.5. GPS (The Global Positioning System)

GPS, küresel konumlama ya da konumlandırma sistemi ifadesinin kısaltmasıdır. Bu sistem dünyamız çevresinde bulunan uydular kanalıyla yeryüzündeki bir noktanın konumunu belirlemek için kullanırlar. Amacı dünya etrafında dönen uydular aracılığıyla yerdeki nesnelerin konumunu belirlemektir. GPS daha çok ABD Savunma Bakanlığı'nın uyduları üzerinden kullanılsa da Çin ve Rusya gibi ülkelerin uyduları üzerinde de kendilerine ait GPS sistemleri mevcuttur. Basitçe anlatılacak olursa sitemde uyduların saçtığı radyo sinyalleri GPS alıcı cihazlar tarafından yakalanır ve bu sinyaller çeşitli işlemler sonucunda konum bilgisi olarak çıktı verir.[18]

Sistemin ilk kuruluşunun amacı askeri işlerde kullanılması yönündeydi. GPS alıcıları askeri araçların yönlerini bulmalarında, çıkartmalarda, roket ve füzelerin hedeflerini vurmaları amacıyla doğru konumlandırma yapılması için kullanılmaktaydı. Bu durum 1983 yılında bir Kore sivil uçağının yanlış konum izlemesi nedeniyle yasaklanmış hava sahasına girmesi sonucu düşürülmesi sonrasında değişmiştir. 269 kişinin öldüğü kaza sonrasında GPS sistemi sivil kullanımına da açılmış olup günümüzde halen navigasyon, jeoloji, haritalama ve izleme gibi işlemler için de kullanılmaktadır.

[18] https://malzemebilimi.net/gps-nedir-nasil-calisir.html (Erişim Tarihi: 18/02/2019)

3.5.3.6. Tablet PC

Sadece tablet olarak ya da tablet bilgisayar olarak kullanılan mobil cihazlar genellikle kablosuz iletişim özelliğine sahip dokunmatik ekranlı ve bataryalı bilişim sistemleridir. Özel üretilmiş kalemlerin ve parmakların hareketlerini algılayabilen, klavye ve fare de kullanılabilen tabletler kamera, ışık, ivmeölçer ve jiroskop gibi donanım ve sensörler ile de donatılmış olabilirler. Dokunmatik ekrandan giriş imkanın yanında bazı özelliklerin kullanımı için ek fiziksel tuşlar içerebilmektedirler. Arama ve veri alış verişi özellikleri de bulunan birçok tablet modeli mevcuttur. Bu özellikleri ile akıllı telefonlar arasında fark görünmüyor gibiyse de ekranı 7 inç ve daha büyük olan cihazlar tablet sınıfında değerlendirilebilir. Bunun yanında akıllı telefon ve tabletin birleşiminden oluşturulmuş ve phablet adı verilen mobil cihazlardan da büyüktürler. 20. Yüzyılda üretilip geliştirilmeye başlanan tabletler 2010 yılı itibarıyla daha çok popüler olmuş ve minibook adı verilen mobil cihazların yerlerini almaya başlamıştır.[19]

Klavye çeşidine ve dış görünüşüne göre sınıflandırıldığında fiziksel klavye kullanmayan sanal klavye kullanan tabletlere "booklet" adı verilebilir. En bilindik booklet cihazlardan biri de Apple firmasının iPad model mobil cihazlarıdır. Hometech WI 10 ve ASUS Transformer Book gibi hibrid ve konvertibl olan tabletler ise her iki tür klavyeye de sahiptirleri. iPad Mini benzeri mini tabletler ile Galaxy Note 3 tarzı phabletler de tablet çeşitlerindendir.

3.5.3.7. Akıllı Saatler ve Diğer Giyilebilir Teknolojiler

Aksesuar ve kıyafet halinde giyilebilen ve kullanılabilen bilgisayar sistemi entegre edilmiş bilişim sistemleri "giyilebilir teknolojiler" olarak adlandırılmaktadır.

[19] Bilgisayarların tarihi gelişimi için bknz. https://www.teknonce.com/tablet-bilgisayar-nedir.html (Erişim Tarihi: 09/02/2019)

Akıllı saat adı verilen cihazlar için de şu aşamada giyilebilir teknolojilerin en önde gelenlerindendir denilebilir.

Akıllı saat, klasik bir saatten daha çok işleve sahiptir. Akıllı saatin en önemli özelliklerinden bir tanesi telefon gibi görüşme sağlamasıdır. Akıllı saate mesaj gelmekte, gelen mesajlar kullanıcı tarafından ret veya kabul edilebilmektedir. Akıllı saatin özelliklerinden biri de, sesli kullanım özelliğine sahip olmasıdır. Cihazda bulunan dâhili hoparlör ile kullanıcı, ahizesiz konuşma yapabilmektedir. Akıllı saatin içinde kamera özelliği bulunmaktadır. Akıllı saat, ses kaydetme özelliğine sahiptir.[20]

Bu özelliklerin yanında sağlıkla ilgili olarak adım sayabilen ve nabız ölçen, çocukların kaybolmaması için konumlandırma sistemi olarak kullanılan, "Google Glass TM" gibi gölüklerle insanları sanal dünyadaymış gibi hissettirebilen ve topladıkları ve işledikleri veriyi iletip alabilen özellikte birçok giyilebilir teknoloji de mevcuttur. Bu cihazlar da içerdikleri hassas ve kritik veriler açısından mobil cihaz adli bilişimi için çok değerli bulgular barındırabilmektedirler.

3.5.3.8. Drone

Drone, uzaktan kumanda veya önceden yazılım ile belirlenmiş komutlar ile otomatik olarak yönetilebilen ve yönlendirilebilen İnsansız Hava Aracıdır (İHA). Helikopter, pilot gibi gider ve maliyeti olmadığı için film çekimi, düşman hedeflerin takip edilmesi gibi askeri ve sivil kullanımda giderleri oldukça düşüren Drone etkin şekilde kullanılmaktadır. Günümüzde çok farklı şekil, ebat, konfigürasyon ve karakterde araçlar üretilmektedir.

İlk İHA'lar Vietnam Savaşı sırasında gövdelerine yerleştirilen kameralar ile film ve resim çeken uçaklardı. Bu uçaklar ya düz bir hat üzerinde veya dairesel hareketlerle uçar, görün,tüyü toplar, yakıtı bitene kadar uçar sonra yere inerdi. İnişten sonra

[20] https://www.sabah.com.tr/teknoloji/2016/05/31/akilli-saat-nedir (Et.: 18/02/2019)

resimler analistler tarafından çıkartılıp incelenirdi. Drone adı da verilen bu basit yapıdaki araçlar sadece uzaktan kumanda ile uçabilen basit bir uçaktı. Yeni nesil radyo frekanslarının kullanılmaya başlanması ile İHA'lar uzaktan kumanda ile çok daha fazla kullanılmaya başlandı ve "uzaktan kumandalı araç" terimi gelişti. Günümüzde birçok İHA hem uzaktan kumanda hem de bilgisayarlı otomasyon yardımı ile uçmaktadır. Daha gelişmiş sürümleri hız ve uçuş yolunu sabitleyen, yerleşik kontrol ve / veya rehberlik sistemlerinin yardımıyla düşük seviyeli insan pilot görevlerinde uçabilir.[21]

Bu araçların bazı modelleri belirtilen ve uluslararası standartlarda mobil cihaz adli bilişimi inceleme yazılımı olarak kullanılan Cellebrite UFED inceleme yazılımında incelenebilmektedir. UFED bu inceleme işlemi için Multimedia (çoklu ortam), Storage Extraction (depolama birimi çıkarımı) ve Storage Extraction (Recommended) (depolama birimi çıkarımı, önerilen) olmak üzere 3 başlık halinde seçenek sunmaktadır. Multimedia seçeneği ile IHA'dan çıkarılmış microSD hafıza kartı içerisindeki resim ve videolar alınır. Storage extraction metodunda IHA'nın hafızasına mikro USB portundan erişim sağlanır. Son seçenek ile ise dahili microSD kart çıkarılarak işlem yapılır. Storage extraction metodunda drone çalışır vaziyette olacağından karttaki veriler çıkarım tarihine kadar güncellenecektir. Bu açıdan raporda belirtilmesi gereken tarih değişimleri ve kayıtlarına ayrıca dikkat etmek gerekecektir. Tavsiye edilen metotta ise drone kapalı olacağından ekstra bir tarih güncellemesi olmayacaktır.

3.5.3.9. Kart Kopyalayıcılar ve ATM Skimmer

ATM skimmer, card skimmer gibi birçok farklı isimle anılan manyetik kart kopyalama cihazları bu manyetik alandaki kullanıcı bilgilerini okuyarak dijital veya analog olarak kaydederler. Bu kayıtlar, kötü niyetli insanlarca uygun yazılım, donanım veya şifreleme metoduyla okunabilir hale getirilerek yeni bir karta aktarma ya da çevrimiçi alışverişte kullanma yoluyla menfaat sağlanabilmektedir. Bu kopyalama

[21] İnsansız hava araçları için bknz. www.hurriyet.com.tr/teknoloji/drone-nedir-ne-ise-yarar-40502732 (Erişim Tarihi: 09/02/2019)

sistemlerine karşı çeşitli önlemler alınsa da kredi kartlarında bulunması gereken standartlar gereği farklı bir sistem kullanılmadığından halen kopyalama cihazları kötü niyetli kişilerce kullanılabilmektedir. Buna ek olarak bir kere cihazı yerleştirdikten sonra skimmer tarafından kaydedilen veriyi kablosuz olarak aktaran cihazlar ile temin etmek ve bu yolla da yakalanmamak mümkündür. Verilen bilgiye göre yetenekli bir suçlu tarafından bu cihazın bir benzin pompasına yerleştirilmesi 10 saniye gibi kısa bir sürede gerçekleştirilebilmektedir ve bunun yanında tespiti için de bazı yöntemler mevcuttur.[22] Uygun cihaz ve yazılımlar ile metro kartları, telefon kartları vb. kartların kopyalanması ve izinsiz ya da yasadışı olarak kullanılması mümkündür.

Bunun yanında Yakın Alan İletişimi – Near Field Communication (NFC) teknolojisi ile birlikte bu teknolojiyi kullanan kapı geçiş sistemleri ve ödeme sistemleri gibi sistemlerin güvenlikleri ve güvenlik ihlalleri durumunda neler yapılması gerektiği hususlarında adli bilişim alanında da eğitime ve geliştirilmeye ihtiyaç vardır. Örneğin kriptosuz olarak kullanılan bir mifare kart artık birçoğumuzun cebinde taşıdığı akıllı cep telefonlarındaki NFC okuma ve yazma özelliği ile kopyalanabilir ve başka bir karta kolayca kopyalanabilir.

[22] https://www.wivb.com/news/local-news/illegal-card-skimmers-now-using-bluetooth-to-steal/1491121517, (Et. 18/02/2019)

4. TARTIŞMA

4.1. CMK 134. Maddesi Kapsamı Dışında Kalan Adli Bilişim İncelemeleri, İleri Düzey Teknik Yöntemlerin Uygulanabilirliği ve Tartışmalı Konular

4.1.1. Müşteki, Mağdur ve Maktul Açısından CMK 134. Maddesi

Türkiye'de kolluk kuvvetleri ideal olarak müştekinin doğrudan başvurusu ile adli dijital veri incelemesi gerçekleştirmemektedir. İşlemlerin suiistimal edilebilme ve başvuranın müşteki sıfatının adli süreçte şüpheliye dönme ihtimalinin bulunması gibi sebeplerden dolayı ilgili işlemin bu şekilde uygulanma usulü uygun görünmektedir. Bununla birlikte müşteki ve maktul işlemleri için, dijital verinin hassasiyeti göz önünde bulundurularak kolluk kuvveti tarafından Cumhuriyet savcısından alınacak inceleme talimatı talep edilmektedir. Dolayısı ile konunun hukuki açıdan CMK 134. Maddesi hükümleri dışında kaldığı değerlendirilmektedir. Ancak teknik açıdan aynı hassasiyet gösterilmeli, dijital materyali ve bulgunun bütünlüğü ile güvenilirliğini sağlayacak, delil zincirinin sakatlanmadığını gösterecek iş akışları, standart ve prosedürler işletilmelidir.

Şüpheliye koruma amaçlı olarak tanınmış olan bir kopyanın müvekkiline veya kendisine verilmesi hükmü ile veri bütünlüğünü ve güvenilirliğini sağlayacak diğer tüm prosedürler, mağdur ve müşteki açısından da uygulanmalıdır.

4.1.2. İdari Soruşturmalarda CMK 134. Maddesi Uyarınca Karar Alınıp Alınamayacağı Hususunun Değerlendirilmesi

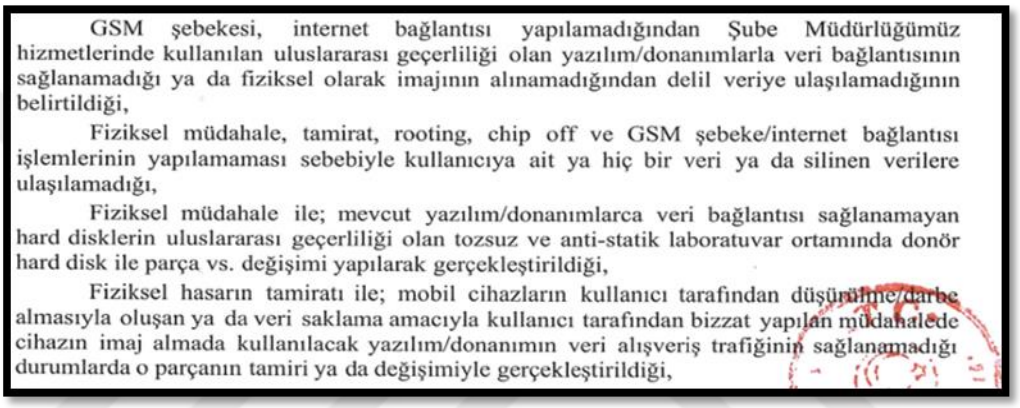
Adli bilişim inceleme adımlarının uygulanacağı bir diğer alan ise idari soruşturmalar olabilmektedir. İdari soruşturmalarda ise CMK 134. Maddesi uyarınca hakim kararı alınıp alınmayacağı hususu bir dönem tartışmalara neden olmuştur. Ancak, süreç içerisinde çeşitli mahkeme ve üst mahkemelerin verdiği kararlar ve yetkili adli makamların görüşleri doğrultusunda idareye ait olup da çalışanın kullanımına tahsis edilmiş bilişim sistemlerinin incelenmesi hakkında idarenin inceleme talebi bulunması halinde görevlendirilmiş kişilerce hakim kararı olmaksızın inceleme yapılabileceği görülmüştür. Bu durumun hukuki dayanaklarından biri olarak Yargıtay 9. Hukuk Dairesinin ittihaz etmiş olduğu 13.12.2010 tarih ve E:2009/44-K:2010/37516 sayılı kararı gösterilebilir. Kararın gerekçesinde "İşverenin kendisine ait bilgisayar ve e-mail adresleri ile bu adreslere gelen e-postaları her zaman denetleme yetkisinin bulunduğu" ifadesi geçmektedir. Bu karar doğrultusunda kuruma ait olan dijital materyaller üzerinde, ön inceleme, disiplin soruşturması ve diğer idari soruşturmalar ile teftiş ve denetim çalışmalarında ön inceleme ya da soruşturma görevlileri ile teftiş veya denetim yetkisi bulunanalar tarafından hakim kararı olmaksızın inceleme gerçekleştirilmesi mümkündür. Ek olarak Polis Vazife Ve Salahiyet Kanunu (PVSK) Ek. 7. Maddesi 9. Fıkrası ve 4483 Sayılı Kanunun 6. Maddesi ile İçişleri Bakanlığı Mülkiye Teftiş Kurulu Tüzüğünün 35. Maddesi doğrultusunda kuruma ait olan ve kurum görevleri için kişilerin kullanımına tahsis edilmiş dijital materyallerin disiplin soruşturması yapmaya yetkili disiplin amirleri veya denetim yetkisi bulunanlar tarafından hakim kararı olmaksızın incelenebileceği yetkili adli makamların görüşleri arasındadır.[23]

[23] 4/7/1934 tarihli kanunun tam metni için bknz.
http://www.mevzuat.gov.tr/MevzuatMetin/1.3.2559.pdf (Erişim Tarihi: 23.04.2019)

4.1.3. CMK 134. Maddesi ve İleri Düzey Teknik Yöntemlerin Kullanılabilme Durumu

CMK 134. Maddesinde doğrudan belirtilmemiş olan ancak adli bilişimde veri kurtarma ve gizlenmiş verilere ulaşabilmek adına ileri düzey ek tekniklerin uygulanması gerekebilmektedir. Gereklilik, ulaşılmak istenen dijital verinin normal yollardan ulaşılamıyor oluşu ve ancak ileri düzey teknik yöntemler (veri barındırmayan bozuk elektronik veya mekanik parçanın değiştirilmesi, tamiri, root, jailbreak vb.) kullanılarak ulaşılabilir oluşundan kaynaklanmaktadır. Bu durum hukuki açıdan rahatsız edici olabilecek olan "fiziki müdahale" tabiri ile tanımlanmaktaydı. Ancak dijital haldeki suç verilerine ulaşabilmek için gerçekleştirilmesi gereken teknik yöntemlerin uygulanması için CMK 134. Maddesinde anılmayan "fiziki müdahale" ibaresinin kolluk tarafından, taktir yetkilerinin kullanarak hakim inisiyatifi ile kararda geçirilmesi talep edilmekteydi. Bu talep, ileri düzey teknik yöntemler kullanılırken verinin tamamen kaybedilmesi veya cihazın kullanılmaz hale gelerek farklı hukuki sonuçlar doğurabileceği endişesi açısından makul sayılabilir. Ayrıca adli bilişim incelemesini usulüne uygun olarak gerçekleştiren kolluğun, bilirkişinin veya incelemecinin de böyle olumsuzluklara karşı bir güvencesinin olması, işlemlerin sağlığı açısından da önem taşımaktadır. Ancak, fiziksel müdahale ibaresinin mahkeme kararlarında belirtilmesi talepleri 3 farklı mahkeme kararı içeriği ile karşılaşılması sonucunu doğurmuştur. Bunun sebebinin, fiziksel müdahale tabirinin bu şekilde vurgulanan rahatsız edici algısı olduğu değerlendirilmektedir. İlk tip kararda "fiziki müdahale işlemine izin verilmesine" tabiri kullanılırken bir diğerinde CMK 134. Maddesinde böyle bir ibare bulunmadığından fiziki müdahaleye izin verilmemesine, üçüncü tip bir kararda ise ek tabir kullanılmasına yer olmadığına ve CMK 134 Maddesinin fiziki müdahale ve gerekli diğer teknik işlemleri gerçekleştirmek için yeterli olduğuna karar verilmiş oldu. Bu durum hukuki görüş alınmasını elzem kıldı ve yetersiz kalan fiziki müdahale tabiri geliştirilerek, veriye kısmen veya tamamen ulaşılamaması halinde gerekli teknik yöntemlerin (tamirat, rooting, j-tag, jailbreak, chip-off..) kullanılmasına, tespiti halinde şüpheliye ait şifreli bulut ve uzak sistem hesaplarına (facebook, twitter, gmail, google drive, web sunucusu vb.) ulaşılarak raporlanmasına, mobil cihazlarda bulunan bulgu dijital veriyi tespit için gerektirmesi halinde cihazdaki ilgili uygulamaların GSM şebekesine veya kurum

