TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

ADLİ BİLİŞİMDE İNCELEME SÜREÇLERİ

Ramazan OĞUZ

DİSİPLİNLERARASI ADLİ BİLİMLER ANABİLİM DALI
YÜKSEK LİSANS TEZİ

DANIŞMAN
Doç.Dr. Recep ERYİĞİT

ANKARA
2018

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

ADLİ BİLİŞİMDE İNCELEME SÜREÇLERİ

Ramazan OĞUZ

DİSİPLİNLERARASI ADLİ BİLİMLER ANABİLİM DALI
YÜKSEK LİSANS TEZİ

DANIŞMAN
Doç.Dr. Recep ERYİĞİT

ANKARA
2018

Etik Beyan

Ankara Üniversitesi
Sağlık Bilimleri Enstitüsü Müdürlüğü'ne,

Yüksek Lisans tezi olarak hazırlayıp sunduğum **"ADLİ BİLİŞİMDE İNCELEME SÜREÇLERİ"** başlıklı tez; bilimsel ahlak ve değerlere uygun olarak tarafımdan yazılmıştır. Tezimin fikir/hipotezi tümüyle tez danışmanım ve bana aittir. Tezde yer alan deneysel çalışma/araştırma tarafımdan yapılmış olup, tüm cümleler yorumlar bana aittir.
Yukarıda belirtilen hususların doğruluğunu beyan ederim.

Öğrencinin Adı Soyadı: Ramazan OĞUZ
Tarih:12.04.2018
İmza:

Ankara Üniversitesi Sağlık Bilimleri Enstitüsü
Disiplinlerarası Adli Tıp Anabilim Dalı, Fiziki İncelemeler ve Kriminalistik
Yüksek Lisans Programında **Ramazan OĞUZ** tarafından hazırlanan
"ADLİ BİLİŞİMDE İNCELEME SÜREÇLERİ" adlı tez çalışması aşağıdaki jüri tarafından **Yüksek Lisans Tezi** olarak OY BİRLİĞİ ile KABUL edilmiştir.

Tez Savunma Tarihi: 12 / 04 / 2018

Prof. Dr. Nergis CANTÜRK
Ankara Ü. Adli Bilimler Enstitüsü
Jüri Başkanı

Doç.Dr. Recep ERYİĞİT
Ankara Ü. Mühendislik Fakültesi
Üye

Dr.Öğrt.Üyesi Cahit DOĞAN
Hacettepe Ü. Fen 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

ÖNSÖZ

Meslek hayatımın son 13 yılında olay yeri delillerin/bulgularının toplanmasından, laboratuvar ortamındaki incelemelerine kadar sürecin tüm aşamalarında çalışmış biri olarak, yaptığım çalışmanın adli bilişim incelemelerine küçükte olsa bir katkı sağlamasını temenni ederek ve bu bilim alanı içerisinde yapılan çalışmalara bir tuğla da benden olsun düşüncesiyle, tez çalışmalarım boyunca bana destek olan Danışmanın **Doç.Dr. Recep ERYİĞİT**'e ve tabiki her zaman ve her konuda desteklerini esirgemeyen canım **AİLEME**;

Teşekkür ederim.

SİMGELER VE KISALTMALAR

CD	Compact Disc
CMK	Ceza Muhakemesi Kanunu
DNA	Deoksiribo Nükleik asit
DVD	Digital Versatile Disc
DVR	Dijital Kayıt Cihazı
EXIF	Exchangeable Image File Format (Değiştirilebilir Resim Formatı)
FBI	Federal Soruşturma Bürosu
GB	Gigabyte (Sayısal Veri Kapasite Ölçü Birimi)
GMT	Greenwich Mean Time (Başlangıç Meridyeni Üzerinde Ortalama Güneş Zamanı)
GPRS	General Packet Radio Service
GPS	Global Positioning System
HEX	Hexedecimal (16 lık sayı sistemi)
IMEI	International Mobile Equipment Identity (Uluslararası Mobil Cihaz Kodu)
IOS	iPhone/iPad Operating System
IP	Internet Protocol
MB	Megabayt (Sayısal Veri Kapasite Ölçü Birimi)
MD5	Message-Digest Algorithm 5 (Şifreleme algoritması)
PDA	Personal Digital Assistant (Avuç İçi Bilgisayar)
PIN	Personal Identity Number (Kişisel Kimlik Numarası)
POS	Point Of Sales Terminal (Satış Noktaları Terminali')
SD	Secure Digital
SHA1	Secure Hash Algorithm 1 (Şifreleme algoritması)

SIM	Subscriber Identity Module (Abone Kimlik Modülü)
SMS	Short Message Service (Kısa Mesaj Servisi)
SSD	Solid State disk
TB	Terabyte (Sayısal Veri Kapasite Ölçü Birimi)
USB	Universal Serial Bus (Evrensel Veri Yolu)
VPN	Virtual Private Network (Sanal Özel Ağ)

ŞEKİLLER

ÇİZELGELER

1. GİRİŞ

Adli bilişim denince akla bir suçta kullanılan bilişimle ilgili bulgularının incelenmesi gelebilir. Bu doğru bir yaklaşımdır, fakat teknolojinin gelişmesi ile birlikte hayatımızın her anında bilişim sistemlerini kullanmaktayız, bu adli bilişimin alanını çok geniş bir alana yaymaktadır**.**

Adli bilişim incelemelerinin başlangıç döneminde incelenecek dijital delillerin çeşitliliğinin azlığı, kapasitelerinin küçüklüğü ve içerisindeki barındırdığı sınırlı veri türü bakımından bir inceleme ve tespit kolaylığı sağlamakta idi.

Öte yandan teknolojinin her geçen gün daha da hızlı bir şekilde hayatımıza girmesi ile birlikte hayatımızı kolaylaştırmasının yanında, adli bilişim alanında yapılan incelemeleri zorlu bir hale getirmiştir. Akıllı telefonlar henüz hayatımıza girmediği dönemlerde bir cep telefonunun barındırabildiği bilgi rehber bilgisi, arama kayıtları ve SMS mesajları iken günümüzde marka ve modeline göre farklılık göstermekle birlikte akıllı bir telefona yüklenebilecek binlerce program bulunabilmekte, çektiği bir fotoğraf üzerine fotoğrafın çekildiği bölgenin koordinat bilgilerini kaydedebilmekte, modem olarak başka cep telefonları ve bilgisayarlara internet hizmeti sağlayabilmekte, çeşitli veri aktarım yolları ile her türlü dosya paylaşımı yapabilmekte, internet geçmişi, sohbet ve elektronik posta kayıtlarını ve burada bahsetmediğimiz birçok veriyi barındırabilmektedir. Bununla birlikte cep telefonları üzerinde tuttuğu bilginin kapasitesi ve çeşitliliği arttığı sürece bilginin tespitini de zorlaştırmaktadır.

Cep telefonlarının güvenliğini ve daha optimize kullanımını sağlamak amacıyla piyasada ücretsiz birçok uygulama mevcuttur. Uygulamalar virüs taraması yapmak suretiyle cep telefonu içerisindeki zararlı yazılımları tespit etmekte, cep telefonundan kaldırılmış uygulamaların kalıntılarını silmek suretiyle gereksiz kapasite işgalinin önüne geçmektedir. Tabiidir ki bu uygulamalar kullanıcı açısından faydalı görülmektedir, buna rağmen adli bilişim açısından delil olabilecek veri kalıntıları da sildiği için inceleme yapan bilirkişinin işini zora sokmaktadır.

Akıllı cep telefonları (android, iOS vb işletim sistemlerine sahip) üzerine binlerce uygulama kurulabildiğinden bahsettik, örnek olarak Scope uygulaması ile ilgili olarak uygulamanın cep telefonu üzerinde kurulu olup olmadığı, kullanıcının takip ettiği kişiler, cep telefonu üzerinden yapılan canlı yayınlar, canlı yayınların yapıldığı konum bilgileri gibi birçok bilgi adli makamlar tarafından talep edilebilmektedir.

Gününüzde artık en önemli konu güvenlik olmuştur. Şirketler sunduğu hizmetlerin ve satmış olduğu elektronik cihazların güvenlikli olduğundan bahisle bolca reklam yapmaktadır. Abc firması piyasaya sürdüğü cep telefonunun şifresinin kırılmadığı güvencesi ile satışlarını gerçekleştirmektedir. Kullanıcı açısından talep edilen bir özellik olmakla birlikte adli bilişim incelemeleri açısından büyük engeller oluşturmaktadır.

Bilgisayar incelemeleri açısından da durum farklı değildir. Bir bilgisayar içerisinden talep edilebilecek veriler sınırlı iken teknolojinin gelişimi ile birlikte artık talepler de değişmektedir. Örneğin müşteki internet üzerinden oynadığı xxx oyunundaki savaşçı karakterin çalındığını bahisle şikayette bulunabilmektedir.

Bilgisayar veya cep telefonları üzerinden suç işleyecek kişiler, gizleyici tedbirler almak suretiyle kendilerini garanti altına almaya çalışmaktadırlar (Kendilerine ait olmayan modemler üzerinden internete çıkış yapmakta, IP değiştirmeye imkan sağlayan VPN kullanımı veya güvenli silme programlarının kullanımı gibi). Bu durum inceleme yapan uzmanların işini hayli zorlaştırmaktadır.

Gelişen teknoloji ile birlikte veri çeşitliliğinin artmasının yanı sıra verinin depolanması anlamında bellek kapasitelerinde de büyük bir genişleme bulunmaktadır. Önceleri ortalama bir bilgisayar diski 40-80 GB iken şimdi 2 - 4 TB olabilmektedir. Bir CD 700 MB iken bir Blu-ray disk 50 GB kapasitesinde olabilmektedir. Bir USB bellek 1 GB iken şimdi ise 1 TB kapasitesinde olabilmektedir. Örneklerden de anlaşılacağı üzere gelecekte veri depolama kapasitelerin daha da hızlı bir şekilde artacağı değerlendirilmektedir.

Veri depolama alanlarına ihtiyacın artması ile birlikte ticari firmalar kullanıcıya ücretsiz veya ücretli olarak bulut depolama alanları tahsis etmekte, kullanıcılar verilerini bilgisayar veya cep telefonu haricinde bulut depolama alanlarında saklayabilmektedir. Bu noktada eğer şüpheli suç konusu verilerini bulut depolama alanlarında saklıyorsa, bilgisayarında veya cep telefonunda yapılan incelemede istenilen verilere ulaşılamayabilinir.

Araba üretim teknolojilerinde meydana gelen büyük ilerlemeler neticesinde; artık arabalarında uçaklar gibi kara kutuları bulunacak ve bir araç kazasında, aracın kaç km hızla gittiği, hangi viteste olduğu, sürücünün kaç saattir araba kullandığı, kaza esnasında frene basıp basmadığı, kazanın araç arızasından mı, yoksa sürücüden mi kaynaklandığı, araç içerisinde bulunan kamera görüntülerinin incelenmesi vs birçok sorunun cevabını (“Car Forensic” olarak tabir edilen bir alt adli bilişim dalı), bu kara kutu diye tabir ettiğimiz dijital kayıtların incelenmesi sonucunda olayların aydınlatılmasında katkı sağlayacağını değerlendirmekteyiz.

Öte yandan teknolojinin gelişmesine uygun olarak adli bilişim uzmanlarının ve adli bilişim yazılımlarının kendilerini bu hızda geliştirmeleri ve teknolojinin gerisinde kalmaması gerekmektedir.

1.1. Bilişim Nedir?

Türk Dil Kurumu Güncel Türkçe Sözlük'te "Bilişim" "İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik." olarak tanımlanmıştır.

"Bilişim aşağıda belirtilen alanları içeren bilim ve teknoloji olarak tanımlanmaktadır. Bilginin ve iletişimin yapısı ve özellikleri; bilginin aktarılması, organize edilmesi, saklanması, tekrar elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemler ve öte yandan da; bilgiyi kaynağından alıp kullanıcıya aktaran ve genel sistem bilimi, sibernetik, otomasyon ile insanın çalışma çevrelerindeki yerinde ve zamanında kullanılan teknolojileri temel alan bilgi sistemleri, şebekeleri, işlevleri, süreçleri ve etkinlikleridir" (Aydın, 1992: s.:3).

Bu tanımlardan görüldüğü üzere bilişim, bilginin elektronik cihaz ve sistemler ile işlenmesi, iletilmesi ve saklanması olarak ifade edilebilir.

1.2. Adli Bilişim Nedir?

Bu alan, teknolojinin gelişmesi ile birlikte daha çok insan yaşamında yer almaya başlamış ve hatta hayatımızın her alanının vazgeçilmez bir parçası olmuştur. İnsanoğlu teknolojinin faydalı taraflarını kullandığı gibi bilinçli veya bilinçsiz olarak kötü emellerine alet etmek suretiyle adli bilişim alanının doğmasına sebep olmuştur.

Adli Bilişim sanılacağının aksine adli ve bilişim kelimelerin bir araya getirilmesi ile oluşturulmuş bir kavram degildir. Dilimize "computer forensics" (Türkçe karşılığı ile "bilgisayar adli bilimi") tanımından çevrilmis olan adli bilişim kavramı, "bilgisayar adli bilimi" olarak kullanılmak yerine kapsamının genişliği ve neredeyse teknolojik her şeye karşılık gelen sihirli kelime bilişimin baz alınması dolayısıyla "adli bilişim" olarak kullanılmıştır (Aydoğan, 2009 s.:7).

Adli Bilişim üzerine şimdiye kadar yapılmış olan çeşitli tanımlarına bakacak olursak;

Türk Dil Kurumu Bilim ve Sanat Terimleri Ana Sözlüğü'nde adli bilişimi "Sayısal verileri elde etme, muhafaza etme ve çözümleme işlemlerinin delilin gereklerine uygun olarak mahkemeye sunulması aşamasına kadar uygulanmasıdır." şeklinde tanımlamıştır.

Potaczala bir sistem yöneticisinin, sistemine giren davetsiz bir misafirin, ne zaman ve nasıl girdiğini araştırmasını ilk adli bilişim çalısmasına örnek olarak vermektedir (Potaczala, 2001: s.:3).