İnternet bağlantısından İnternete erişimine izin verilerek tespitlerin raporlanmasına şeklinde yetkili adli makamlara sunuldu. Yetkili adli makamlardan uluslararası standartlara uygun şekilde adli bilişim alanında diğer ülkelerde de uygulanan bu işlemlerin ülkemizde de verinin özgünlüğüne zarar vermeden ve işlemlerin dökümante edilmesi kaydıyla, CMK 134 Maddesi uyarınca alınan hakim kararı ile yapılabileceği, bu işlemin uygun şekilde uygulandığında kanun koyucunun cevaz vermek istemeyeceği durumlara yol açmayacağı görüşü alındı. Gerekli yerleri kapatılmış ve mahkeme kararları ve Cumhuriyet Başsavcılığı taleplerinden alınmış örnekler Şekil 4.1, 4.2 ve 4.3'te verilmiştir:



GSM şebekesi, internet bağlantısı yapılamadığından Şube Müdürlüğümüz hizmetlerinde kullanılan uluslararası geçerliliği olan yazılım/donanımlarla veri bağlantısının sağlanamadığı ya da fiziksel olarak imajının alınamadığından delil veriye ulaşılamadığının belirtildiği,

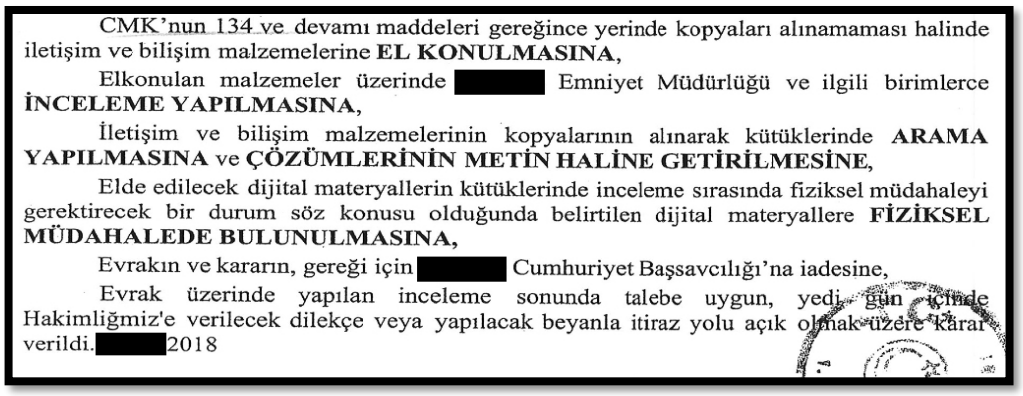
Fiziksel müdahale, tamirat, rooting, chip off ve GSM şebeke/internet bağlantısı işlemlerinin yapılamaması sebebiyle kullanıcıya ait ya hiç bir veri ya da silinen verilere ulaşılamadığı,

Fiziksel müdahale ile; mevcut yazılım/donanımlarca veri bağlantısı sağlanamayan hard disklerin uluslararası geçerliliği olan tozsuz ve anti-statik laboratuvar ortamında donör hard disk ile parça vs. değişimi yapılarak gerçekleştirildiği,

Fiziksel hasarın tamiratı ile; mobil cihazların kullanıcı tarafından düşürülme/darbe almasıyla oluşan ya da veri saklama amacıyla kullanıcı tarafından bizzat yapılan müdahalede cihazın imaj almada kullanılacak yazılım/donanımın veri alışveriş trafiğinin sağlanamadığı durumlarda o parçanın tamiri ya da değişimiyle gerçekleştirildiği,

Şekil 4.1 Cumhuriyet Başsavcılığı Talep Örneği

(Cumhuriyet savcılığı)



CMK'nun 134 ve devamı maddeleri gereğince yerinde kopyaları alınamaması halinde iletişim ve bilişim malzemelerine **EL KONULMASINA**,

Elkonulan malzemeler üzerinde [redacted] Emniyet Müdürlüğü ve ilgili birimlerce **İNCELEME YAPILMASINA**,

İletişim ve bilişim malzemelerinin kopyalarının alınarak kütüklerinde **ARAMA YAPILMASINA** ve **ÇÖZÜMLERİNİN METİN HALİNE GETİRİLMESİNE**,

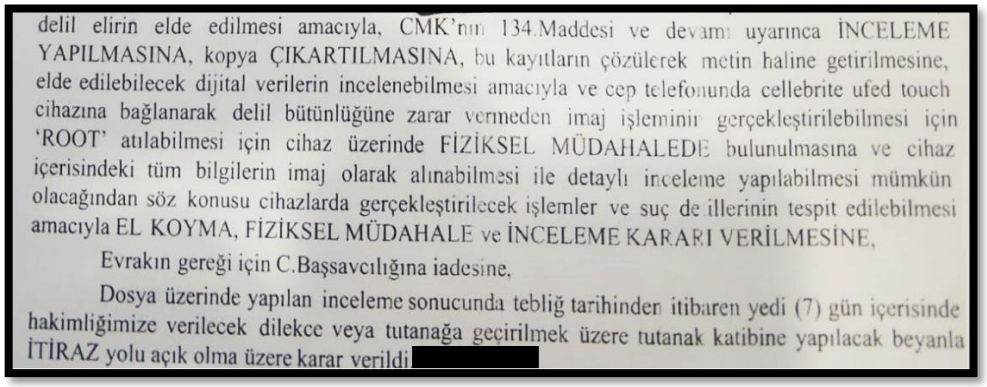
Elde edilecek dijital materyallerin kütüklerinde inceleme sırasında fiziksel müdahaleyi gerektirecek bir durum söz konusu olduğunda belirtilen dijital materyallere **FİZİKSEL MÜDAHALEDE BULUNULMASINA,**

Evrakın ve kararın, gereği için [redacted] Cumhuriyet Başsavcılığı'na iadesine,

Evrak üzerinde yapılan inceleme sonunda talebe uygun, yedi gün içinde Hakimliğimiz'e verilecek dilekçe veya yapılacak beyanla itiraz yolu açık olmak üzere karar verildi.[redacted]2018

Şekil 4.2 Uygun Bulunduğu Mahkeme Hükmü Örneği

(Adliye)



delil elirin elde edilmesi amacıyla, CMK'nın 134.Maddesi ve devamı uyarınca İNCELEME YAPILMASINA, kopya ÇIKARTILMASINA, bu kayıtların çözülerek metin haline getirilmesine, elde edilebilecek dijital verilerin incelenebilmesi amacıyla ve cep telefonunda cellebrite ufed touch cihazına bağlanarak delil bütünlüğüne zarar vermeden imaj işleminin gerçekleştirilebilmesi için 'ROOT' atılabilmesi için cihaz üzerinde FİZİKSEL MÜDAHALEDE bulunulmasına ve cihaz içerisindeki tüm bilgilerin imaj olarak alınabilmesi ile detaylı inceleme yapılabilmesi mümkün olacağından söz konusu cihazlarda gerçekleştirilecek işlemler ve suç delillerinin tespit edilebilmesi amacıyla EL KOYMA, FİZİKSEL MÜDAHALE ve İNCELEME KARARI VERİLMESİNE,

Evrakın gereği için C.Başsavcılığına iadesine,

Dosya üzerinde yapılan inceleme sonucunda tebliğ tarihinden itibaren yedi (7) gün içerisinde hakimliğimize verilecek dilekce veya tutanağa geçirilmek üzere tutanak katibine yapılacak beyanla İTİRAZ yolu açık olma üzere karar verildi [redacted]

Şekil 4.3 Uygun Bulunduğu Mahkeme Hükmü Örneği

(Adliye)

4.1.4. Mahkeme Kararında Dijital Materyal Özelliklerinin Geçmemesi, Olay Yerinde Tutulmuş Tutanakların Değerlendirilmesi ve Bu Evraklarda Sehven Gerçekleştirilmiş Maddi Hatalar

Bu bölüme kadar bahsedilen ana başlıklar ve alt başlıkları değerlendirildiğinde, bir adli bilişim incelemecisi açısından gerçekleştirilecek işlemlere dayanak olması için adli talimatın alınmış veya idari prosedürün usulüne göre işletilmiş olması gerektiği görülmektedir. Yani adli bilişim incelemecisinin aynı zamanda bu sürece de hakim olması ve gerekli kontrolleri yapabiliyor olması gereklidir. Adli talimat şüpheli, müşteki veya maktulün belirlenmiş dijital materyalleri hakkında verilmektedir. Başka bir deyişle incelenecek bilişim sistemlerinin özellikleri genel olarak CMK 134. Maddesi uyarınca alınmış kararda geçmektedir. Bununla birlikte olay yerinde karşılaşılabilecek diğer bilişim sistemleri öngörülemediği için kolluk tarafından tutulan tespit tutanakları da adli bilişim incelemecisi tarafından kontrol edilmelidir. Adli talimatta ve/veya ilintili tutanaklarda belirtilmemiş veya karışıklığa sebebiyet verecek şekilde yanlış belirtilmiş olan bilişim sistemleri ilgili makam veya birimden akıbeti araştırılmak üzere tutanağa geçilmeli ve incelenmemelidir. Tutanakta veya adli talimatta sehven olduğu ve ağır sayılamayacak hatalar kayıt altına alınarak işlemlere devam edilebilir. Bu durum adli sürecin tıkanmaması açısından önemlidir ancak maddi hatalar da mutlaka belirtilmelidir. İdari işlemler tarafında ise incelenmesi talep edilen bilişim sisteminin idareye ait olduğunu belirtir resmi beyan veya belgeler aranmalıdır.

4.1.5. CMK 134. Maddesi Doğrultusunda Alınan Hakim Kararında İncelemeci Birimin Belirtilmesi

CMK 134. Maddesi uyarınca alınmış hakim kararlarında adli süreçte karşılaşılan bir diğer sorun ise bilişim sistemi incelemesi yapması istenen birimin özellikle belirtilmesidir. Bu durum iki açıdan sorun teşkil edebilmektedir. Mahkeme kararı adli bir talimat olduğundan adli bilişim incelemesini gerçekleştirecek birim bu talimatı uygulamakla sorumludur. Ancak özel ve geçerli bir nedeni olmadan ve hatta başka bir birim de bu incelemeyi yapmaya kabiliyetli ise bu birimin özellikle belirtilmesi taraflı karar verilmiş olması olarak algılanabilir. Bir diğer sorun ise materyaller içerisinde farklı bir birimin çözme yeteneği olduğu materyallerin bulunması durumu olacaktır. Mahkeme kararında sabit bir birim belirtildiğinde incelemeyi veya bir başka ileri düzey teknik yöntemi uygulayabilecek diğer birim kendisi talimatta belirtilmediği için bunu incelemekte tereddüt edecektir. Bu durumda tekrar mahkeme kararı alınması istenir ve adli süreç istenmedik şekilde uzar. Bu sorunlar göz önünde bulundurularak adli bilişim incelemesini yapacak kişi veya kuruma soruşturmayı takip eden Cumhuriyet Savcısının karar vermesinde fayda vardır.

CMK 134. Maddesi uyarınca hakim kararı alınmamış bir suç soruşturmasında gerçekleştirilen arama neticesinde işyerindeki bilgisayarlardan elde edilen dijital bulgular "Müşteki vekilinin şikayeti üzerine başlatılan soruşturmada, 1. Sulh Ceza Mahkemesi'nin 21/08/2009 tarihli, 2009/1034 D. İş sayılı kararında, CMK'nın 119. maddesi uyarınca sanık tarafından işletilen iki ayrı işyerinde arama yapılmasına karar verilmesine karşın, aynı işyerinde bulunan bilgisayarlar üzerinde arama yapılabilmesine olanak tanıyan CMK'nın 134. maddesine göre verilmiş bir arama kararı bulunmadığı" gerekçesiyle Yargıtay 19. Ceza Dairesi 6.5.2015 tarihli, 2015/2092 Esas ve 2015/1175 karar numaralı kararı ile hukuka aykırı sayılmıştır. Bu bilgilere ek olarak bu bilgi de değerlendirildiğinde gerekli adli ve idari talimat ve prosedürlere uyulmadığı taktirde, bulgu suçu işaret etse dahi geçerliliği sakatlanacak

ve delil olarak sayılmayabilecektir. Yargıtay 19. Ceza Dairesi'nin bahse konu kararı aşağıdaki şekildedir:

T.C.

Yargıtay

19. Ceza Dairesi

Esas No:2015/2092

Karar No:2015/1175

K. Tarihi:6.5.2015

T.C.

YARGITAY 19. Ceza Dairesi

Esas: 2015/2092

Karar: 2015/1175

Yerel Mahkemece verilen hüküm temyiz edilmekle, başvurunun süresi ve kararın niteliği ile suç tarihine göre dosya incelendi, gereği görüşülüp düşünüldü:

Temyiz isteğinin reddi nedenleri bulunmadığından işin esasına geçildi.

Vicdani kanının oluştuğu duruşma sürecini yansıtan tutanaklar, belgeler ve gerekçe içeriğine göre yapılan incelemede;

Müşteki vekilinin şikayeti üzerine başlatılan soruşturmada, ...1. Sulh Ceza Mahkemesi'nin 21/08/2009 tarihli, 2009/1034 D. İş sayılı kararında, CMK'nın 119. maddesi uyarınca sanık tarafından işletilen iki ayrı işyerinde arama yapılmasına karar verilmesine karşın, aynı işyerinde bulunan bilgisayarlar üzerinde arama yapılabilmesine olanak tanıyan CMK'nın 134. maddesine göre verilmiş bir arama kararı bulunmadığı anlaşılmakla, işyerinde bulunan bilgisayarlar üzerinde yapılan arama sonucunda elkonulan ve içerisinde müşteki firmaya ait lisanssız yazılımların olduğu belirtilen harddiskler ve CD'ler hukuka aykırı delil niteliğinde olup hükme esas alınamayacağından, sanık hakkında verilen beraat kararı usul ve yasaya uygun görülmekle,

Eyleme ve yükletilen suça yönelik katılan vekilinin temyiz iddiaları yerinde görülmediğinden tebliğnameye uygun olarak, TEMYİZ DAVASININ ESASTAN REDDİYLE HÜKMÜN ONANMASINA, 06/05/2015 tarihinde oybirliğiyle karar verildi.”

4.1.6. Kovuşturma Aşamasında CMK 134. Maddesi Tedbirlerinin Uygulanabilirliği

Önceki bölümlerde de belirtildiği üzere CMK 134. Maddesi tedbirlerine, madde hükümleri gereği soruşturma evresinde ve başkaca delil elde etme imkanı bulunmadığı durumlarda başvurulması gerekmektedir. Bu açıdan Cumhuriyet savcısı tarafından hazırlanmış olan iddianamenin kabulü ile başlayan kovuşturma evresinde CMK 134. Maddesi tedbirlerine başvurulup başvurulamayacağı tartışma konusu olabilmektedir. CMK 134. Maddesi, özü gereği birey haklarını ve özel hayatlarının gizliliğini ihlal etmeden, suçla mücadelenin de kamu adına kamu yararına en etkin şekilde gerçekleştirilmesi gerektiği unutulmadan uygulanmalıdır. Bu yönlerden konu değerlendirildiğinde kovuşturma aşamasına geçildi ise soruşturma aşamasındaki süreçte elde edilen bazı bulguların suç ile ilişkili olabileceği kesin olarak kabul edilmiştir. Ancak süreç ilerledikçe bu bulguların yeterli olmadığı mahkeme ve hakim tarafından anlaşılabilir. Bu durumda başka kaynaklarda bulunabilecek başkaca bulguların değerlendirilmesi söz konusu olacaktır. Gelinen noktada hakim veya mahkemenin resen bulgu toplama durumu ya da sanık veya müdafinin lehe kullanılabilecek bulguları sunması durumları söz konusu olacaktır.

Yürürlükten kaldırılmış olan 1412 Sayılı Ceza Muhakemeleri Usulü Kanunu (CMUK) 237, 238 ve 239. Maddeleri incelendiğinde kovuşturma aşamasında mahkemenin resen bulgu toplama yetkisinin bulunduğu anlaşılmaktadır. Ancak bu maddelerin karşılığı sayılabilecek olan CMK 206 ve 207. Maddelerine bakıldığında mahkemenin resen bulgu toplamasının kapsam dışı kaldığı değerlendirilmektedir.[24] Tamamlanmamış, eksik kalmış soruşturma sonucunda mahkemenin Cumhuriyet savcısı yerine geçerek sanık aleyhine bulgu toplayan bir görevi edinmiş durumda kalabildiği gibi sanık ya da müdafi yerine geçerek sanık lehine bulgu toplayan taraf konumunda kalabileceği de değerlendirilebilir. Bu açıdan, CMK'nın kovuşturma aşamasında mahkemenin bulgu toplamaması yönünde olduğu değerlendirilen yeni anlayışının mahkemenin tarafsızlığı açısından uygun olduğu değerlendirilmektedir.

[24] Kanunun tam metni için bknz. http://www.mevzuat.gov.tr/MevzuatMetin/5.3.1412.pdf

Ancak yargılamanın amacının mutlak hakikate ulaşmak olduğu düşünüldüğünde kovuşturmada da olsa lehte ve aleyhte bulguların toplanması gerekmektedir. Kovuşturma aşamasına geçildikten sonraki süre de hesaplanırsa sanığın dijital materyallerde bulunacak verileri bu sürede yok etme ihtimalinin bulunmasından dolayı CMK 134 tedbirinin uygulanmasının faydası olmayacağı düşüncesi yanlış olacaktır. Bu bilgilerle birlikte CMK 190/1'e göre duruşmanın en kısa zamanda tamamlanması gerektiği ve CMK 134/1'e göre somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması hükümleri de mutlaka ilk değerlendirilecek hükümler arasında olması gerektiği unutulmamalıdır.

Bu açılardan ve özellikle kişi hakları ve özel hayatın gizliliği açısından, CMK 134. Maddesi tedbirlerinin uygulanması için soruşturma evresinin çok sağlam temellere oturtulması gerektiği ve elde edilen bulguların kuvvetli şüpheye dayanan somut olgular olması gerektiği aşikârdır. Bu bilgilerden hareketle mevcut bulguların kovuşturma aşamasında yetersiz kalması durumunda CMK 134. Maddesi tedbirinin uygulanması usulünün uygulanabileceği değerlendirilmektedir. Birey haklarının da korunması açısından inceleme kararının belirlenmiş başka bir mahkemede şeffaflık açısından hızlıca değerlendirilmesi ve tedbirin uygulanması yönünde aynı kanaate varması durumunda uygulanması şeklinde bir koruma mekanizması getirilmesinde fayda olacaktır.

4.1.7. PUK Bilgisinin Elde Edilmesi

Teknik detayları ilerleyen bölümlerde anlatılacak olan SIM (Subscriber Identity Module) kartlar GSM (Global System for Mobile) servis sağlayıcılarının telefon servislerinden kullanıcıların cep telefonları aracılığı ile kullanmalarını sağlayan bilişim sistemidir. SIM kart rehber bilgisi, abonelik bilgisi, şahsın telefon bilgisi ve kısa mesaj içerikleri ve bilgilerini içerebilmektedir.

Günümüz teknolojisinde üretilen SIM kartların güvenlik önlemlerinden biri olan PIN kodlarına atak yapılamamaktadır. Bununla birlikte PIN kodlarının unutulma

ihtimaline karşı PUK (Personal Unblocking Key) adı verilen 8 basamaklı rakamlardan oluşan bir kod tanımlanmıştır. PUK kodu kullanılarak SIM kart tekrar erişilebilir hale getirilir ve içerisindeki bilgiler okunabilir. SIM kartın erişilebilir hale gelmesi ile ulaşılabilecek diğer bilgiler ise, genellikle iki adımlı doğrulamalar için kısa mesaj kullanıldığı veriler olabilecektir.