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

Delilin değiştirilmeden ve orijinalinin bozulmadan elde edilmesi, elde edilen verilerin degişime uğratılmadan analiz edilmesi adli bilişimin temelini oluşturmaktadır (Kruise ve Heiser, 2002 s.:3).

Adli Bilişim, adli bilimler gibi geniş bir çalışma sahasını kapsamaktadır ve sahanın genişleme ivmesi bilişim teknolojisinin modern yaşamı etkilemesiyle doğru orantılıdır. Basitçe adli bilişim disketlerden, sabit disklerden ve çıkarılabilir disklerden veri kurtarmaktır (Schweitzer, 2003).

Adli Bilişim "potansiyel yasal delillerin elde edilmesi amacıyla bilgisayar inceleme ve analiz teknikleri kullanılarak yapılan bir uygulama" şeklinde tanımlanabilir (Berber, 2004 s.:39).

"Adli Bilişim, bilgisayar biliminin yasal sürece katkıda bulunmak üzere uygulanması bilimi ve sanatıdır" (Brown, 2006: s3).

"Adli Bilişim en basit tanımıyla, bir yargılama esnasında kullanılabilecek potansiyel delillerin belirlenmesi için bilgisayar araştırma ve analiz tekniklerinin kullanılmasıdır. Bilgisayardaki verilerin korunması, tanımlanması, 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" (Bthukuku'dan aktaran Aydoğan, 2009 s.:7).

"Adli Bilişim (Computer Forensics – Bilgisayar Kriminalistigi) bilimi; suçun aydınlatılabilmesi için bilimsel metotlar kullanılarak, çesitli 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 Bilişimi; elektromanyetik-elektrooptik ortam(lar)da muhafaza edilen ve/veya bu ortamlarca iletilen; ses, görüntü, veri/bilgi veya bunların birleşiminden oluşan her türlü bilişim nesnesinin, mahkemede sayısal (elektronik-dijital) delil niteliği taşıyacak şekilde: Tanımlanması, Elde edilmesi, Saklanması, İncelenmesi ve Mahkemeye sunulması çalışmaları bütünüdür, şeklinde tanımlamıştır (Koltuksuz, 2010).

Adli Bilişim, bilişim sistemleri ve üzerinde bulunan depolama ünitelerinin, herhangi bir suçu işlemede veya yasaklanmış bir faaliyette kullanılıp kullanılmadığını tespit etmek amacıyla yapılan çalışmaların tümüdür (Henkoğlu, 2014:s.:1).

Yukarıda yapılan tanımları incelediğimizde ortak noktanın elektronik delilleri elde etme, inceleme süreci ve mahkemeye sunulması aşamalarının bir bütünü olarak değerlendirilebilir.

1.3. Delil Nedir?

Türk Dil Kurumu Güncel Türkçe Sözlük'te Delil, "insanı aradığı gerçeğe ulaştırabilecek iz, emare" şeklinde ifade edilmiştir.

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

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

Hukuk açısından ise delil, uyuşmazlık konusu olayın gerçekleşip gerçekleşmediği konusunda mahkeme heyetinde bir kanı oluşturmaya yarayan ispat aracıdır (Bayraktar, 2011 s.:9).

1.4. Elektronik (Sayısal- Dijital) Delil Nedir?

Türk Dil Kurumu Bilim ve Sanat Terimleri Ana Sözlüğü'nde sayısal delili "Elektronik veya manyetik medya üzerinde sayısal olarak saklanan veya iletilen ve olayla ilintili değeri olan veri" olarak tanımlanmıştır.

Elektronik delil konusunun doğup geliştiği Amerika Birleşik Devletlerinde uygulama ve doktrinde elektronik kayıt (electronic records), elektronik veriler (elecrtonic data), elektronik bilgi (electronic information), elektronik belge (electronic document) gibi kavramların bazen birbirleri yerine bazen de farklı anlamlarda kullanıldığı görülmektedir. Bu sebeple 2006 yılında ABD Federal Hukuk Uaulü Kanunu'nda (FRCP) yapılan bir değişiklik ile bu yönde bir bütünlük sağlanması amacı da güdülerek, daha kapsayıcı bir kavram olan " Elektronik Yolla Saklanmış Bilgi" (Electronically Stored Information) ifadesi getirilmiştir (Bragdon'dan aktaran Göksu, 2010 s:17).

Ülkemizde yapılan araştırmalarda, kullanlan terminolojilere bakıldığında elektronik delil, sayısal delil ve dijital delil tanımlamalarını görmekteyiz. Tanımlamaların tamamı aynı kapsamda olduğu değerlendirilmekle birlikte elektronik delil kavramı kullanılmıştır.

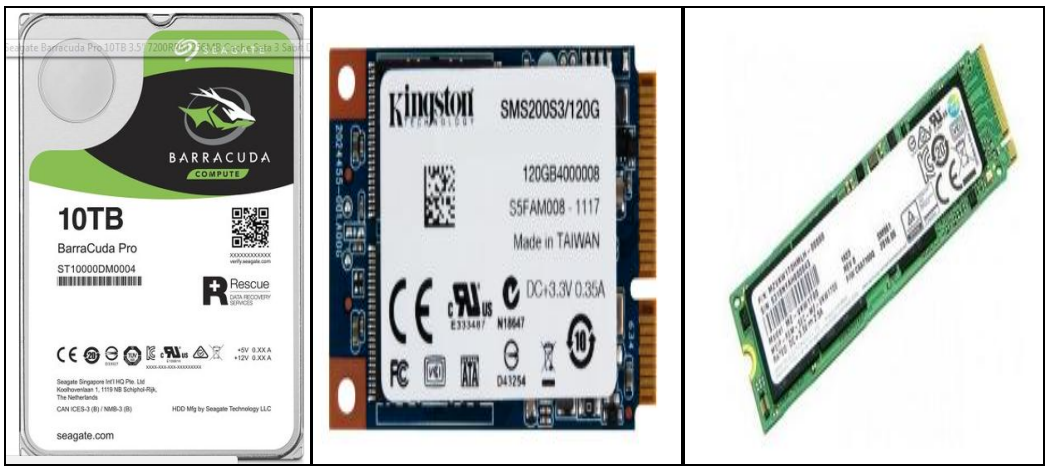
Bilişim sistemlerinin veya bilgileri otomatik olarak işleme tabi tutma ve depolama özelliğine sahip elektronik cihazların içerisinde bulunan, suç ile ilgili delil niteliği taşıyabilecek ve suçun aydınlatılmasını sağlayacak verilerdir (National institute of Justice, 2001).

Dijital deliller, adli bilişimle ilgili bir çalışma esnasında, bilişim sistemleri (bilgisayarlar, mobil telefon, dijital fotoğraf makineleri, dijital videolar, dijital faks makineleri vb.) ve bu kapsamdaki depolama aygıtları üzerinden elde edilen adli delillerdir. Bilişim suçlarını işleyen kişilere verilecek cezalar, elde edilen dijital delillerin gücü oranında mümkün olabilmektedir (Henkoğlu,. 2014 s.:5).

Elektronik delil, bir elektronik araç üzerinde saklanan veya bu araçlar aracılığıyla iletilen soruşturma açısından değeri olan bilgi ve verilerdir. Elektronik deliller az önce bahsettiğimiz gibi; parmak izi veya DNA delili gibi çoğu kez gizli, görünmeyen bir yapıya sahiptir. Sınırları kolayca ve hızlı bir şekilde geçebilir. Hassastır ve kolayca değiştirilebilir, tahrip edilebilir veya yok edilebilir (Berber, 2004 s.:46).

Yukarıda yapılan tanımlardan da anlaşıldığı üzere elektronik veri kaydı yapabilen medyalar içerisinde bulunan ve suç ile ilgili delil niteliği taşıyabilecek ve suçun aydınlatılmasına katkı sağlayacak bilgilere elektronik delil denilebilir.

1.5. Elektronik Delil Türleri Nelerdir?



Şekil 1.1. Sabit Disk - SSD

Şekil 1.2. Taşınabilir Disk- USB bellek

Şekil 1.3. Hafıza Kartları (SD, MicroSD, MMS vb.) - Disket

Şekil 1.4. CD/DVD/BD

Şekil 1.5. MP3/MP4/MP5 Çalarlar

Şekil 1.6. Ses Kayıt Cihazları

Şekil 1.7. Veri Yedekleme Birimleri (ZIP,DAT,DLT gibi kaset ve kartuşlar)

Şekil 1.8. El Bilgisayarları (PDA, PALM, Pocket PC vb.) - Dijital Kol Saatleri

Şekil 1.9. Dijital Kameralar- Dijital Fotoğraf Makineleri

Şekil 1.10. Cep Telefonları

Şekil 1.11. SIM Kartlar - Telsizler

Şekil 1.12. Oyun Konsolları

Şekil 1.13. Bazı Yazıcı ve Belgegeçerler - GPS Cihazları

Şekil 1.14. Manyetik Kartlar - Manyetik Kart Kopyalama Cihazları

Şekil 1.15. Network Cihazları (modem vb.) - POS makineleri

Şekil 1.16. Takoğraf

Şekil 1.17. Görüntü Kayıt Cihazları DVR ile veri depolayabilen diğer materyaller.

1.6. Adli Bilişimin Ülkemizdeki Hukuki Boyutu

Adli bilişimin hukuki boyutunu ele alacak olursak, ülkemizde adli bilişimi ilgilendiren kanun maddeleri aşağıya çıkarılmıştır.

5271 Sayılı Ceza Muhakemesi Kanununda;

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma

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 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.

5237 Sayılı Türk Ceza Kanununda;

Madde 243- Bilişim Sistemine Girme

Madde 244- Sistemi Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme

Madde 245- Banka Veya Kredi Kartlarının Kötüye Kullanılması

Madde 246- Tüzel kişiler hakkında güvenlik tedbiri uygulanması

1.7. Yurt Dışı ve Yurt İçi Adli Bilişim İnceleme Süreçleri

Gelişen teknoloji ile birlikte, dijital medyaların suç oluşturan eylemler ile birlikte kullanılmasıyla, suçu aydınlatmakla görevli kolluk kuvvetleri de dijital materyalleri dikkate almaya başladılar. İlk dijital verilerin suçu aydınlatmada kullanılması 1984 yılına kadar dayanmaktadır. 1984 yılında FBI (Federal Bureau of Investigation- Federal Soruşturma Bürosu) laboratuvarı ve diğer kolluk kuvvetleri tarafından bilgisayar kalıntılarını incelemek için bir program geliştirmeye başlandı ve bilgisayar incelemeleri için Computer Analysis Response Team (CART)'i kuruldu.

1991 yılının başlarında 6 uluslararası kolluk kuvvetinden oluşan bir grup Amerika Birleşik Devletlerinde birleşerek **adli bilişimi ve incelemede standart bir yaklaşımı belirleme** konularını tartıştı.

1993 yılında adli bilişim üzerine düzenlenen Uluslararası Kolluk Kuvvetleri konferansına FBI ev sahipliğini yaptı. Konferansa Ulusal ve Uluslararası alanda 70 temsilci katıldı. Katılımcıların tamamı da **adli bilişim standartlarının eksikliği ve bu standartların ihtiyaç olduğunu kabul etti**.

1995 yılında Amerika Birleşik Devletleri Gizli Servisi tarafından yürütülen bir araştırmada gösterildi ki; kolluk kuvvetlerinin %48 inin adli bilişim laboratuvarlarının olduğu ve bilgisayar kanıtlarının %68 inin bu laboratuvarlara gönderildiği tespit edilmiştir. Yine bu araştırma laboratuvarlarının %70 inde yazılı bir prosedürünün olmadığını gösterdi (Noblett ve ark., 2000).

1995 yılından itibaren tespit edilen bu eksikliğin giderilmesine yönelik "adli bilişim inceleme süreçleri" tasarlanmaya başlandı. O tarihten günümüze kadar yüzlerce süreç tasarımı yapıldı. Bu süreçlerden **on yedisi tarafımızdan incelendi.** Bu süreçlere bakıldığında, birçoğunun birbiri ile aynı olduğu, kiminin bir süreçte gördüğü eksikliği tasarladığı başka bir süreç ile tamamladığı, bazılarının süreci genel olarak değerlendirirken, bazılarının her aşamayı süreç içerisinde tanımladığı, bazılarının ise olayı teknik boyutuyla ele aldığı görülmüştür. Tüm süreçler öncüllerinin tecrübelerinden faydalanmak suretiyle kendi özgün süreçlerini tasarlamışlardır. Tasarlanan süreçlerde kullanılan terimler ve adımların sırası farklılık gösterse de aynı sonuçlara sahiptir.

Türkiyede Adli Bilişim Sürecini incelediğimizde; 2004 yılında 5271 sayılı CMK'nın yürürlüğe girmesi ile birlikte 134. maddesinde bilgisayar ve kütüklerinde yapılacak aramaların ve incelemelerin tanımlanması yapılmıştır. Müteakibinde hukuk sistemimize uygun adli bilişim süreçleri tasarlanmaya başlanmıştır.

Tasarlanan bu süreçlerden **6 tanesi tarafımızdan incelendi.**

1- Doc.Dr. Leyla Berber KESER süreci 5 aşamada **(Toplama, İnceleme, Analiz Etme, Belge Hazırlama ve Raporlama)** değerlendirmiştir.

2- Doç.Dr. Ahmet KOLTUKSUZ'da süreci 5 aşamada **(Tanımlama, Elde Etme, Saklama, İnceleme, Mahkemeye Sunum)** değerlendirmiştir.

3- Jandarma Genel Komutanlığı/Kriminal Daire Başkanlığı süreci 4 aşamada **(Elde Etme, Tanımlama, Değerlendirme** ve **Sunum)** değerlendirmiştir.

4- Yrd.Doc.Dr. Türkay HENKOĞLU süreci 3 aşamada **(Delillerin Tespit Edilmesi, Toplanması ve Muhafazası - Delilleri Açığa Çıkartma, İnceleme ve Analiz Yapılması** ve **Delillerin Raporlanması)** değerlendirmiştir.