Bu teknik hususlar değerlendirildiğinde SIM karta erişimin de suçun aydınlatılmasında önemli olduğu görülmektedir. Bu erişim sağlandığında birkaç yöntem daha kullanarak daha fazla veriye de ulaşabilme imkânı olduğu anlaşılmaktadır. SIM kartın bir bilişim sistemi olması sebebiyle yine CMK 134. Maddesi kapsamında değerlendirilmesi gerektiği tartışmasızdır. Farklı ülkelerde de PUK bilgisinin alınması için adli talep gerçekleştirilmesi gerektiği bilinmektedir (Bair, 2018, 81). Bununla birlikte PUK kodu ihtiyacı olduğunda, alınmış olan hâkim kararı doğrudan bu kodun alınmasını ön görmediği için Cumhuriyet savcısı talimatı ile ilgili talep GSM operatörlerine yazılmakta ve PUK kodları temin edilebilmektedir. Bu uygulamanın yerine olduğu değerlendirilmektedir. Ancak incelemeci SIM kartı aktive ettikten sonra ulaşma imkânı kazanacağı bilgilerden hangisini inceleyeceği konusunda dikkatli olmalıdır. Bu konu ile ilgili Cumhuriyet savcısı ile irtibatlı olunmasında fayda vardır. Örneğin hâkim kararı, şüphelinin evde kullandığı dijital materyalleri için çıkarılmış ise, SIM karta istenecek doğrulama kodu ile ulaşılabilecek bir e-posta verisine ulaşmak ve incelemek buradan elde edilebilecek bulgunun delil niteliğini sakatlayabilecek ve olumsuz hukuki sonuçlar doğurabilecektir.

4.1.8. Bilişim Sistemleri Açısından Müsadere

CMK 134. Maddesi uyarınca bilişim sisteminin iadesi söz konusu olduğundan müsadere uygulanmasının meri mevzuat açısından uygun olmadığı değerlendirilmektedir. Ancak çocuk istismarı, terör, organize suçlar vb. ağır suçların işlenmesi esnasında kullanılmış bilişim sistemlerinin mahkeme sonucu hükmün kesinleşmesi ile birlikte müsadere edilmesinin kamu yararına olacağı değerlendirilmektedir. Aksi ispat edilene kadar herkesin masum olduğu karinesi

nedeniyle mahkeme sürecinin tamamlanması beklenmelidir. Ancak bu durum fiziksel imaj olarak tabir edilen ve bilişim sisteminin bire bir kopyasının alındığı durumlar için uygulanmalıdır. Buradaki mantık, verilerin doğruluğunun ve bütünlüğünün gösterilmesi için orijinal materyale ihtiyaç olabilmesidir. Bunun yanında teknik imkânlardan dolayı her zaman bire bir kopya alınamayabilir ve silinmiş verilerin genellikle geri getirilemeyeceği ve mantıksal imaj adı verilen adli kopya türü alma yolu uygulanmış olabilir. Fiziksel imaj alınamadığı ve mantıksal imaj alınabildiği durumlarda müsadere konusu mahkeme tarafından değerlendirilmelidir. Bu durumda temyize başvurma süresi sonu da beklenebilir. Müsadere hükmü bilişim sistemleri için diğer eşyalardan farklı olarak değerlendirilmeli ve yine CMK 134 içerisinde ayrıca düzenlenmelidir.

Sadece Siber Suçlarla Mücadele Daire Başkanlığı ve bağlı birimleri tarafından 2018 yılında 631.233 dijital materyal incelemiştir.[25] Adli bilişim incelemelerinde şahıs başına ortalama 8 ila 12 dijital materyal ile karşılaşılmaktadır. Bu sayıların ortalaması alınırsa kişi başı 10 materyal düştüğü hesaplanabilir. Bu hesaplama sonucu 631.233 dijital materyalin 63.123 kişiye ait olduğu sonucuna ulaşılırsa bu sayının iki katı kadar da adli kopyalar için kullanılacak olan depolama birimine ihtiyaç olacaktır. Bu kaleme yapılan harcama düşünülürse müsadere işleminin bu açıdan da kamu yararı sağlayacağı değerlendirilebilir.

Müsadere edilen dijital materyaller aynı zamanda veri kurtarma işlemleri için donör parça ihtiyacını karşılayacak şekilde de değerlendirilebilir. Hasarlı, özellikle veya yanlışlıkla zarar verilmiş, suya atılmış vb. cihazlardan veri kurtarmak için bozuk parçaları tamir etmek veya değiştirmek gerekir. Tabi bu kısımlar veri içermeyen kısımlardır. Bozuk olan parçanın değiştirileceği sağlam parça donör olarak adlandırılır. Müsadere edilecek materyallerin yanında gümrükte kalmış, kaçak olarak yakalanmış ve belli zamanlarda imha edilen dijital materyaller de imha edilmeden bu amaçlar için kullanımı yönünde değerlendirilmelidir.

[25] İçişleri Bakanı Süleyman Soylu tarafından incelenen dijital materyal sayısı hakkında kamuoyu ile bilgi paylaşılmıştır. Açıklamanın ayrıntıları için bknz. (http://t24.com.tr/haber/soylu-incelenen-dijital-materyal-sayisini-acikladi-2018de-ortalama-45-binden-631-bin-233e-yukseldi,749982 (Et. 09/02/2019)

4.1.9. Tesadüfi Delillerin Değerlendirilmesi

CMK 134. Maddesi uyarınca bir suç araştırması için incelenmeye alınmış dijital materyal içerisinde bu suçtan farklı bir suç ile ilişkili bulgu da doğal olarak tespit edilebilir. Bu durumda "Tesadüfen Elde Edilen Deliller" başlıklı CMK 138. Maddesine göre hareket edilmelidir. Böyle bir tespit gerçekleştirilmesi durumunda bulgu doğrudan rapora işlenmemelidir. Tespit Cumhuriyet savcısına bildirilmeli ve alınacak olan talimata göre hareket edilmelidir.

4.1.10. Bölümün İrdelenmesi

7145 Sayılı kanun ile birinci fıkrada gerçekleştirilen değişiklik sonucunda hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından da inceleme kararı verilebilmektedir. Cumhuriyet savcısı tarafından bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine karar verildiği durumlarda bu karar 24 saat içerisinde hakim onayına sunulmak zorundadır. Hakim tarafından 24 saat içerisinde karar onaylanmaz veya süre dolması durumu yaşanırsa çıkarılan kopyaların ve çözümü yapılan metinlerin imha edilmesi gerekmektedir. Sonuç olarak Cumhuriyet savcısı tarafından verilen karar hakim tarafından da onaya sunulmak zorunda olduğundan suçla mücadele açısından bu sistem ideal olarak işletildiği taktirde adli ve hukuki sürece uygun olduğu değerlendirilmektedir. Bunun dayanağı dijital verinin çok hızlı bir şekilde yok edilebilme ihtimalinin bulunmasıdır. Ana anlayış olarak dijital veriden delil elde etmenin son çare olarak uygulandığı düşünülürse, başkaca delili olmayacak bir suçta bu veriye en kısa sürede ulaşabilmek suçun aydınlatılması için gereklidir. Ancak kişi hakları ve hürriyetleri açısından bakıldığında, bu maddenin işletilmesi önceki haline göre daha pratik olduğundan adli süreçte olmaması gereken keyfiyet sayılabilecek ve kanun ve hukuk ile bağdaşmayacak şekilde alınabilecek kararların yol açabileceği hak ihlalleri endişesi de doğal karşılanabilir. Bunun yanında Cumhuriyet savcılarının da kanun savunucu konumunda olduklarına ve kesinlikle

hukuk dışında karar vermeyeceklerine inanç tam olmalıdır. Teknik incelemeyi yapacak olan görevliler ile Cumhuriyet savcısının irtibatının da iyi olması gereklidir. Aksi taktirde silinmesi gereken verilerin silinmemesi veya unutulması gibi nedenler kişi hakları açısından olumsuz hukuki sonuçlar doğurabilir. Dijital verinin hassasiyeti, kişilerin hayatlarına dair birçok bilginin dijital materyallerde bulunabilmesi, bu verilerin kısa sürede kopyalanabilecek olması durumları da göz ününde bulundurularak kanun maddesinin kamu vicdanı açısından endişeye yer verilmeyecek şekilde uygulanması en doğrusu olacaktır.

İkinci fıkrada el koyma gerekçeleri arasına "işlemin uzun sürmesi" ihtimali de eklenmiştir. Aslında şifrelerin çözülememesi hususu bu konudan önce değerlendirilmelidir. Olay yerinde adli kopyası alınacak olan cihazın bir giriş şifresi olmayabilir. Bununla birlikte içerisinde sonradan karşılaşılabilecek şifreleme durumları bulunabilir. İlgili durumu anlayabilmek için olay yerinde canlı inceleme yapmak gerekli olacaktır. Ancak birçok durum için olay yerinde kapalı sistemlerde alınabilecek fiziksel imaj bu durumları önemsiz kılacaktır. Alınacak adli kopyanın fiziksel kopya olmaması ise hem silinmiş verilerin kurtarılamaması hem de diğer detaylı incelemelerin gerçekleştirilememesi ve şifrelerin çözümlenememesi anlamına gelebilir. Ek olarak işletim sistemi tarafından şifrelenmiş dosyalar da mevcuttur. Tüm bu şifre durumları el koyma gerekçesi olarak kullanılabilir. Ancak esas olan bütün işlemlerin olay yerinde sağlıklı bir şekilde bitirilmesi üzerine olmalıdır. İşlemin uzun sürmesi durumu ise kabul edilebilir gerekçe olabilir. Çünkü günümüzde birçok kişi boyutları gerçekten büyük bilişim sistemlerine sahiptir. Genellikle her evde her bireyin en az bir cep telefonu, bir dizüstü bilgisayar, bir masaüstü bilgisayar, bir tablet gibi birçok dijital materyal ile karşılaşılmaktadır. Bu durum ise veri boyutunun büyük olması nedeniyle olay yerinde geçirilecek sürenin uzaması ve bilişim sistemi çeşitliliğinden dolayı olay yerinde yeterli ekipmanın bulundurulup bulundurulamaması hususlarını gündeme getirmektedir. Süre açısından bir adli kopya alma cihazı olan Tableau Forensic Duplicator isimli cihazın bir modeli olan TD2U isimli modeli örnek verilebilir. Bu model en hızlı ve en güvenilir adli kopya alma cihazlarından biri olarak kullanılmaktadır. TD2U 1.3.0 Versiyonun kullanım kılavuzunda veri kopyalama hızının ölçülmesinde birim olarak 150 MB/Saniye veri

transfer kapasitesi olduğu ve saniyede 150.000.000 byte veri transfer ettiği varsayılan harddisk üzerinden ölçüm yapıldığı belirtilmektedir.[26] Aynı kılavuzda veri kopyalama hızının hash hesaplaması da aynı anda yapılmak suretiyle 16 GB/Dakika olduğu belirtilmektedir. Bu hız ideal hızdır ve gerçek olayların tamamına yakınında bu hız işlemin başından sonuna kadar korunmaz. Gerçek olaylarda örnek olarak 1 TB boyutundaki bir harddiskin adli kopyasının alınması ortalama 2 saat sürmektedir. Olay yerinde materyal bırakılacaksa bir de hash doğrulamasının gerçekleştirilmesi gerekmektedir ve bir 2 saat de bu hash doğrulaması için kullanılır. Yani 1 TB boyutundaki bir harddiskin adli kopyası için en az 4 saat zaman gereklidir. Kanun maddesi gereği bir adli kopya da şüpheli veya vekili için çıkartılması gerektiğinden aynı anda iki kopya çıkarma imkanı yok ise bir 4 saat daha bu işleme eklenmelidir veya disk-to-disk kopyalama yapılarak bu ek süre 2 saate düşürülebilir. Sonuç olarak 1 TB boyutundaki bir diskin adli bilişim işlemleri için olay yerinde ekipman yeterliliği doğrultusunda 4, 6 veya 8 saat zaman geçirilmesi gerektiği görülmektedir. Bu süreye işlemin teknik olarak sekteye uğraması durumunda başa dönme süresi, dokümantasyon ve tutanak işlem süreleri de eklenmelidir. Ek olarak bütün laboratuvar ekipmanlarını olay yerine taşımak da mümkün değildir. Bu nedenle karşılaşılabilecek beklenmedik bir dijital materyalin adli kopyasının olay yerinde alınması mümkün olamayabilecektir. Ev veya iş yeri sakinlerinin de uzun süre rahatsız edilmeleri söz konusu olacaktır. Belirtilen bu sebepler nedeniyle olay yerinde imaj alma işlemi optimal faydayı sağlayamayabilecektir. Bununla birlikte bir bilişim sistemine el konulması demek kişilerin birçok iş ve işlemlerinin aksaması veya durması anlamına gelebilecektir. Ek olarak, doğabilecek kişisel verilerin gizliliğinin ihlali endişeleri de dijital verinin çok çabuk şekilde çoğaltılabilmesi ve sızdırılabilmesi ihtimalinden dolayı doğal karşılanmalıdır.

Bu soruna sunulabilecek diğer ortak bir çözüm ise daha önce de bahsi geçen ve yine birçok farklı ülke kolluk kuvveti tarafından uygulanan "triage" yöntemidir. Triage kavramının başka bir tanımı da adli bilişim kapsamında objelerin öncelik veya önemine göre derecelendirilmesi şeklinde yapılabilir (Debrota ve ark, 2006: 26).

[26] https://www.guidancesoftware.com/docs/default-source/document-library/user-guide/td2u-forensic-duplicator-user-guide.pdf?sfvrsn=1ad48bad_16, (Et. 18/02/2019)

İhtiyaç olan verinin, yani öncelikli olarak suç ile ilgili olduğu değerlendirilen verinin kısa zamanda tespiti ve bu verinin bulgu olarak muhafaza edilmesi olarak da adlandırılabilir. Triage işlemi aslında ilk etapta ve genel manada olay yerinde canlı inceleme işlemine işaret eder. CMK 134. Maddesi incelendiğinde görülecektir ki bu kanun maddesi hükümleri öncelikli olarak olay yerinde incelemeyi işaret eder. Olay yerinde inceleme yapılması için aranacak verinin özelliklerinin iyi bilinmesi ve canlı gerçekleştirilen adli bilişim incelemesinde veri bütünlüğü çok hassas olacağından incelemeyi gerçekleştiren görevlinin gerçekten işinde ehil ve tecrübeli olması gereklidir. Bu nedenle triage işlemi gerçekleştirilecekse suç ile ilgili ön araştırma işleminin iyi yapılmış olması gerekmektedir. Bahse konu ön çalışma büyük oranda Cumhuriyet Savcılığı kontrolünde kolluk kuvveti eliyle gerçekleştirilmektedir. Zaten CMK 134. Maddesinde belirtildiği üzere dijital materyal üzerinde adli bilişim incelemesi gerçekleştirebilmek adına alınacak adli talimata yer olabilmesi için suç ile alakalı olarak başkaca delil elde etme imkânı bulunmamalıdır. Somut delillere dayanan kuvvetli şüphe varlığı hükmü ise kişi hak ve hürriyetleri açısından bir başka garanti konumundadır. Sözü edilen ön araştırma veya karara dayanak olacak bilgiler CMK 134. Maddesi uyarınca hakim kararı talep edilebilecek kadar güçlü olmalıdır. Uygulandığı takdirde olay yerinde asıl materyale el koymanın alternatifi olabilecek triage yöntemi çok titiz ve işinin ehli kişilerce uygulanması gerektiğinden ayrıca detaylı şekilde ele alınmalıdır. Ülkemiz adli bilişim işlemleri açısından değerlendirildiğinde, hukuki kaygıların bir bölümüne çare olabilecek bu yöntemi gerçekleştirebilecek personelin yetiştirilmesinin ve gerekli hukuki alt yapının oluşturulmasının sağlanması gerektiği görülmektedir.

Bu bilgilerden hareketle uygulamada kaygıların el koyma işleminin yapılıp yapılmaması veya bu kararların hangi merci tarafından verilmesinin uygun olacağı üzerinde yoğunlaştığı görülmektedir. Kanun koyucu CMK 134. Maddesi ile bilişim sistemleri üzerinde adli bilişim incelemesi gerçekleştirilebilmesi işlemlerini haklı olarak zorlaştırmaktadır. Dijital verinin hassasiyeti ve kırılganlığı açısından bu katı tutumun faydalı olduğu değerlendirilmektedir. Ancak bu katı tutuma rağmen hem adli makamlar ve kolluk kuvvetleri açısından hem de şüpheliler açısından birçok tartışma konusunun halen gündemde olduğu görülmektedir. Bu nedenle ideal bir adli bilişim

uygulaması için güven tesisisin kişi veya kurumlar üzerine değil, standartlar, iş akışları ve prosedürler üzerine kurulmuş ve kamu vicdanı tarafından ortak kabul görmüş bir sistem üzerine tesis edilmesi gerektiği düşünülmektedir. Gelişmiş ülkelerde mahkeme önünde değerlendirilen husus genellikle uygun ve güvenilir paydaşlarca oluşturulmuş sistematik akışın usulüne uygun takip edilip edilmediği ve delil zincirinin bozulup bozulmadığıdır. Yine ilerleyen bölümlerde ideal sistemin kurulmasında faydalı olabilecek sistematik adımlar ve iş akışı bilgileri verilecektir.

4.1.11. Çözüm Değerlendirmesi

Konu toparlanacak olursa, adli bilişim işlemlerinin birçok farklı boyutu olduğu görülmektedir. Bu farklı boyutların tamamı kanunlarda detaylı olarak belirtilemez. Bu adımlar yönerge veya yönetmelikler ile düzenlenmelidir. Bu nedenle öncelikli olarak dünya standartları değerlendirilerek hem hukuk alanında hem de teknik alanda adli bilişim uygulayıcılarının takip edecekleri ve uygulayacakları iş akışları ve prosedürler oluşturulmalıdır.

Bu değerlendirmeler eşliğinde, CMK 134. Maddesinde gerekli iyileştirmeler yapılarak dijital materyallerden elde edilecek bulguya olan ihtiyacın kuvvetli şüpheye dayanacak şekilde son çare olması, soruşturma evresinin sağlam temellere dayandırılması ve güçlü bir şekilde yürütülmesi sonucu adli talimatın isabetli şekilde alınması, teknik adli bilişim işlemlerinin en güvenilir yöntemleri kullanan uzman ve uzman yardımcısı sınıflandırmasına sahip eğitimli ve tecrübeli kişilerce yürütülmesi ve mümkün olan en kısa zamanda sonuçlandırılması şeklindeki kriter ilkelerin vazgeçilmez olarak benimsendiği, delil zincirini ön planda tutan bir iş akışına sahip yönerge veya yönetmeliğin oluşturularak bu modelin uygulanması ortak kamu vicdanının adalet hissiyatı açısından da gereklidir. Bu modelin oluşturulması için önerilebilecek kurul ise bu çalışma tarihi itibari ile adli bilişim alanında en çok materyal incelemesi tecrübesine sahip olan EGM Siber Suçlarla Mücadele Daire Başkanlığı'nın koordinesinde ilgili diğer kolluk kuvvetlerinin, adli makamların, uygun üniversitelerin, teknik yönü olan özel ve kamu tüzel kişilerinin katılımıyla

oluşturulabilecek kurul olacaktır. Burada ön plana çıkması gereken husus adalet ve hukuk kavramları bağlamında kişi haklarına saygı duyan ve ülke yararına en uygun sistemin oluşturulması olmalıdır. Diğer yandan Türk Akreditasyon Kurumu (TÜRKAK) ve Türk Standartları Enstitüsü (TSE) kurumlarının da bu sürece dahil edilerek donanım ve yazılım ile laboratuvar akreditasyonları, personel yeterliliğine standart kazandırılması gibi hususlarda destek alınması faydalı olacaktır. Örnek bir uygulama olarak olay yerinde kullanılabilecek olan yazılımlar uygulayıcı birimler ve kişiler tarafından sınırı belirlenmiş süre içerisinde test edilir. Test sonuçları kurulda değerlendirilir ve oy birliği ile kabul gören yazılımlar TSE tarafından halka açık olarak yayımlanır. Aynı şekilde benzer bir uygulama örneği olarak olay yerinde uygulanması gereken temel adımlar kontrol listesi olarak hazırlanır. Uyulması zorunlu olan bu adımlar kurul tarafından değerlendirilir ve yöntem TÜRKAK tarafından uluslararası standartlara da uygun şekilde akredite edilerek yayımlanır. Yayımlanan bu çalışmalar, teknolojik gelişmelere ve anlık gelişmelere bağlı olarak güncelleme gerektirebileceğinden yılın belli zamanlarda kurulun planlı toplantılar yapması ve plansız da olsa toplanarak en pratik şekilde çözüm üretebilmesi faydalı olacaktır.

4.2. Almanya ve Amerika Ülkelerindeki Hukuki Durum

Özellikle bu aşamada inceleme işlemlerine başlanması ya da el koyma işlemi gerçekleştirilmesi gibi asli hususlara karar verileceğinden önemli olan bu noktada diğer ülkelerin işlemlerine de göz atmak faydalı olacaktır.

Hukukumuzda dijital veriler ile alakalı olarak hem el koyma hem de inceleme açısından diğer eşyalardan farklı şekilde bir düzenleme yapıldığı buraya kadar irdelenen konulardan anlaşılmaktadır. Bunun gerekliliği ise tartışılmazdır. Adli bilişimin bu safhasında ise kanunun öngördüğü özelliklerden biri de arama ve el koymanın keyfi olmaması için önlem almış olmasıdır. Karşılaştırmak gerekirse, Amerikan hukukunda dijital verinin el konulması ve aranması ile ilgili ayrıca bir kanun ön görülmemiş olsa da olayda dijital materyal söz konusu ise yazılı birçok kanun

maddesinin ve düzenlemenin dikkate alınması gerektiği, alınmadığı taktirde de cezai sorumluluk gerektirdiği görülmektedir.

ABD'nin siber alanda işlenen suçlar ile ilgili olarak savunma, ilk müdahale ve operasyonel bütünleşme görevlendirmede amiral gemisi olarak bilinen Ulusal Sibersuç ve Haberleşme Entegrasyonu Merkezi'nin (NCCIC) United States Computer Emergency Rediness Team (US-CERT) isimli birimi tarafından verilen bilgilere göre göre, Amerikan hukukunda dijital materyal adli işlem konusu olacak ise üç kanun alanındaki düzenlemelere görevlilerin dikkat etmesi gerektiği görülmektedir.[27] Gereken üç hukuki düzenleme olarak Amerika Birleşik Devletleri Anayasası, yazılı yasalar (3 adet) ve duyum delil, en iyi delil ve delilin doğrulanabilirliği ve güvenilirliği bağlamında delil hakkındaki federal kurallar olarak gösterilmektedir.

Anayasaları açısından The Fourth Amendment olarak adlandırılan ve anayasadaki dördüncü ek madde olarak çevrilebilecek olan düzenleme ile arama ve el koyma işlemlerinde kesinlikle keyfiyete izin verilmediği gözlemlenmektedir. The Fifth Amendment (beşinci ek madde) ise kendi aleyhine tanıklık etmeye karşı koruma sağlamaktadır.

ABD'de dijital veri güvenliği açısından adli bilişim incelemelerinde de dikkat edilmesi gerektiği belirtilen 3 yazılı düzenleme olarak; "WireTap Act" (18 U.S. Code § 2511), "Pen Registers and Trap and Trace Devices Statute" (18 U.S. Code Chapter 206) ve "Stored Wired and Electronic Communication Act" (18 U.S. Code Chapter 121) düzenlemeleri gösterilmektedir.

WireTap Act isimli düzenlemede yetkilendirilmemiş kablo, elektronik veya konuşma iletişiminin dinlenmesinin yasaklanması, dinleme yapmak için gerekli adli talimatların alınma prosedürleri ile soruşturmacı ve kolluk kuvvetinin yetki ile elde etmiş olduğu verileri nasıl sunacağı hususlarına yer verilmektedir. Bahse konu düzenlemenin konusunun karşılığı ülkemizde CMK 135. Maddesinde belirtilen iletişimin tespiti hususu olduğu değerlendirilmektedir. Bununla birlikte CMK 134.

[27] https://www.us-cert.gov/sites/default/files/publications/forensics.pdf, (Et. 18/02/2019)

Maddesi tedbirlerinin uygulanması esnasında sonraki bölümlerde de belirtileceği üzere CMK 135. Maddesindeki tedbirlere başvurmayı gerektiren durumlarla karşılaşılabilecektir.

"Pen Registers and Trap and Trace Devices Statute" isimli tüzükte herhangi bir elektronik veya kablo iletişimini kaydeden yöntem veya cihaz (Pen Registers) ve yine benzer kayıt işlemleri gerçekleştiren tuzak ve izleme cihazları olarak tanımlanabilecek cihazların (Trap and Trace Devices) kullanımlarının düzenlendiği görülmektedir. Bu düzenlemenin ağ veya benzeri bir ortamda akan verinin adli olarak kopyalanması hakkında bir düzenleme yaptığı söylenebilir ve mobil cihazlarla alakasının kablolu veya kablosuz (WiFi, bluetooth, AirDrop vb.) iletişimleri esnasında verinin adli kopyasının alınması olarak gösterilebilir. İlgili düzenlemede bu cihazların kullanılması için öncelikli şartın bir mahkeme kararı olduğu belirtilmektedir. Bakım çalışması, kullanıcının veya servis sağlayıcının izni gibi durumlar dışında mahkeme kararının şart olduğu görülmektedir. İhlal edenlerin bir yıldan fazla olmamak şartıyla hapis cezası ile cezalandırıldığı da düzenlemeler arasındadır.

"Stored Wired and Electronic Communication Act" düzenlemesinde ise kaydedilmiş iletişime kanunsuz erişim, müşteriye ait kayıt ve iletişimin gönüllü ifşası, yedeklerin muhafaza altına alınması ve videoteyplerin kiralama veya satış kayıtlarının ifşası ve bunlar hakkındaki yaptırımlardan bahsedilmektedir.

ABD'ne siber güvenlikle alakalı ağ verisi ile ilgili olarak iki ana hukuki yönetim alanı vardır denmektedir. Bunlardan ilki veriyi toplamak ve izlemek için yetki alınmış olması ikincisi ise yöntemlerin kabul edilebilirliğidir. İlk alan için ABD Anayasası ve yazılı diğer kanunlar işletilirken ikinci alanı düzenleyen kurallar Federal kurallardır.

Ülkemiz ile karşılaştırmak gerekirse yetki alınması ve kullanılması kısmında Anayasa ve CMK 134. Maddesi eşdeğer olarak işletiliyor denilebilir. Ancak yöntemlerin doğruluğu açısından ülkemiz adli bilişim kurumlarının kendine has akış ve yöntem teyit mekanizmasını çizmesi gerekmektedir. Bu durum daha önce de bahsedildiği gibi ilgili kurum ve kuruluşların koordinesinde ortak olarak belirlenecek

delil zinciri sisteminin örneğin bu iş ile yoğun şekilde uğraşan SSMDB tarafından yönerge olarak çıkartılması ve diğer kurum ve kişilerce kabul edilmesi ile sağlanabilir. Bu çözüm önerisi ülkeye has ve kamu vicdanını rahatlatan bir model olacaktır.

Alman yetkililerle gerçekleştirilen toplantılarda Bundeskriminal ismi verilen birimin altında adli bilişim bulunmaktadır. Bu model doğrultusunda adli bilişime bir adli tıp bilim dalı olarak bakıldığı söylenebilir. Bu birim altındaki adli bilişim iş ve işlemlerinin ISO 17025 ve 17020 numaralı kriterleri doğrultusunda akredite edildiği görülmektedir. ISO 17025 standardına uygun bir laboratuvar, gerçekleştirdiği iş ve işlemler ile bunların sonuçları konusunda yetkin manasında gelmektedir. ISO 17020 standartlarında ise ürün, tesis, süreç ve iş akışlarının akredite edilmesine yönelik maddeler bulunmaktadır.[28]

Ayrıca işlemlerin normal arama prosedürlerine tabi olduğu, şüpheliye ait bilişim sistemlerinde uygulamanın öncelikli olarak el koyma olduğu, müşteki veya mağdura aitse olay yerinde bir an önce imajının alınıp orijinalinin geri verilmesi şeklinde olduğu bilgileri alınmıştır. Bu aşamaya kadar gelecek işlemlerde hazırlık aşamasının iyi yapıldığı bilinmektedir ve bunun gerekliliği çalışma içerisinde daha önce vurgulanmıştır.

4.3. Budapeşte Sözleşmesi ve Değerlendirme

Avrupa Konseyi (AK) bünyesinde hazırlanan ve AK üyesi olmayan ülkelerin de taraf olmasına imkân tanıyan, Sanal Ortamda İşlenen Suçlar Sözleşmesi olarak da bilinen sözleşmedir. 2001 yılında imzaya açılan ve 2004 yılında yürürlüğe giren sözleşmeyi ülkemiz 2010 yılında imzalamış, 6533 Sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun (2014, 22 Nisan) şeklinde ülkemizde kabul edilmiştir. Adli bilişimle alakalı olarak ilgili sözleşmenin sadece 31 ve 32. Maddeleri irdelenecek olursa, ilk eleştiri anlamında bir bilişim sistemi

28 https://www.bka.de/EN/OurTasks/SupportOfInvestigationAndPrevention/Technologies/technologies_node.html, (Et. 09/02/2019).

içerisinden taraf karşı ülkeden veri alınacaksa karşı tarafın iznini almak gerektiği görülmektedir. Eğer bu veriyi paylaşabilecek kanuni yetkiye sahip kişinin izni alınırsa karşı devletin iznini almak gerekmemektedir. Bu hükümler ciddi bir şekilde eleştirilmektedir. Bir görüşe göre bu hükümler ile bir kişinin rızası olduğu takdirde karşı ülkedeki yargı yetkisinin, konuyu icra eden ülke tarafından kullanılmakta olduğu şeklinde yorumlanmaktadır ve bu durumun düzeltilmesi gerektiği savunulmaktadır.

Diğer taraftan bakıldığında ise karşı devlet iradesi kişi iradesinin üzerine yazmaktadır. Burada rıza ve üzerine yazmak eylemleri tabi ki kanun hükümleri çerçevesinde kişinin veri üzerindeki tasarrufunun kaldırılması veya yetkili tarafından kullanılması şeklindedir. Kanunlarımızda rıza ile arama yapılmasının uygun olmadığı daha önce belirtilmişti. Önceki bakış açısı mantığıyla karşı ülkede kişinin izni alınarak ülkemizdeki bir bilişim sistemi üzerindeki veriler kendi adli çerçevemizin dışında incelenmiş olacaktır. Gelişen teknolojinin gereği olarak daha sonra da belirtilecek bulut teknolojisinde pratikte bu şekilde olmasa da teknik olarak buluttan kullanılan verilerin bir kısmının Avrupa kıtasındaki sunucularda bir kısmının ise Afrika kıtasındaki sunucularda olması muhtemeldir. Ancak kişinin şifre bilgileri ile giriş yapıldığında veriler toplu halde bulunur ve görülür. Bu açıdan örneğin şahsın GoogleDrive isimli bulut veri depolama sistemindeki hesabında bulunan veriler açısından CMK 134. Maddesi yeterli olarak düşünülmektedir. Fakat log, port bilgisi, IP bilgisi gibi ekstra bilgilerin gerekeceği durumlarda karşı taraf ile görüşmeye başlanması daha uygun olacaktır. Bulut servisinin kullanıldığı alanda anlık iletişim söz konusu olması muhtemel ise daha sonra da bahsedileceği gibi adli kopya alma süresince geçerli olacak CMK 135. Maddesi tedbirinin alınması faydalı olacaktır.

4.4. Teknik Boyutta Karşılaşılan Sorunlar ve Çözüm Tartışmaları

Günümüzde mobil cihaz adli bilişiminde hem delil zinciri açısından dikkat edilmesi gereken hem de teknolojik olarak araştırma geliştirme gerektiren birçok sorun ve engel ile karşılaşılmaktadır. Kullanıcı verisinin korunması odaklı olan yeni kriptolama sistemleri, işletim sistemi kısıtlamaları, verilerin bulutta tutuluyor olmaları,

cihazların kullanıcı tarafından kolayca hasar verilebilir olması, kullanılan birçok yazılımın yabancı ülke menşeili olması ve yeterince teknik destek sunmamaları gibi hususlar bu soruların başında gelmektedir. Kolluk kuvvetleri ve adli bilişim görevlileri açısından da geçerli olan bu sorunların büyük bir kısmı gelişen teknoloji ile birlikte gündeme gelmektedir. Devam eden bölümlerde ilişkili olgular ve kavramlar ortaya konacaktır. Bu kavram ve olguların ne gibi sorunlar ile bağlantılı oldukları ve mevcut veya muhtemel çözüm yolları irdelenecektir. Bazı yöntemler ve sorunlar açısından gerçek cihazlar üzerinde gerçekleştirilen testlere ve sonuçlarına da yer verilecektir. Bahsi geçen olgular, bu olgularla ilgili karşılaşılan sorunlar, uygulamadaki durumları ve çözüm önerileri takip eden şekildedir.

4.4.1. İmaj Alma Olgusu

İmaj alma, adli bilişim alanında adli kopyanın alınması manasında kullanılmaktadır. Bir bilişim sisteminin bit-by-bit tabir edilen ilk sektörden son sektöre kadar içerdiği bütün verilerin alınması şeklinde (fiziksel imaj) elde edilebileceği gibi verinin bir kısmının yedeğinin (mantıksal imaj) alınarak bunun adli özelliklere uygun hale getirilmesi yöntemi ile de elde edilebilir. Görüldüğü üzere adli bilişim literatüründe temelde iki tip imaj alma çeşidi vardır ve iki ana başlık mobil cihaz adli bilişimi alanı için de geçerlidir. Cihazın veya sisteminin izin vermiyor oluşu, teknik imkân bulunmuyor oluşu veya bilişim sisteminin hasarı gibi nedenlerden ya da verinin büyüklüğü sebebiyle gerekli kısmının alınmasına karar verilmiş olmasından dolayı fiziksel imaj alınamayabilir. Bu durumda mobil cihaz adli bilişiminde alınan adli kopyalar yaygın olarak dosya sistemi imajı ve mantıksal imaj olarak adlandırılmaktadır. Dosya sistemi imajı tabiri mobil cihaz adli bilişim alanında en yaygın kullanılan araçlardan olan Cellebrite UFED® ürününde kullanılmaktadır.

Dosya sistemi imajı aslında bir mantıksal imaj türüdür. Mantıksal imaj, çoğunlukla üreticilerin cihazları yedeklemek için kullandıkları yazılımlar aracılığı ile alınır. Örneğin Apple firmasının üretmiş olduğu iTunes yazılımı ile alınan yedekler

mantıksal imajlardır. Dosya sistemi imajı ise genellikle cihaza özel olarak üretilmiş benzer yazılımlar ile alınır.

Mobil cihazlarda imaj alınırken değinilebilecek en önemli husus hash kavramıdır. Çünkü birçok mobil cihazın imajı alınırken cihaz ile etkileşim halinde olmak gerekir ve cihaz çalıştığı için de ayrıca barındırdığı verilerde de değişiklik olacaktır. Değişiklik olan veriler cihaz hafızasının genellikle kullanıcı verisinin bulunduğu alanında değil sistem alanında olduğundan değerlendirmeler bu yönde yapılır. Tabi ki sistem alanındaki verilere de delil niteliği taşıyan bulgular olabilirler. Bu nedenle imaj alma işlemi mümkün olan en kısa sürede bitirilmelidir.

İmaj alma işlemi için mobil cihaz adli bilişimi yazılımları ajan adını verdikleri küçük yazılımlar yükleyebilmektedirler. Bu yöntemle adli kopya alınması durumunda işlemin vurgulanmasında fayda olacaktır. İşlemler delil zincirine uygun şekilde açıkça dokümante edilmelidir. Bu açıdan bakıldığında delil zincirinin mobil cihaz adli bilişimi açısından ayrıca önemli olduğu görülmektedir.

Cihaz açık olduğundan dolayı verilerde kabul edilebilir değişikliklerin olabileceği belirtilmiştir. Bu değişikliklerden dolayı mobil cihaz adli bilişiminde verinin değişmediğinin göstergesi olan hash algoritması normal uygulamalardan biraz farklı olarak kullanılabilir. Dosya sistemi veya mantıksal imaj alınıyor ise çıkarılan verilerin tamamının hash'lerinin hesaplatılması sağlanabilir veya veriler RAR vb. sıkıştırma yazılımları ile tek parça haline getirilerek bunun hash bilgisi çıkarılabilir.

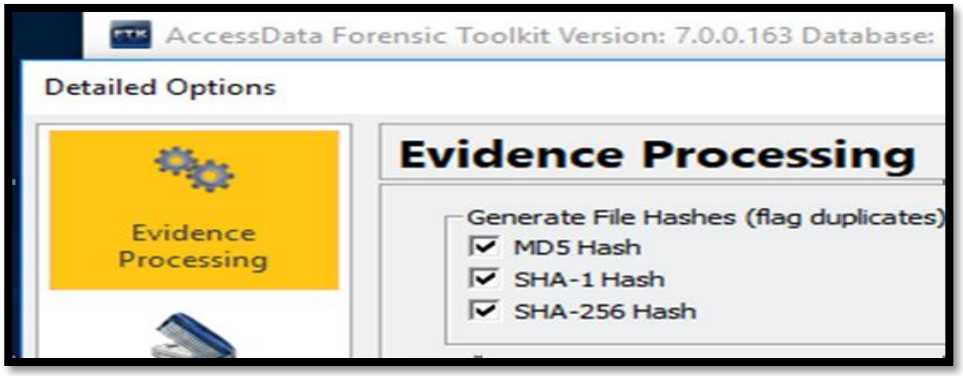
Mobil cihazlarda imaj alma işlemini etkileyebilecek bir diğer konu ise bağlantı protokolü ve yöntemleridir. Sorunlar fiziksel hasardan veya protokol ya da yöntemin desteklenmiyor oluşundan kaynaklanabilir. Suç tespiti için ulaşılması gereken veriler adalet açısından önemli olduğu için bütün yöntemlerin delil zincirine uygun şekilde uygulanmasında fayda olacaktır.