5- Yrd.Doç.Dr. Hüseyin ÇAKIR süreci 4 aşamada **(İlk Müdahale, Delil Toplama, Analiz** ve **Rapor)** değerlendirmiştir.

6- Doç.Dr. Harun ARTUNER de süreci 4 aşamada **(Elde Etme, Tanımlama, Değerlendirme ve Sunum)** olarak değerlendirmiştir.

Yurt içerisinde tasarlanmış 6 sürecin tamamı incelendiğinde;

- Süreçlerin aşama sayılarında farklılık olmasına rağmen kapsam olarak birbirleri ile büyük oranda aynı olduğu,

- Süreçlerin Elde Etme/Toplama/Tanımlama/Delillerin Tespit edilmesi/İlk Müdahale ile başladığı,

- Tamamında süreçlerin Raporlama/Sunum ile tamamlandığı anlaşılmıştır.

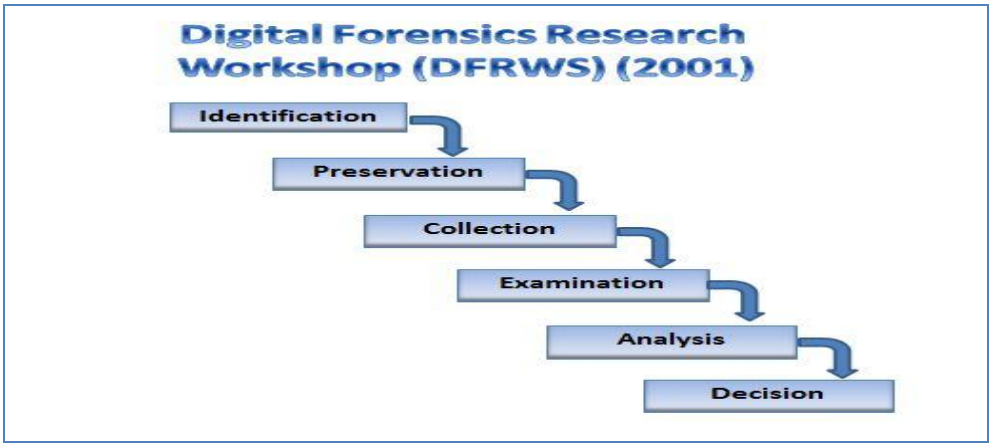
Yurt dışı ve yurt içi inceleme süreçleri **Şekil 1.18. - 1.40.**'da sunulmuştur.

1.7.1. Yurt Dışı Adli Bilişim İnceleme Süreçleri

M.Pollitt 1995 yılında **"Computer Forensic Investigative Process"** olarak adlandırdığı adli bilişim sürecini **4 aşamada** oluşturmuştur. Bu aşamalar **"Acquisition- Identification- Evaluation - Admission"** olarak belirlenmiştir (Pollitt, 1995).

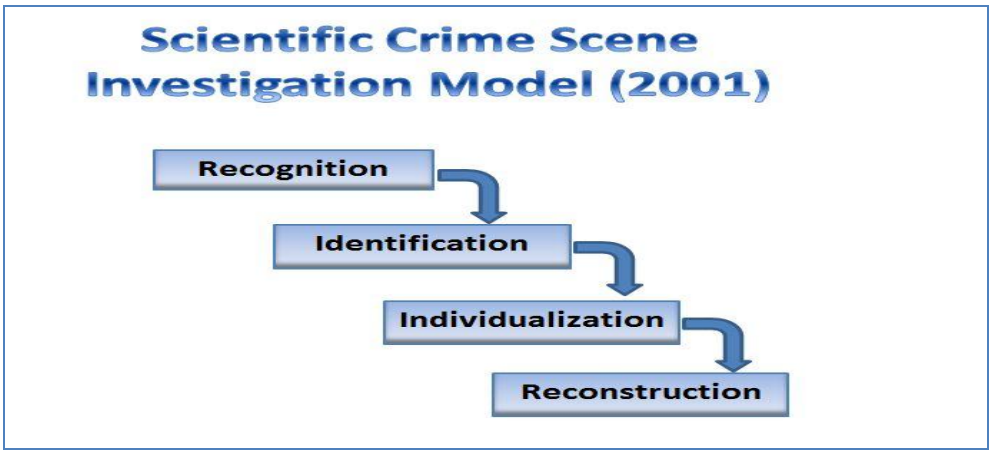
Şekil 1.18. Computer Forensic Investigative Process isimli Adli Bilişim Süreci.

G. Palmer, 2001 yılında **"Digital Forensics Research Workshop(DFRWS)"** olarak adlandırdığı adli bilişim sürecini **6 aşamada** oluşturmuştur. Bu aşamalar **"Identification- Preservation – Collection – Examination – Analysis - Decision"** olarak belirlenmiştir (Palmer, 2001).



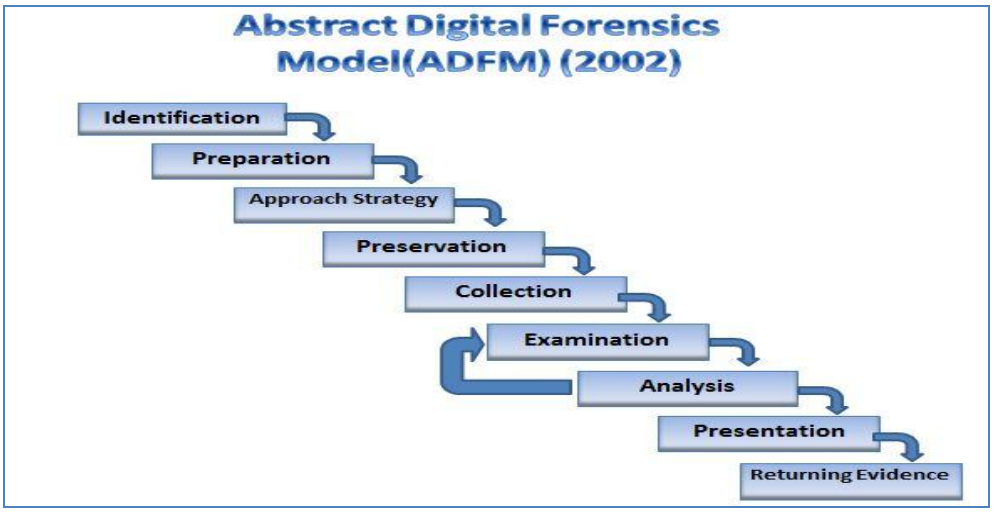
Şekil 1.19. Digital Forensics Research Workshop isimli Adli Bilişim Süreci.

Lee et all, 2001 yılında **"Scientific Crime Scene Investigation Model"** olarak adlandırdığı adli bilişim sürecini **4 aşamada** oluşturmuştur. Bu aşamalar **"Recognition – Identification – Individualization - Reconstruction"** olarak belirlenmiştir (Sachowski, 2016).