İmaj almak için bağlantı protokol ve yöntemleri kullanılamıyor veya alınan imaj içerisinden istenilen veriye erişilemiyor ise elle inceleme yöntemi kullanılabilir. Örneğin her cihazın fiziksel imajını almak mümkün değildir ve bazı cihazlarda fiziksel imaj alınamadığı durumlarda Whatsapp mesaj içeriklerine ulaşılamamaktadır. Bu durumda elle inceleme ile mesajlar kayıt altına alınabilir. Alınan imaj içerisinden istenilen veriye erişilememesinin nedenleri ilerleyen bölümlerde verilecek olan bilgilerle pekiştirilecektir. Elle inceleme yöntemine delil zincirine uygun şekilde geçilir ve incelenen veriler kayıt altına alınır. Kayıt altına alma için sürekli bir video kaydı yapmak ve bu videoyu kayıt sonunda hash bilgisi ile saklamak ya da bu iş için üretilmiş Eclipse adı verilen cihazlar ile hash bilgisi tutularak fotoğraflanması sağlanabilir. [29]

4.4.2. Hash Olgusu

Hash algoritmaları ile alakalı olarak devam eden tanımlar yapılabilir. Hash, orijinal diziyi temsil eden değerden daha kısa sabit uzunluktaki değere veya anahtara dönüştürülmesidir. Bir başka deyişle değişken uzunluktaki bir verileri sabit uzunluktaki verilere indirgeyen sayısal işlemlerdir. Hash fonksiyonu, bir girdi değerini sıkıştırılmış sayısal değere dönüştüren matematiksel bir işlevdir. Hash işlevi için girdi keyfi uzunluktadır, ancak çıktı her zaman sabit uzunluktadır. Tipik olarak uzunlukları 128 bit ve 512 bit arasında olup en çok bilinen algoritmalar MD5, SHA1, SHA256, SHA512, CRC32 ve HAVAL isimleri ile anılırlar. Adli bilişim alanında ise en çok MD5, SHA1 ve SHA256 algoritmaları kullanılmaktadır. Aşağıda güçlü ve ticari bir adli bilişim yazılımı olan AccessData firmasına ait Forensic Toolkit (FTK) yazılımının bu çalışma tarihi itibarıyla en güncel versiyonu olan 7.0.0.163 versiyonunun işlem seçenekleri penceresinden alınmış Şekil 4.4'te hangi hash algoritmalarını kullandığı görülmektedir:

[29] Bknz. (http://www.teeltech.com/mobile-device-forensic-tools/eclipse-3-pro-kit/, (Et. 09/02/2019)



Şekil 4.4 FTK 7.0.0.163 Hash Algoritmaları
(Accessdata, 2018)

Hash algoritmalarının güvenilir olmasının sebepleri arasında fonksiyonların geri döndürülemez olması ve 1 bit veri dahi değişse sonuç olarak çıkacak olan özet verinin değişecek olması sayılabilir. Ancak bu bilgiler yanında MD5'in açıkları olduğu ve güvenilmez olduğu iddiaları da mevcuttur. Gerçekleştirilen çalışmalar incelendiğinde MD5 algoritmasında içeriği farklı olduğu halde aynı MD5 değerine sahip verilerin oluşturulabildiği görülmektedir.[30] Bu bilgiler değerlendirildiğinde örnek olarak çalışmada verilen verilerin MD5 değerlerinin aynı olduğu iddia edilmiştir. Veriler içeriklerinde bazı farklılıklar olsa da MD5 değeri olarak aynı değeri vermektedirler ve fakat SHA1 değerleri farklı çıkmaktadır. Ancak bu çakışma çok küçük boyuttaki veriler için geçerli olabilmektedir. Bu durum karşısında MD5 kullanımının adli bilişimde kullanımının güvensiz olduğu çıkarılmamalıdır. Öyle ki bir disk imajı için aynı MD5 değerine sahip fakat içeriği farklı iki imaja rastlanması halen pratik olarak imkânsız kabul edilmektedir.

Bir diğer çalışmada ise aktarım yöntemlerine ve depolama türüne göre değerlendirilen durumlarda aktarılan ve mobil cihazlardan elde edilen verilerin hash bilgilerinin önceki hallerine göre değişiklik gösterip göstermediği araştırılmıştır (Ayers ve ark, 2009). Araştırma neticesinde aktarılan grafik dosyalarında, bluetooth ile aktarılan verilerde, MicroSD kart ve telefon arasında aktarım olan verilerde, duvar kâğıdı ve kamera ile çekilmiş olup incelenmek üzere dışarı aktarılan resim dosyalarının hash bilgilerinde tutarlılık görülmüştür. Bununla birlikte resim ekleyip mesaj olarak gönderme servisi olan Multimedia Messaging (MMS) servisi

[30] https://www.mathstat.dal.ca/~selinger/md5collision/, (Et. 18/02/2019)

kullanıldığında farklı telefon aileleri arasında gönderilen resimlerde ve gelen MMS'teki resmin tekrar MMS olarak gönderilmesinde ilk dosya ile ikincisi arasında hash tutarsızlıkları görülmüştür. Bu açıdan değerlendirildiğinde aktarılan birçok verinin hash bilgisinin kaynaktaki ile aynı olacağı görülmekle birlikte verilerin mobil cihazlardan delil zincirine uygun şekilde aktarıldığının dökümante edilmesinin ve hash bilgilerine yer verilmesinin uygun olacağı değerlendirilmektedir.

Hash algoritmasının bir diğer kullanım alanı ise işletim sistemine ait veriler gibi suçla alakası olmadığı bilinen verilerin önceden oluşturulmuş ve bu verilerin hash setlerini içeren dosyalar ile karşılaştırıp inceleme sürecini hızlandırmak adına veri işleme süreci dışında tutmaktır. Benzer şekilde bir diğer alan, çocuk istismarı verilerinin önceden tespit edilen suç verileri kullanılarak hash setlerin oluşturulması ve bulgu bilişim sistemindeki verilerin hash bilgileri ile karşılaştırılarak suç verisinin tespit edilmesi yöntemidir. National Center for Missing and Exploited Children (NCMEC) ve Interpol gibi kuruluşlar bu hash setlerini güncel tutarak kolluk kuvvetleri ile de paylaşmaktadırlar. İki ülke arasında doğal olarak veri paylaşımı bazı prosedürlere tabidir. Ancak bilinmelidir ki hash bilgisi kullanılarak orijinal veri elde edilemez ve bu açıdan paylaşılmasında hiçbir sakınca yoktur. Aksine çocuk istismarının önlenmesi gibi çok önemli bir mücadele için hash seti veri tabanı genişletilmeli ve tespit edilen hash setlerin paylaşımında ise tereddüt edilmemelidir.

4.4.3. İleri Düzey Teknik Yöntemler ve Zorluklar

İleri düzey teknik yöntemler başlığı ile anlatılmak istenen mobil cihazlarda bulunan verilere normal bağlantı yolları veya yöntemlerle ulaşılamadığı durumlarda daha fazla uzmanlık gerektirebilecek ve belli ölçüde de veri kaybı riski taşıyabilen veriye ulaşma yöntemleridir. Belirtilen risk suç verisine ulaşmak için göze alınabilecek bir risk olmalıdır ve diğer bütün yollar denenmiş olmalıdır. Riskin göze alınabilme durumu ise bulgu veriye hali hazırda zaten erişilemiyor olmasıdır.

İleri düzey teknik yöntemler arasında rootlama, jailbreak, joint test action group (J-TAG), chip-off, in-system programming (ISP) gibi yöntemler sayılabilir. Bu yöntemler ile veriye erişim sağlandıktan sonra verilerin imajının alınması ve anlamlandırılması için programlayıcı, okuyucu ve box cihazları adları verilen cihazlar kullanılır. Sayılan yöntemlerin detaylandırıldığı farklı bir çalışmada ayrıca tanımlarının yapılmasının daha faydalı olacağı değerlendirildiğinden bu çalışmada tanımlarına değil zorluklarına yer verilecektir.

Bu yöntemlere ihtiyaç duyulmasının sebepleri arasında üreticilerin kullanıcı verilerini korumak amaçlı olarak geliştirdikleri yeni teknoloji yazılım ve işletim sistemlerinin kullanılması, cihazlara çeşitli şifreler konulması ve bu şifrelerin bir kısmının bu yollarla aşılabiliyor olması, cihazların kasten veya başka sebeplerle hasarlanmış olması gibi sebepler sayılabilir. Ancak bir teknoloji geliştirildiğinde bir süre sonra bu teknolojinin getirdiği güvenliği aşmak için karşı yöntemler de geliştirilmektedir. Örneğin 2009 yıllında yaygınlaşmaya başlayan Android işletim sistemli telefonların desen kilidi (pattern lock) adı verilen güvenlik sistemi o zamanlar için geçilmesi zor bir güvenlik sistemiydi. Ancak araştırmacıları telefon hafızasına fiziksel erişim sağladıklarında bu kilide ait şifrenin SHA1 hash bilgisinin gesture.key isimli bir dosyada olduğunu tespit ettiler (Github, 2012). Bu dosyaya erişim sağlayan bir phyton kodu oluşturulup SHA1 hash bilgisine sözlük ya da önceden hesaplanmış tablolar veya bruteforce yöntemi ile atak yapılarak şifrelerin geçilmesi sağlandı. Bu açıdan değerlendirildiğinde üzerinde yeterince çalışıldığında birçok güvenlik yöntemine karşı yöntem geliştirme imkânı olduğu anlaşılmaktadır.

Hukuki boyut irdelenirken değinildiği üzere bu yöntemlerin ülkemizde kullanılması için CMK 134. Maddesi tedbirleri yeterli olmaktadır. Bununla birlikte takip eden Cumhuriyet savcısının bilgisi dahilinde bir sonraki aşamaya geçmek uygun olacaktır.

İleri düzey teknik yöntemlerin uygulanması ihtiyacı en çok Android ve iOS işletim sistemli cihazlarda ortaya çıkmaktadır. Bahse konu her iki işletim sistemine sahip cihazlar kullanılmaya başlandıkları ilk günden itibaren veri güvenliği konusunda

çok ileri seviyelere gelmişlerdir. Kullandıkları ekran şifreleri, telefon hafızasındaki verileri şifreleme metotları, kendilerine özgü işletim sistemleri, güvenlik yamaları, parmak izi ve yüz haritası güvenlikleri gibi teknolojik önlemlerle kullanıcılara ileri düzey veri güvenliği sağlamaya çalışırken bu cihazların suçta kullanılması durumunda kolluk kuvvetlerine de suç verisine ulaşmada ciddi engeller getirmektedir. Bu nedenle devam eden bölümlerde veri güvenliği ve suç verisine ulaşma bağlamında sözü edilen iki işletim sistemi ana başlıklar olacak şekilde irdelenen güvenlik aşamalarının güçlü ve zayıf yanlarının değerlendirilmesi yapılacaktır.

4.4.4. Apple ve Veri Güvenliği

Apple firmasının tarihçesine baktığımızda bilindiği üzere Steve JOBS tarafından iki arkadaşıyla (Steve Wozniak ve Ronald Wayne) beraber 1 Nisan 1976 yılında Kaliforniya'da hayata geçirildiği görülmektedir. İlk iPhone cihaz ise 9 Ocak 2007 yılında tanıtılmış, aynı yılın 29 Haziranında piyasaya sürülmüş olan modeldir. Apple, iOS ve MacOS gibi çok popüler işletim sistemlerinin de sahibidir. iOS, Apple firmasının üretmiş olduğu iPhone, iPad ve iPod cihazlarında kullanılmaktadır. Bu cihazlardan en yaygın olanı iPhone akıllı cep telefonlarıdır.

IPhone telefonlarda ilk günden bu yana ön planda olan kullanıcı verisi katı güvenlik anlayışının özellikle 4S modeli ve sonrasında 64 bit mimariye sahip işlemci kullanımı ile birlikte katlandığı görülmektedir.

4.4.4.1. iOS Veri Şifreleme Sistemi Direnci

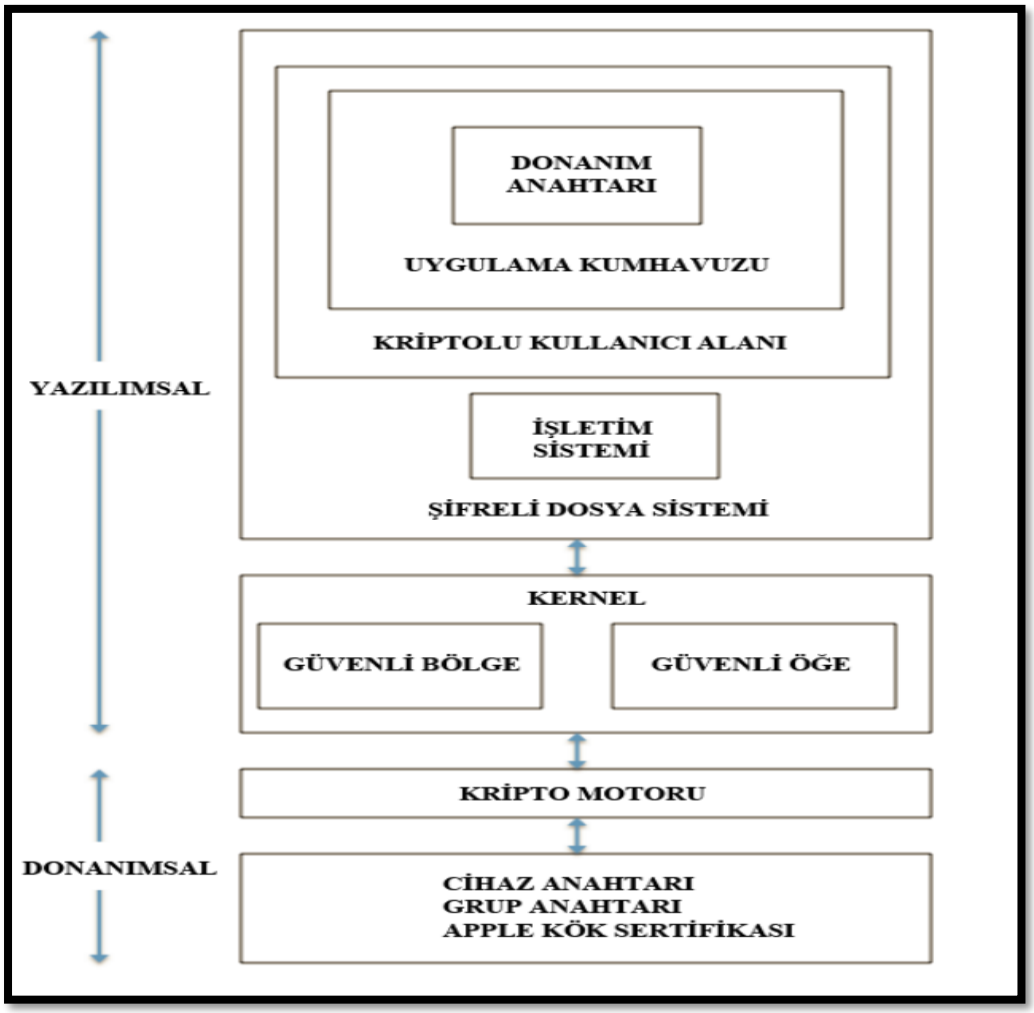
Apple firması iOS işletim sistemi güvenlik basamakları üzerinde yüksek seviye bir değerlendirme yapılırsa en tepede yazılımsal ve donanımsal olarak adlandırılabilecek iki ana başlık altında veri kriptolama işlemlerini gerçekleştirdiği

söylenebilir.[31] Şekil 4.5'te bu kriptolama sisteminin üst seviye bir şeması bulunmaktadır. Donanımsal şifrelemede verilerin cihaz veri depolama çipi üzerinde tutulurken kriptolu tutulması ve belirlenen yöntemlere göre de kriptolu veya açık olarak okunması söz konusudur. Donanımsal şifreleme sisteminin temellerini uniqueID (UID), group ID (GID) ve AES-256 bit anahtar kavramları oluşturur. UID, 256 bit bir AES anahtarıdır ve cihazın işlemcisi içerisindeki silikona gömülmüştür ve AES kripto motoru dışında farklı bir yolla okunamaz. Apple, UID anahtarının her cihaz için benzersiz olduğunu söyler. GID ise aynı işlemciye sahip cihazlar için aynı olan bir diğer anahtardır. UID bilgisi işlemci dışına sadece matematiksel olarak çıkar, dışarıdan okumak için işlemci içerisindeki silikona ciddi ve sofistike atak yapmak gereklidir (Doğanay, 2018).

Donanımsal şifreleme ile gerçekleştirilen işlem neticesi bir sonraki aşama olarak yazılımsal şifreleme ile buluşturulur. Buna ek olarak dosyaların açıkken, kapalıyken ve/veya kullanıcı ilk izni verene kadar korunmasına ya da korumasız olmasına göre sınıflandırılarak bir sınıf anahtarı şifrelemeye dahil edilir. Şekil 4.6'da gösterildiği üzere kabaca donanımsal şifreleme, kullanıcı şifresi, sınıfına göre belirlenmiş anahtar, dosya sistemi anahtarı, her dosya için büyük oranda farklı olacak olan dosya üst verisi kullanılarak üretilmiş per-file adı verilen anahtarlar kullanılarak dosya içeriği şifrelenir. Burada kullanıcı şifresi, yani ekran şifresinin de şifrelemeye dahil edildiğini görmekteyiz. Bu da ekran şifresi ne kadar karmaşık olursa bu sisteme tersine mühendislik uygulamanın o kadar zorlaşacağı anlamına gelmektedir. Bu yollarla üretilen şifreler cihaz veri depolama çipinde effaceable yani silinebilir alan adı verilen yere yazılır ve ihtiyaç olduğunda buradan okunurlar. Bu mantıkla yukarıdaki sisteme sahip bir cihazda verileri erişilmez hale getirmek için kullanıcı verilerinin üzerlerine yazmakla uğraşmak yerine, silinebilir alandaki anahtarları geri dönüştürülemeyecek şekilde silmek ki çok daha kısa sürecektir, kriptografik olarak verilerin erişilmez olması anlamına gelecektir.

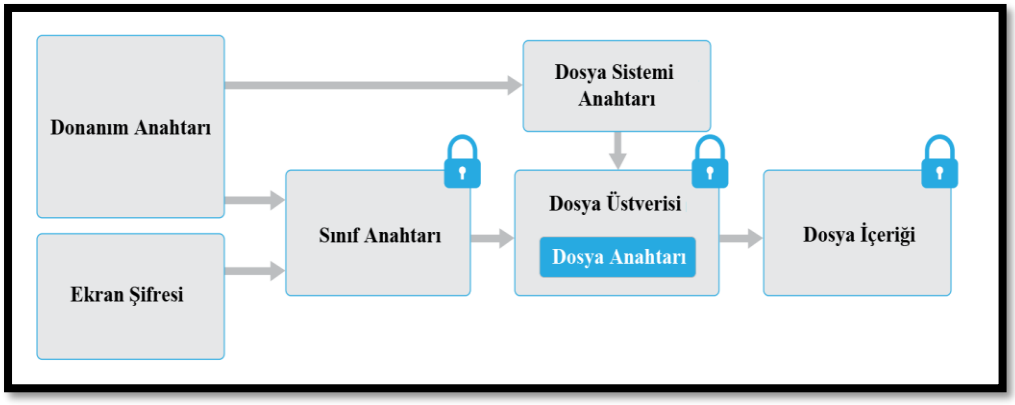
[31] https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf, (18/02/2019)

Apple cihazların şifreleme/kriptolama elemanları ile algoritmalar bilinmeden ulaşılsa bile veri içeriğinin okunabilir hale getirilmesinin Apple firması dışındaki bir çözümle mümkün görünmediği değerlendirilmektedir.



Şekil 4.5 iOS Yazılımsal ve Donanımsal Şifreleme Üst Seviye Şeması

(Apple Inc., 2019)



Şekil 4.6 iOS Yazılımsal Şifreleme Adımları

(Apple Inc., 2019)

4.4.4.2. iOS Veri Şifreleme Sistemi Zayıflığı

iOS veri şifreleme sisteminin tersine mühendislik ve birçok atak yöntemine karşı fazlasıyla dirençli olduğu görülmektedir. Ancak her kompleks sistemin bir zayıflığı olduğu gibi bu sistemin de bazı zayıflıkları bulunmaktadır. Model ve iOS versiyonuna bağlı olarak değişiklik gösteren ve istismar edilen açıklara işletim sistemi güncellemeleri ile gelen açıklar ve çeşitli yazılım ve donanımlar ile kırılabilen kullanıcı şifreleri örnek verilebilir. Yeni güncellemeler ile gelen açıklar kullanıcı verilerine izinsiz erişim imkânı sağlayabilmekle beraber, bu açıkları tespit eden kişilerin bildirmesi veya kendilerinin tespit etmesi sonucunda üretici tarafından sunulan yeni güncellemeler ile kapatılmaktadır.

Veri güvenliği açısından diğer bir zafiyet ise kullanıcı şifresinin, diğer bir deyişle ekran kilidinin çeşitli yazılım ve donanımlar ile kırılabiliyor olmasıdır. Bu alanda en çok bilinen cihazlardan bir tanesi 2015 yılında adını duyurmaya başlamış olan IP-Box isimli cihazdır. iPhone model telefonlarda şifre ataklarına karşı aynı zamanda 10 yanlış deneme yapıldığı taktirde telefonun otomatik olarak sıfırlanmasını sağlayan bir güvenlik seçeneği mevcuttur. Manuel şifre ataklarına karşı, fazla yanlış deneme olması durumunda, takip eden şifre denemeleri arasına aşamalı olarak artan bekleme süreleri

tanımlanmış, belli bir sayıda denemenin üzerinde de cihazın etkin değil durumuna düşmesi sağlanarak Apple tarafından ek bir güvenlik önlemi alınmaya çalışılmıştır. IP-Box cihazı ise ekran ve aynı zamanda USB arabiriminden etkileşimde bulunarak bu güvenlik önlemlerini aşmış, bir süre revaçta kalmış ve iOS 8.1.1 ve altı versiyonlarında şifre kırma işlemi yapılabilmiştir.[32] Apple, iOS 8.1.1 sürümünden sonra ise bu açığı kapattığı ve IP-Box cihazının kullanımının azaldığı bilinmektedir.

iPhone cihazların birçok iOS versiyonu ekran şifrelerine atak yapabildiği bilinen yazılım ve donanım bütünün en popülerleri Cellebrite Advanced Services (CAS) ve sonrasında piyasaya sürülmüş olan GreyKey isimli ürünlerdir. CAS ürününün iOS 5 versiyonundan iOS 11 versiyonu aralığındaki işletim sistemine sahip olan iPhone 4S'ten iPhone X modellerine kadar olan iPhone modelleri ile iPad, iPad mini, iPad Pro ve iPod modellerini desteklediği bilinmektedir ("Cellebrite", t.y.). Bunun yanında sadece Amerika ve Kanada ülkelerinin kolluk kuvvetlerine satıldığı bilinen GreyKey isimli diğer ürün ise iOS 9 ve üzerindeki işletim sistemine sahip cihazların şifrelerini kırdığı çeşitli kaynaklardan anlaşılmaktadır. GreyKey cihazının Apple firmasından ayrılan eski bir çalışanı tarafından üretildiği de mevcut bilgiler arasındadır. Bu çalışma tarihi itibarıyla en güncel iOS versiyonu 12.1.3 versiyonudur.

iPhone kullanıcı şifresi konusunun en çok gündeme geldiği olaylardan bir tanesi Aralık 2015 yılında gerçekleşen ve 14 kişinin hayatını kaybettiği San Bernardino saldırısıdır. Bu saldırıdan sonra saldırgana ait bir iPhone 5C marka model telefonun ekran şifresi Federal Bureau of Investigation (FBI) tarafından kırdırılmaya çalışılmıştır.

Bilgilere göre FBI, San Bernardino olayında cihaz şifresinin kırılmasının 1.3 milyon dolara mal olduğu görülmektedir. Resmi devlet kayıtlarına göre FBI'ın Cellebrite ile gerçekleştirdiği telefon kilitlerinin açılması için 187 adet kontrat yaptığı ve telefon başına ortalama 10.833 dolar ödendiği söylenmektedir.[33] (Aynı bilgilere

[32] https://appleinsider.com/articles/15/03/18/new-ip-box-tool-bypasses-10-try-limit-for-pins-on-older-ios-versions-automates-brute-force-attacks, (Et. 09/02/2019)
[33] https://www.forbes.com/sites/stevemorgan/2016/04/06/u-s-governments-multi-million-dollar-mobile-forensics-shopping-spree-revealed/#52b94d11b0df, (Et. 18/02/2019)

göre ise FBI'ın mobil cihaz adli bilişimine 2 milyon dolar para harcadığı görülmektedir. Diğer bir bilgiye göre, 218.000 dolarlık resmi bir harcama kaydının duyurulması ile San Bernardino zanlısının telefonunun başarılı şekilde açıldığının bildirilmesi olaylarının aynı gün açıklanması nedeniyle bu harcamanın bahse konu iPhone 5C telefonun şifresinin harcanmasına bağlandığı belirtilmektedir.[34] Aynı bilgilere göre, FBI'ın Cellebrite ile bir çalışma yaptığı, ancak çözen firmanın Cellebrite firması olmadığını duyurduğu görülmektedir. Ancak bu bilgilere telefonun açılmasını takip eden zamanlarda Cellebrite firmasının market değerinin önemli ölçüde yükseliş gösterdiğine değinilmiştir. Bununla birlikte FBI konu ile alakalı Apple firmasından da yardım talep etmiştir (Electronic Privacy Information Center, 2018). Apple firmasının icloud verileri ile ilgili yardımcı olduğu ancak telefonun şifresinin açılması ile alakalı olarak iPhone kullanıcılarının güvenliğini ve gizliliğini düşündükleri için yardımcı olmadıkları haberlere yansıtılmıştır. Ek olarak Apple kendilerine bu yönde bir mahkeme kararı çıkartılmasına rağmen Random Access Memory'de (RAM) çalışacak ve cihazı açacak bir yazılım yapmanın Anayasa ve bazı diğer kanunlarına aykırı olduğu ile ilgili açıklamada bulunmuştur. Diğer bir bakış açısıyla bu işlemin gerçekleştirilemeyeceğini söylememiştir. Bu olaylar neticesinde Apple firmasının müşteri verilerinin güvenliğine önem verdiği, Cellebrite firmasının birçok mobil cihazın şifresine atak yapabildiği ve FBI'ın görevinin gereğini yaparak veriye ulaşacak bir çözüm yolu bulabildiği gösterilmiştir.

Bu olaylar cereyan ederken Cambridge Üniversitesi'nde görevli olan araştırmacı Dr. Sergei Skorobogatov mobil cihazın çipini sökerek kendi dizayn ettiği maliyeti ucuz bir düzenekle iPhone 5C cihazında güvenlik önlemlerine takılmadan şifre atağı yapabilme yöntemi keşfettiğini duyurmuştur (Paganini, 2016). Nand Mirroring adı verilen yöntemi kullanan sistemdeki risk veri depolama çipinin sökülmesi gerektiğidir. Dr. Skorobogatov, yeterli teknik kapasiteye sahip herkesin bu yöntemi uygulayabileceğini söylemiştir. Ancak gerçekleştirilen çalışmalarda görülmüştür ki özellikle eski model iPhone cep telefonlarda zarar vermeden veri depolama çipini sökme oranı % 50 olarak ölçülmüştür. Bunun nedeni olarak üzerinde

[34] https://money.cnn.com/2016/03/31/technology/cellebrite-fbi-phone/, (Et: 09/02/2019)

çalışılan cihazların eski model cihazlar olduğu değerlendirilmiştir. Dolayısıyla Dr. Skorobogatov'un çalışmış olduğu yöntem bu açıdan belli riskler içermektedir.

Müşterilerin veri güvenliğini yüksek seviyeli olarak ön planda tuttuğu görülen Apple firmasının bu amaç için aşırı güçlü şifreleme algoritma ve yöntemleri üreten ekibinin kolaylıkla düşünüp şifre kırma ataklarına karşı aktive edebileceği USB kısıtlama önlemini neden geç getirdiği değerlendirme konusu olmalıdır. Bu özellik, 1 saat boyunca kullanıcı şifresi girilmediğinde USB veri alış veriş özelliğini devre dışı bırakmakta, bu yolla CAS ve GreyKey ürünlerini devre dışı bırakabileceği görülmekte olan 9 Temmuz 2018 tarihinde sunulmuş 11.4.1 iOS versiyonu ile hayata geçirilmiştir. Sonraki versiyonlarda bu özellik güçlendirilse de 11.4.1 versiyonunda bir telefonun bu moda girmemesi için hemen şarja takılmasının yeterli olacağı keşfedilmiştir. Burada husus cihazın bu moda girmesini ertelemektir. Yani cihaz USB kısıtlı moda girdiyse cihaza USB veri yolu ile erişmek için ekran şifresinin girilmesinden başka yol yoktur.

Bu çalışma açısından teknik çıkarım ise iPhone cep telefonlarının şifrelerinin belli durumlarda kırılabilme yöntemlerinin var olduğunun anlaşılmasıdır. Ancak şifreleme algoritmaları, iOS işletim sistemi çalışma prensipleri ve cihazın fiziksel özellikleri düşünüldüğünde şifre kırma işlemlerinin en sağlıklı şekilde RAM'de çalışan bir yazılım ile yapılabileceği anlaşılmaktadır. Cellebrite CAS ve GreyKey cihazlarının çalışma mantıklarının bu şekilde olduğu bilinmektedir. Bu alanda yeterli çalışma yapıldığı taktirde cihaz şifrelerinin kırılması için yöntemlerin inşa edilebileceği değerlendirilmektedir.

4.4.4.3. Apple Cihazlarda Parmak İzi Güvenliği (TouchID) Aşma Yöntemi

TouchID, bazı iPhone, iPad ve Mac cihaz modellerinde cihaz yeniden başlatıldığında, 48 saat şifre girilmediğinde, yeni bir parmak izi tanımlanacağında veya silineceğinde, 5 kez tanınmayan parmak izi ile deneme yapıldığında, şifre değiştirilmek istendiğinde ve Mac cihazda oturum kapatıldığında devreye almak için cihaz şifresinin girilmesi gereken parmak izi kullanılan güvenlik yöntemidir. Sistemin

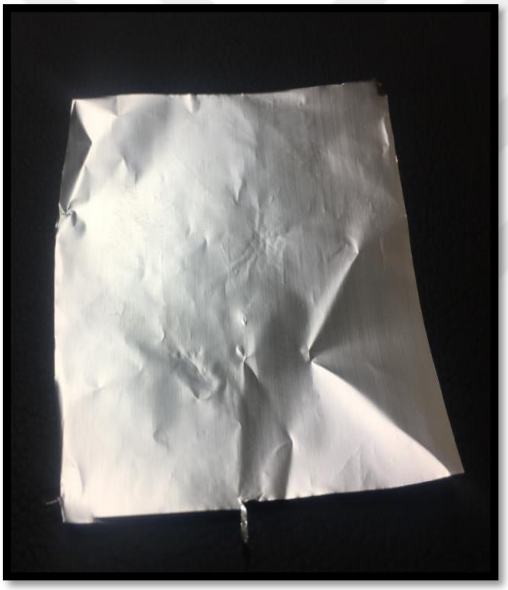
kapasitif dokunuş (capacitive touch) özelliği olan bir parmak izi okuma entegresi ile çalıştığı bilinmektedir.[35] Diğer bir deyişle parmak izi okuma entegresi izini okuyacağı parmağın iletkenliği ile de ilgilenmektedir. Parmak izi okuma entegresinin algılamaya çalıştığı izin bir canlıya ait olup olmadığını anlama testini kapasitif dokunuş özelliğini kullanarak yaptığı söylenebilir. Bu bilgiler ışığında belli özelliklere sahip ve yeterli iletkenliğe sahip sahte bir parmak izi ile sistemin yanıltılabileceği değerlendirilmektedir. Yanıltma işleminin gerçekleştirilip geçekleştirilmeyeceğini göstermek amacıyla tekrarlanan test yöntem ve sonuçları aşağıdaki gibi sunulmuştur.

TouchID sistemi üzerinde test yapılması için iPhone 6S (A1633) ve Apple Macbook Pro Touch Bar (A1707) cihazları tercih edilmiştir (Laboratuvar Uygulamaları, 2019) . Testte, 4.7, 4.8, 4.9 ve 4.10 numaralı şekillerde gösterildiği gibi bir sıcak silikon tabancası, silikon bar, alüminyum folyo ve beyaz tutkal malzemeleri kullanılmıştır.

[35] https://support.apple.com/en-gb/HT204587, (Et. 09/02/2019)

Şekil 4.7 Silikon Tabancası

Şekil 4.8 Beyaz Tutkal Ön



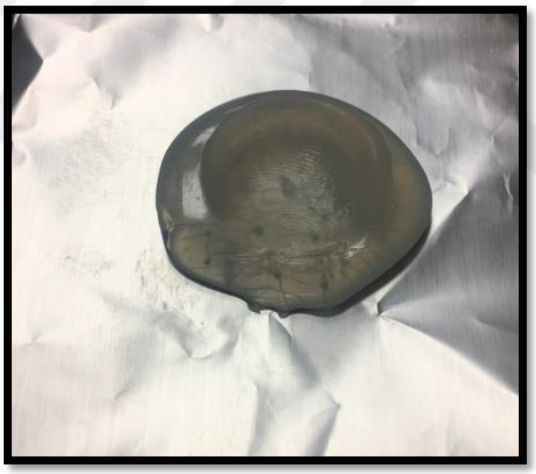
Şekil 4.9 Alüminyum Folyo

Şekil 4.10 Beyaz Tutkal Arka

(Laboratuvar Uygulamaları, 2019)

Silikon tabancası ısıtılarak silikon barın yeterli erimişliğe ulaşması sağlanmış ve alüminyum folyo üzerine sağ el başparmağının izi çıkarılabilecek miktarda bırakılmıştır. Yeteri kadar soğuduktan sonra sağ el başparmak izi silikon üzerine çıkacak şekilde parmak silikon üzerine bastırılmıştır. Bir süre bekledikten sonra parmak silikondan ayrılmış ve 2 saat boyunca silikon kurumaya bırakılmıştır. Kuruyan silikon (Şekil 4.11) üzerine parmak izinin ters bir görüntüsü çıkmış olup, beyaz tutkal ile doldurulduğunda parmak izinin doğru şeklinin çıkması beklenmiştir. Beyaz tutkalın

donarak gerekli şekli alması için 12 saat beklenmiştir. 12 saat sonunda beyaz tutkal silikondan ayrılmıştır. Test cihazlarına sağ el başparmak izi tanımlanmıştır. İşlemin bundan sonraki aşaması video olarak kayıt altına alınmıştır.[36] Videoda, işaretlenmiş olup cihazlarda tanımlı olmayan diğer parmak izleri kullanılarak cihazların açılmadığı gösterilmiş, cihazları açmayan bu parmaklar altına üretilmiş olan sahte parmak izi konularak cihazların açılması denenmiştir. Üretilen sahte parmak izinin iki cihazı da başarılı şekilde açtığı görülmüştür. Aradan 6 saat geçmesinden sonra sahte parmak izi tekrar denendiğinde cihazları açmadığı görülmüştür. Sahte parmak izi ıslatılarak tekrar denendiğinde, cihazları yeniden açacak özelliği kazandığı görülmüştür. Bu durum, bu yolla üretilmiş olan sahte parmak izinin zaman geçtikçe iletkenliğini kaybettiği, sıvı teması ile kapasitif dokunuş sisteminin algılayabileceği yeterli iletkenliğe tekrar kavuştuğu şeklinde yorumlanmıştır.



Şekil 4.11 Silikon Parmak İzi Kalıbı

(Laboratuvar Uygulamaları, 2019)

Uygulanan teste ait sonuçlar veri güvenliği açısından değerlendirildiğinde bir şekilde elde edilebilecek olan doğru parmak izi ile kullanıcı verilerine erişilebileceği ve bu açıdan istismar edilebileceği düşünülmektedir. Diğer taraftan parmak izi veri tabanındaki dijital parmak izlerini uygun hale getirecek yazılımın yazılması ve bu çevrimin doğru iletkenlikteki maddeyi kullanan üç boyutlu yazıcılarda kullanılarak sahte parmak izinin üretilmesi ile kolluk kuvvetleri tarafından suç verisine ulaşmak için kullanılabileceği düşünülmektedir.

[36] Videoya erişim için bknz. https://youtu.be/Y6RDHy5B2P4, (Et. 23/04/2019)

4.5. Android İşletim Sistemi ve Kullanan Cihazlar

Android işletim sistemi koşturan mobil cihazlarda yönetici izni kazanmak, her türlü yazılımı yükleyebilmek, kısacası sisteme tam erişim sağlamak için rootlama ismi verilen bir işlem gerçekleştirilmektedir. Rootlama işlemi ile dosya sisteminin izin vermediği verilere ulaşım veya cihazın fiziksel imajının alınması sağlanabilir. Ancak android ve android işletim sistemi koşturan cihazların geliştirici ve üreticileri tarafından güvenlik önlemleri de geliştirilmektedir. Bu açıdan mantık, verinin dosya sisteminin veya cihazın izin verdiği kadar erişilebilir olması, bunun dışındaki erişim yöntemlerine karşı korumalı olması yönünde kurulmaktadır. Bu açıdan konu değerlendirildiğinde Android 5'ten beri tam disk şifrelemesi Android 7'den beri de dosya bazlı ve üst veri şifrelemesi kullanılmaktadır ("Android", t.y.). Ek olarak özellikle Android 7 ve sonrası işletim sistemini koşturan cihazlarda, daha öncesinde rootlandığında cihazın hafızasına tam erişim sağlanabilirken, yeni önlem olarak cihaza root atma imkanı bulunsa bile birçok cihazda bu işlem artık cihaz tamamen sıfırlanmadan gerçekleştirilememektedir. Güvenlik önlemleri genellikle güvenlik yaması adı verilen güncellemeler ile de desteklenmektedir. Bununla birlikte daha öncesinde fiziksel olarak verilerine erişilemeyen ağustos 2018 ve öncesi güvenlik yamasına sahip android 6-8 arası sürümleri koşturan en az 10 markanın 50'den fazla cihaz modelinde ticari mobil cihaz adli bilişim yazılımlarının çözüm getirdikleri görülmüştür.