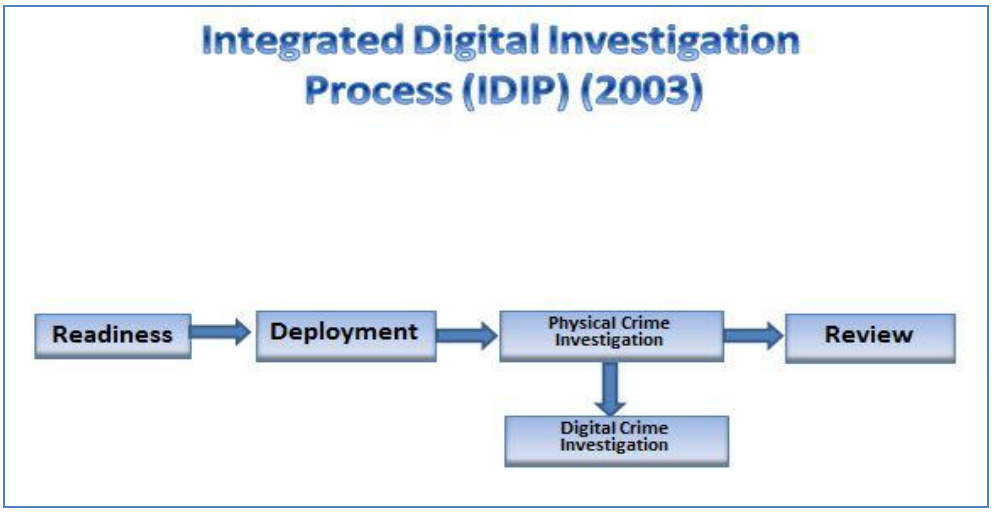
Şekil 1.20. Scientific Crime Scene Investigation Model isimli Adli Bilişim Süreci.

M. Reith, C. Carr & G. Gunsh 2002 yılında **"Abstract Digital Forensics Model (ADFM)"** olarak adlandırdığı adli bilişim sürecini **9 aşamada** oluşturmuştur. Bu aşamalar **" Identification- Preparation – Approach Strategy- Preservation - Collection – Examination – Analysis – Presentation – Returning Evidence"** olarak belirlenmiştir (Reith ve ark., 2002).



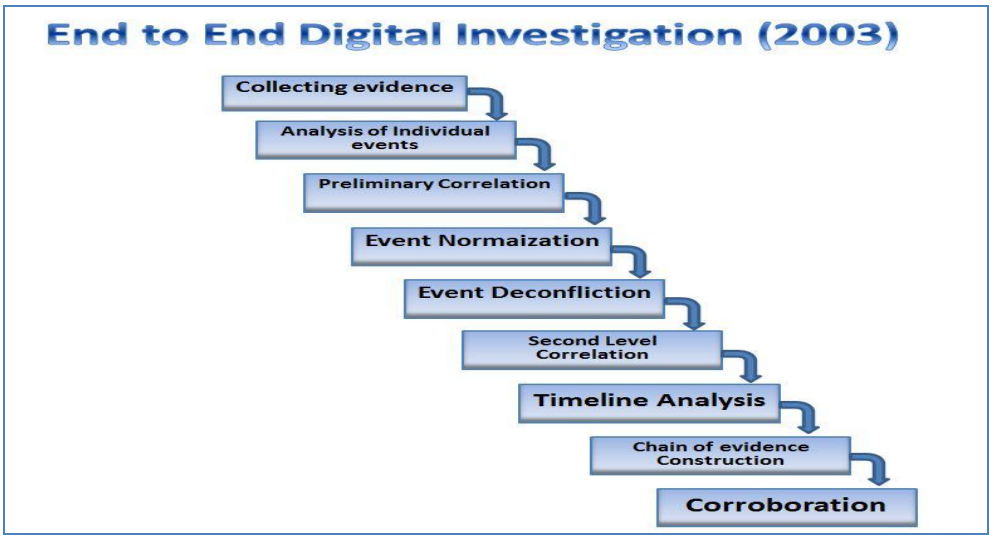
Şekil 1.21. Abstract Digital Forensics Model isimli Adli Bilişim Süreci.

B. Carrier & E. H. Spafford 2003 yılında **"Integrated Digital Investigation Process (IDIP)"** olarak adlandırdığı süreci fiziksel olay yeri incelemesi ile adli bilişim incelemesini eş zamanlı olarak düşünmüş ve sürecini **4 aşamada değerlendirmiştir.** Bu aşamalar **" Readiness- Deployment – Physical Crime Investigation/ Digital Crime Investigation - Review"** olarak belirlenmiştir (Carrier ve Spafford, 2003).



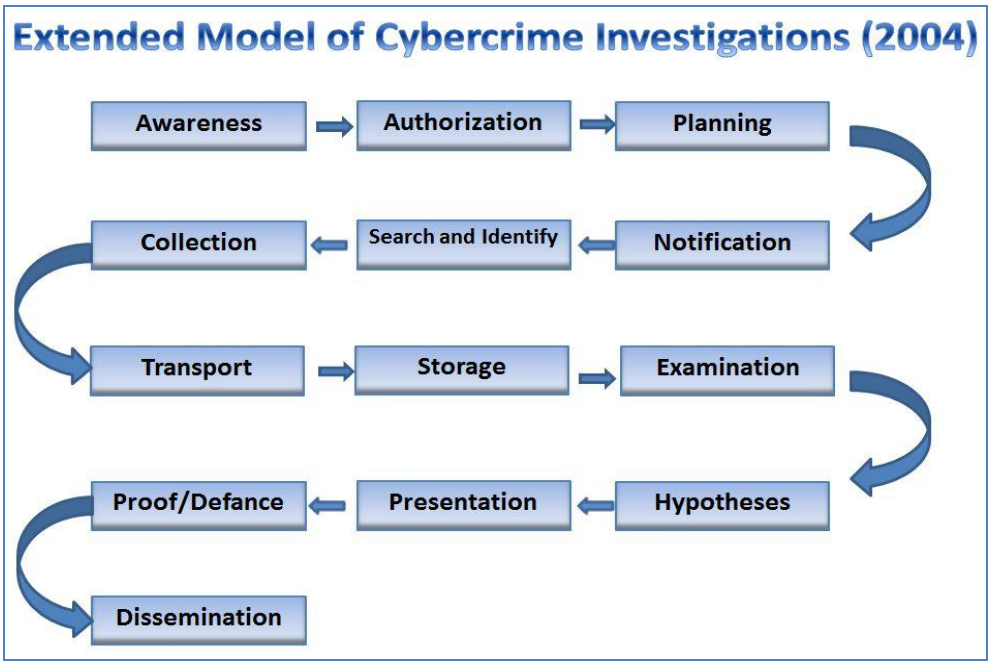
Şekil 1.22. Integrated Digital Investigation Process isimli Adli Bilişim Süreci.

P. Stephenson 2003 yılında **"End to End Digital Investigation"** olarak adlandırdığı adli bilişim sürecini **9 aşamada** oluşturmuştur. Bu aşamalar **"Collecting evidence - Analysis of Individual events – Preliminary Correlation - Event Normaization - Event Deconfliction – Second Level Correlation – Timeline Analysis – Chain of evidence Construction – Corroboration"** olarak belirlenmiştir (Stephenson, 2003).