Android koşturan cihazların belli tarihten önceki modellerinde disk şifreleme ve veri şifreleme bulunmadığından yeterli teknik kapasiteye sahip kişiler bu cihazların hafıza çiplerini sökerek doğru ekipmanlar ile okuyarak veriye rahatça erişebilmektedirler. Tabi ki bu cihazlar ilk çıktıklarında yeni teknoloji olduklarından bu şekilde bir çözüm bulunmamaktadır. Cihazların ve elektronik elemanlarının tanınmasıyla birlikte karşı yöntemler geliştirilmektedir. Bu doğrultuda, üzerinde chip-off ve veriyi anlamlandırma işlemleri başarıyla gerçekleştirilen, aynı zamanda Türkiye'de de kullanılan, farklı denetleyicilere sahip embedded multimedia card (eMMC) hafıza birimi bulunan 5 adet test cep telefonuna chip-off işlemi uygulanmıştır

(Laboratuvar uygulamaları, 2019). Başarılı çip sökme işlemlerine ait bilgiler Çizelge 4.1'de sunulmuştur:

Çizelge 4.1 Başarılı Chip-Off Örnekleri

(Laboratuvar uygulamaları, 2019)

MARKA	MODEL	ZORLUK	OS VERSİYONU	BOYUT
GENERAL MOBILE	Discovery	ZOR	Android 5.1.1	4
GENERAL MOBILE	Android One 4G	ZOR	Android 5.1.1	16 GB
NOKIA	N8-00 (RM-596)	ZOR	Symbian^3 Series (60 5.2)	16 GB
SONY	E2333 M4 Aqua Duos	ZOR	Android 5.0.0	16 GB
VODAFONE	945	ZOR	Android 2.1	528 MB

5. SONUÇ VE ÖNERİLER

Çalışma boyunca irdelenen konular ve gerçekleştirilen uygulamalardan anlaşıldığı üzere mobil cihaz adli bilişimi alanının önemi birçok kez vurgulanmıştır. Bununla birlikte Anayasa ve diğer hukuk kurallarına uygunluk ile adaletin uygun şekilde sağlanarak kamu vicdanını rahatlatacak uygulamalara ihtiyaç duyulmaktadır. Hem hukuki boyuttaki düzeltmelerin hem de teknik boyuttaki gelişimlerin başarılması için uyulması gereken bazı adımlar mevcuttur. Bahsedilen faydaların yanında bu alanda gerektiği şekilde yürütülecek çalışmalar ve uygulanacak adımlar neticesinde ülke ekonomisinde de olumlu ve büyük katkılarda bulunulacağı aşikârdır.

Yukarıdaki bilgilerden hareketle iş bu tez çalışması neticesinde uygulanmasında fayda görülen sonuçlar aşağıda maddeler halinde sıralanmıştır:

1- Adli bilişim ve mobil cihaz adli bilişimi alanında saha tecrübesi çok fazla olan kolluk kuvvetlerinin eşliğinde adli makam yetkilileri, özel ve kamu teknik kurumları ve kuruluşları, üniversiteler, standart kuruluşları, devletin planlama birimleri ve ihtiyaç duyulabilecek diğer kurumlar bir araya gelerek devam eden maddelerdeki sonuç önerilerini gerçekleştirmek için uygun kurulları oluşturmalı, gerektiğinde örneğin sınır bağımsız olan siber suçlarla mücadele alanında gerçekleştirilecek operasyonlar için görev gücü olarak çalışmalıdır.

2- Adli bilişimle alakalı olabilecek bütün görevlilere görevlerinin bu alandaki yeri büyüklüğünde ve derinliğinde eğitim verilmelidir. Hukuki alandaki ve teknik alandaki görevliler karşılıklı birbirlerini eğiterek geliştirmelilerdir.

3- CMK 134. Maddesi, dijital verinin hassasiyeti ile Anayasa ve uluslararası hukuk normları bağlamında kişinin ilgili hakları da her zaman göz önünde bulundurulmak kaydıyla güncel ihtiyaçları işaret edecek şekilde güncellenmeli, şüpheliye verilecek kopya, işlemin uzun sürmesi gibi ibareler yeniden

değerlendirilmeli ve kelime bazında karmaşayı giderecek tabirler kullanılarak anlam güncellemeleri sağlanmalıdır.

4- CMK 134. Maddesi adli bilişim alanında genel hatları çizerken, delil zincirini kuvvetlendirecek iş akışları ve prosedürler belirlenmeli ve herkes ve her kurum için mümkün olduğunca büyük oranda standart hale getirilmelidir. Mobil cihaz adli bilişiminin önemi ve ayrıca daha çok hassasiyet gerektiren işlemleri için özellikle iş akış şemaları itinayla hazırlanmalıdır.

5- Delil zincirinin sağlamlaştırılması için adli bilişim işlemi gerçekleştirilen kurumlardaki laboratuvarlar uluslararası standartlar ve en iyi uygulamalar da gözetilerek akredite edilmeli ve kaliteleri artırılmalıdır.

6- Adli bilişim işlemi gerçekleştiren personelin eğitimli, tecrübeli ve yetkin olması gerekmektedir. Gerekli eğitimlerin alınması sağlanmalı, tecrübe açısından görevlilere uzmanlık sınıfları getirilmelidir. Örnek olarak bir personel gerekli eğitimleri aldıktan sonra 2 yıl asistan olarak çalışmalı, tek başına rapor hazırlamamalı, 2 yıl sonunda uzman sıfatını kazanarak alanında rapor yazacak yetkinliğe ulaşmalıdır. Mevcut duruma uygulanması açısından önerilebilecek model ise, bilirkişilik kanunu göz önüne alınarak 5 yıl tecrübeye sahip olanlar bilirkişilik temel eğitimini tamamlamalı, 2-5 yıl arası tecrübeye sahip olanlar teknik bir konu ile alakalı bir makale yazmalı, 2 yıldan az tecrübeye sahip olanlar ise süresini uzman personelin gözetiminde tamamlayarak makale çalışması ile birlikte uzmanlığa geçmeli şeklinde uygulanabilir. Bir görevlinin uzman sayılması için gerekirse bir kurulun denetiminden geçirilmesi de sağlanabilir.

7- Adli bilişim ile alakalı olarak delil zincirinin sağlamlaşmasını sağlayacak ve daha düzenli bir adli sürecin oluşmasında katkı sağlayacak şekilde inceleme raporlarında standartlar belirlenmelidir. İlgili herkes tarafından anlaşılabilecek ve işlemlerin en uygun halde gerçekleştirildiğini gösterecek şekilde anlaşılır ve yeterli bilgiyi içeren şablonlar oluşturulmalıdır.

8- Adli bilişim alanında kullanılan birçok yazılım ve donanım yabancı ülke kaynaklıdır. Bu açılardan ülke adli bilişim ihtiyaçları doğrultusunda ülkede üretilmiş araçlara ihtiyaç vardır. Cihazların ya da yazılımların ülke dışından getirilerek üzerine marka basılması şeklinden ziyade, projeler kapsamında çalışacak ekiplerin oluşturduğu araçlar üretilmelidir. Aksi taktirde teknik destekte dahi sorunlar çıkmaktadır. Geliştirilen yazılım ve donanımlar doğrudan adli vakalarda kullanılmadan önce alanda birçok teste tabi tutulmalı ve denenmelidir. Özellikle kolluk kuvvetlerinin yeni araçları test etmesi ve test sonuçlarını geliştiriciye bildirmeleri önemli ölçüde faydalı olacaktır. Bilinen ve alanında iyi olan bütün araçların özgeçmişleri bu şekildedir. Bununla birlikte geliştirilen araçların uluslararası geçerlilikleri açısından yurtdışındaki testlerden de geçirilmesi, gelişme aşamasında iş birliği içinde bulunulan ve destek olunan ülkelerde eğitim veren kurumlar tarafından tanıtılarak yaygınlaşmasının sağlanması önemlidir.

9- Teknik boyutta veri güvenliğinin sağlanması adına birçok yeni teknolojik gelişme kaydedilmekte ve takip edilmektedir. Bu gelişmeler suç verisine ulaşma adına engel teşkil ediyor olsalar da gerçekleştirilen çalışmalar neticesinde bir süre sonra çözüm yolları bulunabilmektedir. Kriptoloji, şifre kırma, verileri anlamlandırma ve ihtiyaç duyulan diğer alanlarda birinci maddede bahsedilen kurumlardan ilgili taraflar ortak çalışma yürütmeli ve sonuç üretmelidir.

10- Multidisipliner ve interdisipliner yapısından bahsedilen adli bilişim alanında teknik ve hukuki alanlarda çok faydalı katkılar sağlayan bir diğer unsur ise akademik çalışmalardır. Akademik çalışmalar desteklenmeli ve bu alandaki lisansüstü ve doktora imkânları artırılmalıdır.

ÖZET

Adli bilişim ve özellikle mobil cihaz adli bilişimi hem ekonomik hem de insan hakları açısından bilinçli şekilde geliştirilmesi gereken bilim alanlarıdır. Ülkemizin bu alanda söz sahibi olması için daha çok akademik çalışmaya ve bu alandaki yüksek lisans ve doktora çalışmalarının artırılmasına ihtiyaç olduğu düşünülmektedir. Bu tez çalışmasının amaçlarından biri ise alandaki adli bilişim ve özellikle mobil adli bilişim alanındaki hukuki ve teknik alandaki birçok soru ve soruna cevap ve çözüm önerisi sunmaktır.

Ayrıca hukuki süreçlerin nasıl yürütüldüğü, adli bilişim incelemecilerinin yetkinliği, adli bilişim iş akışları ve teknik yöntemlerinin akredite olma durumları, teknolojik gelişmeler ve delil zincirine riayet hususları adli bilişim yöntemlerinin kişi hak ve özgürlüklerini doğrudan etkileyecek dayanaklarıdır.

Bu tez kapsamında yukarıdaki hususlar değerlendirilirken mobil cihaz adli bilişiminde en güncel sorunlar ortaya konacaktır. Önemli bir nokta olarak, ülkemizde adli bilişim işlemlerinin dayanağı olan 5271 sayılı Ceza Muhakemesi Kanunu (CMK) isimli kanunun 134. Maddesi ve eksiklikleri de irdelenerek bir takım düzeltme önerilerinde bulunulacaktır. Gerçek vakalar ve istatistiksel veriler kullanılarak hem teknik hem de hukuki boyuttaki bu sorunlara çözüm önerileri de sunulmaya çalışılacaktır.

Anahtar Kelimeler: Adli bilişim, adli süreç, delil zinciri, mobil cihaz, mobil cihaz adli bilişimi, yeni teknik yöntemler.

SUMMARY

Digital forensics and especially mobile device digital forensics are science areas that are to be improved consciously because of their importance. To gain more arbiter position for our country, it is important to prepare more academic works and to have more master and PhD programs on digital forensics. The aim of this thesis is to reveal answers and conclusions for many questions and problems in digital forensics, especially in mobile device forensics.

On the other hand, the way of legal procedures, competency of digital forensics experts, accredited situation of workflows and technical procedures, technological advances and the chain of custody issues are the main basis of digital forensics that effect human rights and freedom directly.

In the context of this thesis, the most current problems on mobile device forensics will be explicated while the above issues will be evaluated. As a very important point, the insufficient parts of the article 134 of Law number 5271 named Ceza Muhakemesi Kanunu (CMK) (2004, 4 Aralık) that is the basis of digital forensics procedure in Turkey will be discussed and some fixing offers will be made. Solutions and solution offers in both technical and legislation aspects will be revealed for these problems using the real cases information and statistical data.

Keywords: Chain of custody, digital forensics, legal procedure, mobile device, mobile device forensics, new technical methods.

KAYNAKLAR

668 Sayılı Kanun Hükmünde Kararname (2017, 27 Temmuz). *Resmi Gazete* (Sayı: 29783 (2. Mükerrer)). Erişim adresi: http://www.resmigazete.gov.tr/eskiler/2016/07/20160727M2..htm

ABBOUD G, MAREAN J, YAMPOLSKİY RV (2010). Steganography and Visual Cryptography in Computer Forensics. *2010 Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering*. s:25-32

Accessdata (2018). Forensic Toolkit (Sürüm FTK 7.0.0.163) [Yazılım]. Tedarik edilebileceği adres: https://accessdata.com/product-download/forensic-toolkit-ftk-version-7.0.0

AKALIN U (2016). *Mobil Cihazlarda Adli Bilişim Çalışmalarına Yönelik Bir Model Önerisi* (Gazi Üniversitesi Yüksek Lisans Tezi). Yükseköğretim Kurulu Ulusal Tez Merkezi Veri Tabanından erişildi.

AKBAL E, DOĞAN Ş, BALOĞLU İ (2018). Android İşletim Sisteminde WhatsApp Uygulamasının Adli Bilişim Açısından İncelenmesi. *Bilişim Teknolojileri Dergisi*, ***11*****(2)**: 147-156.

AKBAL E, DOĞAN Ş, KAYA M (2016). Adli Bilişim Mühendisliği Müfredatı ve Gereksinimleri, *Fırat Üniversitesi Mühendislik Bilimleri Dergisi,* ***28*****(2)**: 149-158.

AKINCI SOKULLU F (2001). Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi, İnternet Özel Bölümü. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, ***59*****(1-2)**: 121-134.

Anadolu Ajansı (2018, 9 Kasım). "1 milyon 125 bin dijital materyal inceledik". Erişim adresi: https://www.mynet.com/1-milyon-125-bin-dijital-materyal-inceledik-ankara-5268165-myvideo. Erişim tarihi: 09/02/2019

Android Encryption (t.y.). Erişim adresi: https://source.android.com/security/encryption Erişim tarihi: 9/2/2019

Anonim (2018). Bilgi Teknolojileri ve İnternetin Bilinçli, Güvenli Kullanımı. *Bilgi Teknolojileri ve İletişim Kurumu İnternet Daire Başkanlığı Yayınları*, s:2-5.

Apple (2017). About Touch ID Advanced Security Technology. Erişim adresi: https://support.apple.com/en-gb/HT204587. Erişim tarihi: 18/2/2019

Apple Inc. (2019, Mayıs). iOS Security. Erişim adresi: https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf. Erişim tarihi: 9/2/2019

Appleinsider (2018). New 'IP Box' Tool Bypasses 10-Try Limit For Pins On Older IOS Versions, Automates Brute Force Attacks. Erişim adresi: https://appleinsider.com/articles/15/03/18/new-ip-box-tool-bypasses-10-try-limit-for-pins-on-older-ios-versions-automates-brute-force-attacks. Erişim tarihi: 9/2/2019

Avrupa Birliği Türkiye Delegasyonu (2016). Avrupa Komisyonunun AB-ABD Gizlilik Kalkanı Anlaşması. Erişim adresi: https://www.avrupa.info.tr/tr/eeas-news/avrupa-komisyonu-ab-abd-gizlilik-kalkanini-hayata-geciriyor-transatlantik-veri-akisi-icin. Erişim tarihi: 9/2/2019

Avrupa İnsan Hakları Mahkemesi (1950). Avrupa İnsan Hakları Sözleşmesi. Erişim adresi: https://www.echr.coe.int/Documents/Convention_TUR.pdf. Erişim tarihi: 18/2/2019

Avrupa İnsan Hakları Mahkemesi (2019). HUDOC Veri Tabanı https://www.echr.coe.int/Pages/home.aspx?p=caselaw/HUDOC/tur

Avrupa Konseyi Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (1981, 28 Ocak). Erişim adresi: https://humanrightscenter.bilgi.edu.tr/media/uploads/2016/03/29/KisiselVerilerinOtomatikIslemeTabiTutulmasiKarsisindaBireylerinKorunmasiSozlesmesi.pdf

AYDOĞAN H (2009). *Adli Bilişim'de Yeni Elektronik Delil Elde Etme Yöntemleri* (Yüksek Lisans Tezi). Yükseköğretim Kurulu Ulusal Tez Merkezi Veri Tabanından erişildi.

AYERS I, DANKER S, MISLAN R (2009). Hashing Techniques for Mobile Device Forensics", *Small Scale Digital Device Forensics Journal*, ***3*(1).**

AYERS R, BROTHERS S, JANSEN W (2014). Guidelines on Mobile Device Forensics, *NIST Special Publication Revision 1*, (800-101):27.

BAIR J (2018). Seeking The Truth From Mobile Evidence Basic Fundamentals Intermediate And Advanced Overview Of Current Mobile Forensic Investigations, 1. Baskı, Academic Press, s:81.

BARBAROS İ (2016). *Bulut Depolama Uygulamalarını Kullanan Bilgisayarların Adli Bilişim Açısından İncelenmesi* (Yüksek Lisans Tezi). Yükseköğretim Kurulu Ulusal Tez Merkezi Veri Tabanından erişildi.

BEEBE N (2009). Digital Forensic Research: The Good, The Bad And The Unaddressed. *IFIP Int. Conf. Digital Forensics*. s:30.

BİÇKİN İ (2006). Siber Suç Sözleşmesi ve 5237 s. Türk Ceza Kanununda Bilişim Suçları. *Yargıtay Dergisi*, ***32*(1-2)**: 152.

Bireysel Ders Müfredatı (2019). Mobil Cihaz İnceleme Eğitimi. Kapalı kaynak.

BREIKI H, HASHMI M, BAGGILI I (2010). Defining a Standard for Reporting Digital Evidence Items in Computer Forensic Tools. s: 78-95.

Bundeskriminalamt (2019). Technologies. Erişim adresi: https://www.bka.de/EN/OurTasks/SupportOfInvestigationAndPrevention/Technologies/technologies_node.html. Erişim tarihi: 09/02/2019

CARUSO J (2011, 9 Mayıs). Living legends: Ethernet inventor Bob Metcalfe. Erişim adresi: https://www.networkworld.com/article/2202019/lan-wan/living-legends--ethernet-inventor-bob-metcalfe.html. Erişim tarihi: 18/2/2019

Cellebrite (t.y.). Cellebrite Advanced Services. Erişim adresi: https://www.cellebrite.com/en/cas-sales-inquiry/. Erişim tarihi: 18/2/2019

CEPOL (2016). CEPOL Training Catalogue. Erişim adresi: https://www.cepol.europa.eu/sites/default/files/training-catalogue-2016.pdf Erişim tarihi: 18/02/2019

Ceza Muhakemeleri Usulü Kanunu (1929, 20 Nisan). *Resmi Gazete* (Sayı: 1172). Erişim adresi: http://www.resmigazete.gov.tr/arsiv/1172.pdf

Ceza Muhakemesi Kanunu (2004, 17 Aralık). *Resmi Gazete* (Sayı: 25673). Erişim adresi: http://www.resmigazete.gov.tr/eskiler/2004/12/20041217.htm.

COSIC J, BACA M (2010). *(Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp*. The 33rd International Convention MIPRO. s: 1226-1230

ÇAKIR H, KILIÇ MS (Ed.). (2014a). *Adli Bilişim ve Elektronik Deliller.* Seçkin Yayıncılık, 1. Baskı, Ankara.

ÇAKIR H, KILIÇ MS (Ed.). (2014b). *Güncel Tehdit: Siber Suçlar*. Seçkin Yayıncılık, 1. Baskı, Ankara.

ÇİÇEK İ, (2008). *Ülkemizde Adli Bilişim Laboratuarlarının Kurulumu Ve Bilişim Suçlarıyla Mücadeleye Katkıları (Building A Computer Crime Laboratory İn Our Coutry And İt's*

Contributions On Struggle Against Computer Crime). (Haliç Üniversitesi Yüksek Lisans Tezi). Yükseköğretim Kurulu Ulusal Tez Merkezi Veri Tabanından erişildi.

DEBROTA S, GOLDMAN J, MISLAN R, ROGERS MK, WEDGE T, (2006). "Computer Forensics Field Triage Process Model. *Journal of Digital Forensics Security and Law,* **1(2):** 26.

DIFOSE Adli Bilişim Hizmetleri (2017). Erişim adresi: https://www.difose.com.tr/cep-telefonu-sim-kartlarinin-adli-incelenmesi/. Erişim tarihi: 9/2/2019.

DOĞANAY HA (2018, Kasım). Iphone Data Security. Bilgi Teknolojileri ve İletişim Kurumu'nda Gerçekleştirilen LOCARD Global Cyber Security Summit Konferans Sunumu.

EKİZER AH (2014). Adli Bilişim. Erişim adresi: https://www.ekizer.net/adli-bilisim-computer-forensics/. Erişim Tarihi: 18/2/2019.

Electronic Privacy Information Center (2018). Apple v. FBI Concerning an Order Requiring Apple to Create Custom Software to Assist the FBI in Hacking a Seized iPhone. Erişim adresi: https://epic.org/amicus/crypto/apple/. Erişim tarihi: 09/02/2019

ERCAN T, NACAK D (2009). Kablosuz Ağlardaki Paket Trafiğine Adli Bilişim Yaklaşımı. *Yaşar Üniversitesi Dergisi*, ***4*(13)**:913-925.