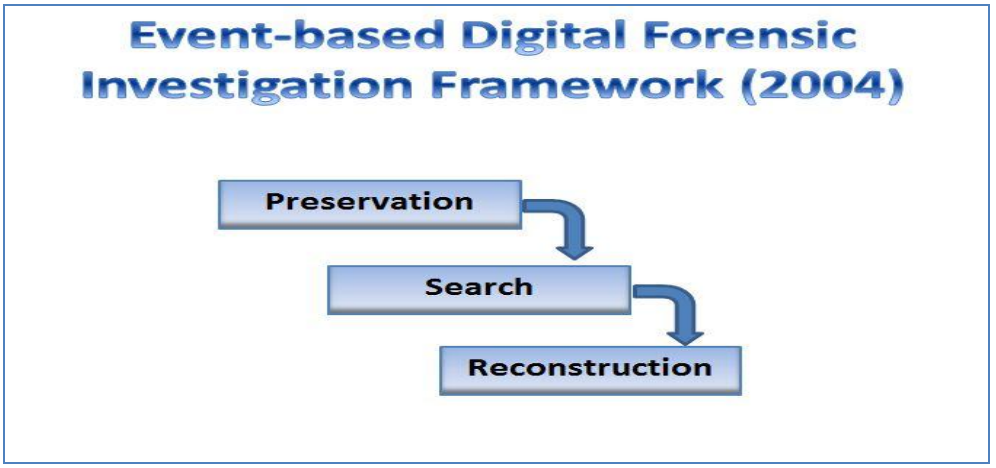
Şekil 1.23. End to End Digital Investigation isimli Adli Bilişim Süreci.

S. Ciardhuain 2004 yılında **"Extended Model of Cybercrime Investigation"** olarak adlandırdığı adli bilişim sürecini **13 aşamada** oluşturmuştur. Bu aşamalar **"Awareness - Authorization – Planning - Notification - Search and Identify – Collection – Transport – Storage – Examination" Hypotheses - Presentation - Proof/Defance - Dissemination** olarak belirlenmiştir (Ciardhuain, 2004).



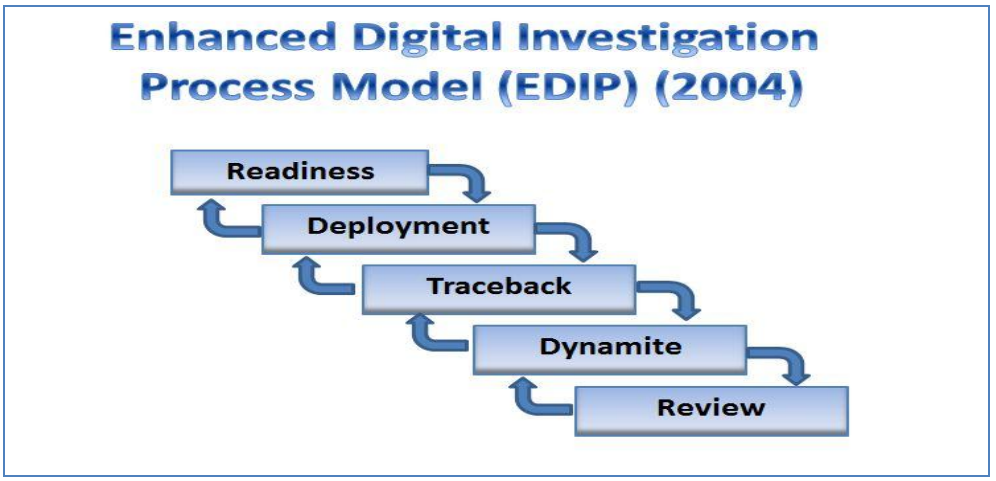
Şekil 1.24. Extended Model of Cybercrime Investigation isimli Adli Bilişim Süreci.

Carrier, B., & Spafford, E. H. 2004 yılında **"Event-based Digital Forensic Investigation Framework"** olarak adlandırdığı adli bilişim sürecini **3 aşamada** oluşturmuştur. Bu aşamalar **"Preservation – Search - Reconstruction** olarak belirlenmiştir (Carrier ve Spafford, 2004).



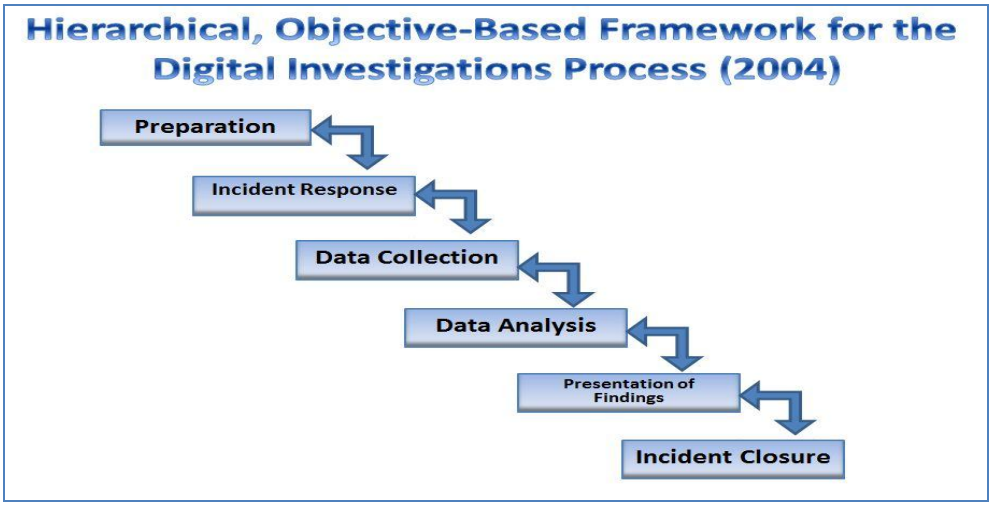
Şekil 1.25. Event-based Digital Forensic Investigation Framework isimli Adli Bilişim Süreci.

V. Baryamereeba & F. Tushabe. 2004 yılında **"Enganced Digital Investigation Process Model (EDIP)"** olarak adlandırdığı adli bilişim sürecini **5 aşamada** oluşturmuştur. Bu aşamalar **"Readiness – Deployment – Traceback – Dynamite- Review** olarak belirlenmiştir (Baryamereeba ve Tushabe, 2004).



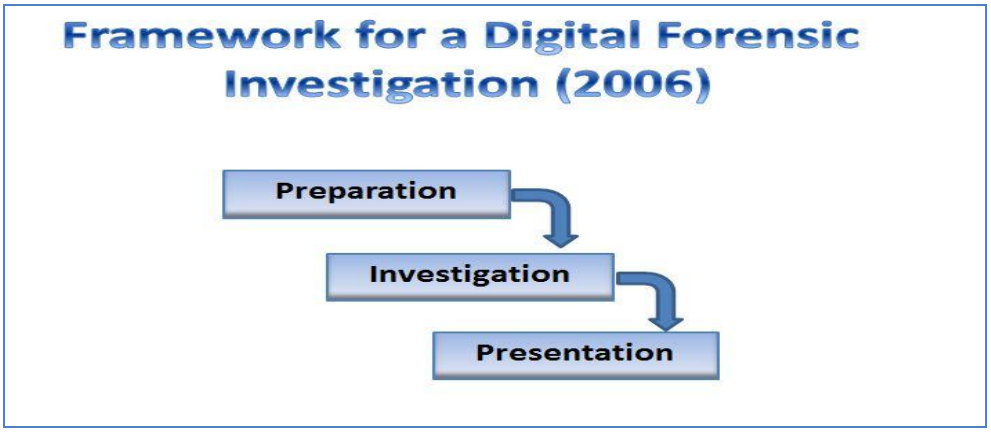
Şekil 1.26. Enganced Digital Investigation Process Model isimli Adli Bilişim Süreci.