ERDOĞAN Y (2012). Bilişim Sistemine Girme ve Kalma Suçu. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi,* **12**: 1363-1433.

Github (2012). Android Pattern Lock. Erişim adresi: https://github.com/sch3m4/androidpatternlock. Erişim tarihi: 09/02/2019

GORDON A (Ed.). (2015). Official (ISC)2 Guide to the CISSP CBK. 4. Baskı, CRC Press, s: 798

Guidance Software (2018, 5 ocak). Tableau TD2u Kullanım Kılavuzu. Erişim adresi: https://www.guidancesoftware.com/docs/default-source/document-library/user-guide/td2u-forensic-duplicator-user-guide.pdf?sfvrsn=1ad48bad_16, Erişim tarihi: 18/02/2019

GÜL M (2018). *Adli Bilişim Atlatma Teknikleri Ve Karşı Tedbirler (Anti Forensics Techniques And Countermeasures).* (Milli Savunma Üniversitesi Yüksek Lisans Tezi). Yükseköğretim Kurulu Ulusal Tez Merkezi Veri Tabanından erişildi.

GÜLLÜCE YZ, BENZER R (2015). Adli Bilişimde Hard Disk Arızaları ve Arızalı Disklerden Veri Kurtarma Yöntemleri. *International Journal of Human Sciences, **12*(1):** 206-225.

GÜLLÜCE YZ, BENZER R, ÇAKIR H (2016). Adli Bilişimde Silinmiş Dosyaların Kurtarılması Üzerine Karşılaştırmalı Yöntemler. *Yönetim Bilişim Sistemleri Dergisi*, ***2*****(**2): 19-28.

Güvenli Web (2018). Türkiye'nin İnternet Kullanım Alışkanlıkları - TÜİK 2018. Erişim adresi: http://www.guvenliweb.org.tr/haber-detay/turkiyenin-İnternet-kullanim-aliskanliklari-tuik-2018. Erişim tarihi: 18/02/2019

HENKOĞLU T (2011). Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi. Pusula Yayıncılık, 2. Baskı, İstanbul.

HEWLING MO (2013). *Digital Forensics: An Integrated Approach For The Investigation Of Cyber/Computer Related Crimes*. (Bedfordshire Üniversitesi Doktora Tezi). Erişim adresi: http://uobrep.openrepository.com/uobrep/bitstream/10547/326231/1/hewling.pdf.

Hürriyet Gazetesi (2017, 27 Haziran). Drone nedir? Ne işe yarar?. Erişim adresi: www.hurriyet.com.tr/teknoloji/drone-nedir-ne-ise-yarar-40502732. Erişim tarihi: 09/02/2019

Industry Analytics Research Consulting (2018). Digital Forensics Market is Anticipated to hit $6.83 billion by 2023 at a CAGR of 14.20%. Erişim adresi: http://industryarcblog.com/digital-forensics-market-analysis-forecast/. Erişim tarihi: 09/02/2019

İnternet World Stats (2018, Mayıs). İnternet Users in OECD Member Countries. Erişim adresi: https://www.İnternetworldstats.com/stats16.htm. Erişim tarihi: 09/02/2019

IRONS AD, STEPHENS P, FERGUSON RI (2009). Digital Investigation As A Distinct Discipline: A Pedagogic Perspective. *Digital Investigation*, **6(1-2)**: 82-90.

JONES A, VALLI C (2008). Building a Digital Forensic Laboratory: Establishing and Managing a Successful Facility. Syngress, 1. Baskı, ABD.

KAHİYE İ (2014). *Adli Bilişim Yazılım Ve Donanımlarının Analizi.* (Yüksek Lisans Tezi). Yükseköğretim Kurulu Ulusal Tez Merkezi Veri Tabanından erişildi.

KAMP S (2018, 30 Ocak). Digital in 2018: World's İnternet Users Pass the 4 Billion Mark. Erişim adresi: https://wearesocial.com/blog/2018/01/global-digital-report-2018 Erişim tarihi: 18/02/2019

KAYIHAN İ (2001). Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, **59(**1-2).

Kişisel Verileri Koruma Kurumu (2019). Kişisel Verilerin Korunması Alanında Uluslararası Ve Ulusal Düzenlemeler. Erişim adresi: https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararasi-ve-Ulusal-Duzenlemeler. Erişim tarihi: 18/02/2019

KOÇAK M, UZUNAY Y (2005). Bilişim Suçları Kapsamında Dijital Deliller. Erişim adresi: https://ab.org.tr/ab05/tammetin/134.pdf . Erişim tarihi: 18/02/2019

KORKMAZ Y, BOYACI A (2018). Adli Bilişim Açısından Ses İncelemeleri. *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*, **30 (1):** 329-343

Laboratuvar Uygulamaları (2019). Android İşletim Sistemi Yüklü Olan 5 Adet Cihazın Hafıza Çiplerine Chip Off İşlemi Uygulanması ve Apple Cihazlar İçin Sahte Parmak Oluşturma İzi Çalışması.

Living İnternet (1995). Merit's History. Erişim adresi: https://www.livingİnternet.com/doc/merit.edu/phenom.html. Erişim tarihi: 18/02/2019

Mali Suçlar Araştırma Kurulu (2018). Kişisel Verilerin Korunması Hakkında Rehber. Erişim adresi: http://www.masak.gov.tr/userfiles/file/kisisel_verilerin_korunmasi_ve_paylsim_rehberi.pdf. Erişim tarihi: 18/02/2019

Malzeme Bilimi (2016). GPS Nedir? GPS Nerelerde Kullanılır? GPS'in Çalışma Şekli Nasıldır?. Erişim adresi: https://malzemebilimi.net/gps-nedir-nasil-calisir.html. Erişim tarihi: 18/02/2019

MARTURANA F (2014). *Device Classification in Digital Forensics Triage*. (University of Tor Vergata Doktora Tezi). Erişim adresi: https://www.researchgate.net/publication/263619846_DEVICE_CLASSIFICATION_IN_DIGITAL_FORENSICS_TRIAGE. Erişim tarihi: 18/02/2019

MORGAN S (2016). U.S. Government's Multi-Million Dollar Mobile Forensics Shopping Spree Revealed. Erişim adresi: https://www.forbes.com/sites/stevemorgan/2016/04/06/u-s-governments-multi-million-dollar-mobile-forensics-shopping-spree-revealed/#52b94d11b0df. Erişim tarihi: 18/02/2019

OĞUZ R (2018). *Adli Bilişimde İnceleme Süreçleri Investigation Processes At Digital Forensics.(* Ankara Üniversitesi, Yüksek Lisans Tezi). Yükseköğretim Kurulu Ulusal Tez Merkezi Veri Tabanından erişildi.

Olağanüstü Hal Kapsamında Alınması Gereken Tedbirler İle Bazı Kurum Ve Kuruluşlara Dair Düzenleme Yapılması Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabul Edilmesine

Dair Kanun (2016, 24 Kasım). *Resmi Gazete* (Sayı: 29898). Erişim adresi: http://www.resmigazete.gov.tr/eskiler/2016/11/20161124-2..htm.

Organisation for Economic Co-operation and Development (2002). Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri. Erişim adresi: https://www.oecd.org/sti/ieconomy/32493366.PDF. Erişim tarihi: 18/9/2019

Orta Doğu Teknik Üniversitesi Bilgi İşlem Daire Başkanlığı (2005). Erişim adresi: http://www.İnternetarsivi.metu.edu.tr/tarihce.php. Erişim tarihi: 18/02/2019

ÖNOK M (2013). Avrupa Konseyi Siber Suç sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi,* **19(**2): 1229-1270.

ÖZBEK M (2013*). Adli Bilişimde Delillerin Toplanması Ve İncelenmesi Evidence Collection And Analysis In Computer Forensics*. (İstanbul Bilgi Üniversitesi, Yüksek Lisans Tezi). Yükseköğretim Kurulu Ulusal Tez Merkezi Veri Tabanından erişildi.

ÖZEN M, ÖZAOCAK G (2015). Adli Bilişim Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi CMK M 134. *Ankara Barosu Dergisi*, **2015/1**: 43-77

ÖZGİT A, ÇAĞILTAY K (2018). *Türkiye'de İnternet: Dünü, Bugünü.* Ankara: ODTÜ

PAGANINI P (2016, 17 Eylül). A Researcher Has Demonstrated That The NAND Mirroring Technique Was Able To Bypass The Passcode Retry Limitations On The San Bernardino Shooter's Iphone. Erişim adresi: https://securityaffairs.co/wordpress/51342/hacking/nand-mirroring.html Erişim tarihi: 18/02/2019

PAGLIERI J (2016). Cellebrite is The FBI's Go-to Phone Hacker. *CNN Business.* Erişim adresi: https://money.cnn.com/2016/03/31/technology/cellebrite-fbi-phone/. Erişim tarihi: 09/02/2019

PİWARİ MTM (2016). *Digital Forensics in the Cloud The Realiability and Integrity of the Evidence Gathering Process.* (Auckland Üniversitesi Mühendislik, Bilgisayar ve Matematik Bilimleri Yüksek Lisans Tezi). Erişim adresi: https://core.ac.uk/download/pdf/56365730.pdf

Polis Vazife Ve Salahiyet Kanunu (1934, 14 Temmuz). *Resmi Gazete* (Sayı: 2751). Erişim adresi: http://www.resmigazete.gov.tr/arsiv/2751.pdf

Programme For The Endorsement Of Forest Certification (2013). Erişim adresi: https://consultations.pefc.org/consult.ti/PEFCsChainOfCustody/viewCompoundDoc?docid=7826164&partId=7826324&sessionid=&voteid= Erişim tarihi: 09/02/2019.

Programme For The Endorsement Of Forest Certification (t.y.). Supply Chain Companies https://www.pefc.org/standards/chain-of-custody Erişim tarihi: 18/02/2019

RAYMOND L (2016). A Multidisciplinary Digital Forensic Investigation Process Model. *Business Horizons,* **59**(6): 593-604.

Sabah Gazetesi (2016, 31 Mayıs). Akıllı Saat Nedir?. Erişim adresi: https://www.sabah.com.tr/teknoloji/2016/05/31/akilli-saat-nedir Erişim tarihi: 18/02/2019

SALİH C (2018). 2018 Türkiye İnternet Kullanım ve Sosyal Medya İstatistikleri. Erişim adresi: https://dijilopedi.com/2018-turkiye-İnternet-kullanim-ve-sosyal-medya-istatistikleri/. Erişim tarihi: 09/02/2019

SÜZEN AA (2018). *Adli Bilişim İçin Ram İmajı Alınarak Elektronik Delil Elde Etme" (Obtaining Digital Evidence By Acquiring Ram İmage For Computer Forensics).* (Süleyman Demirel Üniversitesi, Doktora Tezi). Yükseköğretim Kurulu Ulusal Tez Merkezi Veri Tabanından erişildi.

ŞAHİN C (2001). Ceza Muhakemesinde İspat (Delillerin Doğrudan Doğruyalığı İlkesi). Yetkin Yayınları, 2001 Baskı, Ankara.

ŞİRİKÇİ AS, CANTÜRK N (2012). Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi. *Bilişim Teknolojileri Dergisi*, **5(3)**: 29-34.

T24 Bağımsız İnternet Gazetesi (2018, 16 Kasım). Soylu, İncelenen Dijital Materyal Sayısını Açıkladı: 2018'de, Ortalama 45 Binden, 631 Bin 233'e Yükseldi. Erişim adresi: http://t24.com.tr/haber/soylu-incelenen-dijital-materyal-sayisini-acikladi-2018de-ortalama-45-binden-631-bin-233e-yukseldi,749982 Erişim tarihi: 09/02/2019

TAN A (2009). Adli Bilişim (Computer Forensic). Erişim adresi: https://hukuksokagi.com/kaynak/adli-bilisim-computer-forensic/. Erişim tarihi: 09/02/2019

TEEL Technologies (t.y.). Eclipse 3 Pro Kit. Erişim adresi: http://www.teeltech.com/mobile-device-forensic-tools/eclipse-3-pro-kit/ Erişim tarihi: 09/02/2019

Teknonce (2018, 17 Mart). Cep Telefonunun Tarihsel Gelişimi. Erişim adresi: https://www.teknonce.com/cep-telefonunun-tarihsel-gelisimi.html Erişim tarihi: 18/02/2019

Terörle Mücadele Kanunu Ve Ceza Muhakemesi Kanunu İle Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun (2014, 6 Mart). *Resmi Gazete* (Sayı: 28933). Erişim adresi: http://www.resmigazete.gov.tr/eskiler/2014/03/20140306M1-1.htm

TOROSLU N, FEYZİOĞLU M (2018). Ceza Muhakemesi Hukuku. Savaş Kitap ve Yayınevi, 18. Baskı, Ankara.

TÜRKAK (2017). EGM Akreditasyon Sertifikası Eki. Erişim adresi: http://www.turkak.org.tr/pdf/AB0260T1549.pdf?r=88fa69bd523347b68c9ac33bdf666aaa. Erişim tarihi: 18/02/2019

TÜRKAK (2018). JKDB Akreditasyon Sertifikası Eki. Erişim adresi: http://www.turkak.org.tr/pdf/AB0165T1304.pdf?r=40b71c802c0544d6aa6d2af1e1e96dff. Erişim tarihi: 09/02/2019

Türkiye Büyük Millet Meclisi (2012). Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu. Erişim adresi: https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf Erişim tarihi: 09/02/2019

Türkiye İstatistik Kurumu (2018, 8 Ağustos). Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması, 2018. Erişim adresi: http://www.tuik.gov.tr/PreHaberBultenleri.do?id=27819 Erişim tarihi: 18/02/2019

UKŞAL M (2015). *Mobil Cihazlarda Adli Bilişim.* (İstanbul Bilgi Üniversitesi Yüksek Lisans Tezi). Yükseköğretim Kurulu Ulusal Tez Merkezi Veri Tabanından erişildi.

ÜNSAL Z (2013). Google'ın Yeni Gizlilik Politikası Google Inc. Tarafından 1 Mart 2012 Tarihinde Yayımlanan Politikasının Kişisel Verilerin Korunması İlkeleri İle Uyumluluğu Ve Avrupa Birliği'nin 95/46/Ec Sayılı Veri Koruma Direktifi Açısından Değerlendirilmesi. *Hacettepe Hukuk Fak. Dergisi,* **3 (1)**: 99–124.

VAUGHTERS A (2018, 1 Ekim). Illegal Card Skimmers Now Using Bluetooth To Steal. Erişim adresi: https://www.wivb.com/news/local-news/illegal-card-skimmers-now-using-bluetooth-to-steal/1491121517. Erişim tarihi: 18/02/2019

Wmaracı (t.y.). PDA Nedir?. Erişim adsresi: https://wmaraci.com/nedir/pda Erişim tarihi: 09/02/2019

YILMAZ EN, GÖNEN S, ULUS Hİ (2016). Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme. *Bilişim Teknolojileri Dergisi*, **9(3)**: 229-236.

ÖZGEÇMİŞ

I- Bireysel Bilgiler

Ad ve Soyad : Hamza Aytaç DOĞANAY

Doğum yeri/tarihi : İstanbul / 09/02/1982

Uyruk : Türkiye Cumhuriyeti

Medeni Hali: : Bekar

İletişim Adresi : EGM Siber Suçlarla Mücadele Daire Başkanlığı İncek / ANKARA

E-posta ve iletişim : aytachamzadoganay@gmail.com, Twitter: @4n6_tur

II- Eğitimi

2016 – 2019 Ankara Üniversitesi Sağlık Bilimleri Enstitüsü Disiplinlerarası Adli Bilimler Anabilim Dalı Adli Bilişim Yüksek Lisans Tezi

2000 – 2004 Polis Akademisi, Ankara

- Mezuniyet Notu: 85,96
- Polis Amir Eğitimi (Anayasa, Ceza Hukuku, CMK, Uakın Savunma ve Beden Eğitimi, Ateşli Silahlar ve Atış, Soruşturma Teknikleri, Olay Yeri İnceleme, İstihbarat, Uluslararası İlişkiler, Tarih)

1997 – 2000 Polis Koleji, Ankara

- 3.lük derecesi ile mezun olunmuştur.

Yabancı dili :

İngilizce (YÖKDİL: 87,5)

III- Ünvanları

2014 – Adli Bilişim Uzmanı

2019 – Adli Bilişim Bilirkişi

IV- Mesleki Deneyimi

2014 – (Halen) EGM Siber Suçlarla Mücadele Daire Başkanlığı, Adli Bilişim Şube Müdürlüğü

V- Üyelikler

The European Union Agency for Law Enforcement Training (CEPOL)

VI- Bilimsel İlgi Alanları

Dijital veri kurtarma, mobil cihazlar, bilgisayar bilimi, adli bilişim.

VII- Bilimsel Etkinlikleri

Seminer:

Veri Kurtarma - Ankara Üniversitesi Sağlık Bilimleri Enstitüsü Disiplinlerarası Adli Bilimler Anabilim Dalı Adli Bilişim Yüksek Lisans Semineri

VIII- Diğer Bilgiler

Kurs:

01/2017 – 02/2017 Advanced BGA Chip-Off and JTAG Mobile Forensics, Teel Technologies, Ankara

08/2015 – 09/2015 PC3000 HDD ve FLASH (Fiziksel Veri Kurtarma) ACELAB – Rusya

01/2015 – 01/2015 CCLO ve CCPA (Cellebrite Certified Logical Operator and Cellebrite Certified Physical Analyst), Ankara

03/2009 - 12/2009 Atlı Polis Eğiticilerin Eğitimi, Hollanda Polis Teşkilatı Antalya, Türkiye – Amsterdam, Hollanda

09/2007 - 03/2009 Microsoft Certified Professional (MCP) Certificate

09/2005 - 03/2006 Configuring and Managing of Windows Server 2003, Windows Server 2008, ISA Server 2006(Firewall), Windows XP and Vista OS. Bilge Adam IT Academy, Ankara, Türkiye

Sunumlar:

- Analyze of an Infostealer - Fake Android Mobile APP of a Bank, ISCR (International Symposium On Cybercrime Response), Güney Kore, Mayıs 2019
- Siber Suçlarla Mücadele Daire Başkanlığı Görevleri, MGK Genel Sekreterliği, Mayıs 2019
- Siber Terörle Mücadelede Karşılaşılan Zorluklar, e-Safe Ulusal Güvenlik Etkinlikleri, Bilgi Teknolojileri ve İletişim Kurumu, Mart 2019
- Siber Güvenlik Hukuku ve Adli Bilişim, Türkiye Bilişim Derneği 2. Siber Güvenlik Zirvesi, Bilgi Teknolojileri ve İletişim Kurumu, Şubat 2019
- Iphone Data Security, LOCARD Global Cyber Security Summit, Bilgi Teknolojileri ve İletişim Kurumu, Kasım 2018
- Criminal Justice Statistics on Cyber Crime and Electronic Evidence, Romanya COE, Mayıs 2018
- Hipervisor Teknolojisine Adli Bakış, LOCARD Global Cyber Security Summit, Bilgi Teknolojileri ve İletişim Kurumu, Mayıs 2017
- Veri Kurtarma, LOCARD Global Cyber Security Summit @ İstanbul, Mayıs 2016
- Digital Forensics Capacity of Turkish National Police, CEPOL Polonya, Mart 2016

Diğer Özellikler:

- Türkiye Binicilik Federasyonu Antrenörlük
- Gitar ve bağlama
- Karate
  - 1999 Liselerarası Türkiye Şampiyonluğu
  - 2004 Polis Balkan Şampiyonası Birincilik