V. Baryamereeba & F. Tushabe 2004 yılında **"Hierarchical, Objective-Based Framework for the Digital Investigations Process"** olarak adlandırdığı adli bilişim sürecini **6 aşamada** oluşturmuştur. Bu aşamalar **"Preparation – Incident Response – Data Collection – Data Analysis- Presentation of Findings - Incident Closure** olarak belirlenmiştir (Beebe ve Clark, 2004).



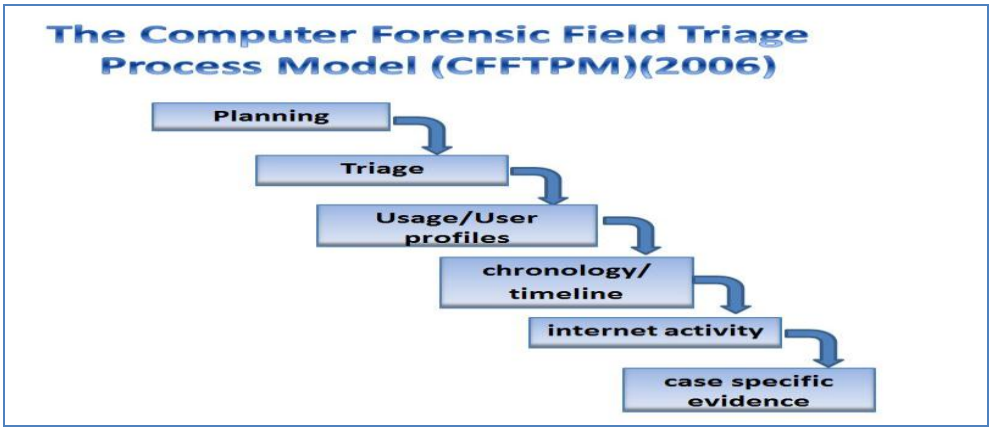
Şekil 1.27. Hierarchical, Objective-Based Framework for the Digital Investigations Process isimli Adli Bilişim Süreci.

M. Kohn, J. H. P. Eloff, & M. S. Olivier. 2006 yılında **"Framework for a Digital Forensic Investigation"** olarak adlandırdığı adli bilişim sürecini **3 aşamada** oluşturmuştur. Bu aşamalar **"Preparation – Investigation – Presentation**" olarak belirlenmiştir (Kohn ve ark., 2006).



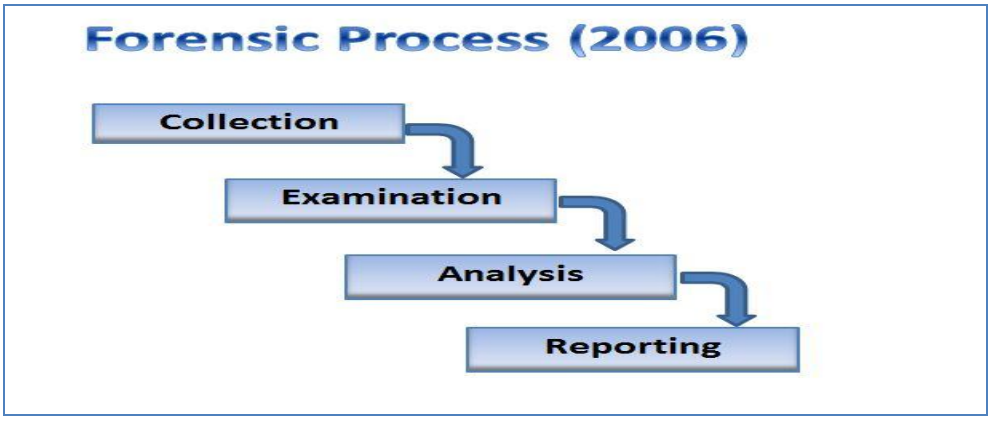
Şekil 1.28. Framework for a Digital Forensic Investigation isimli Adli Bilişim Süreci.

M. K. Rogers, J. Goldman, R. Mislan, T. Wedge & S. Debrota. 2006 yılında **"The Computer Forensic Field Triage Process Model (CFFTPM)"** olarak adlandırılan adli bilişim sürecini **6 aşamada** oluşturmuştur. Bu aşamalar **"Planning – Triage – Usage/User profiles - chronology/Timeline - internet activity- case specific evidence"** olarak belirlenmiştir (Rogers ve ark., 2006).



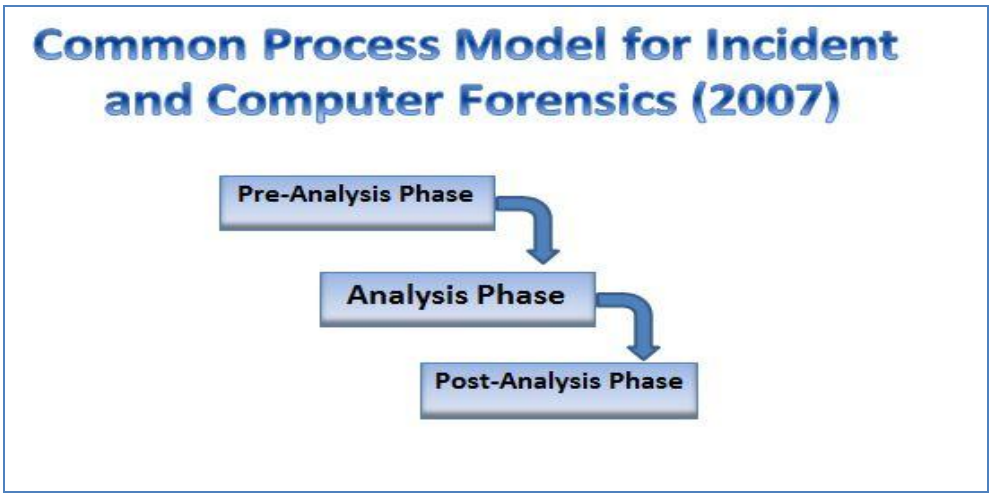
Şekil 1.29. The Computer Forensic Field Triage Process Model isimli Adli Bilişim Süreci.

Amerika Birleşik devletlerinde bulunan Ulusal Teknoloji ve Standart Enstitüsü - NIST (National Instute of Standards and Technology) tarafından **"Forensic Process"** olarak adlandırılan adli bilişim sürecini **4 aşamada** oluşturmuştur. Bu aşamalar **"Collection – Examination- Analysis – Reporting"** olarak değerlendirmiştir (NIST, 2006).



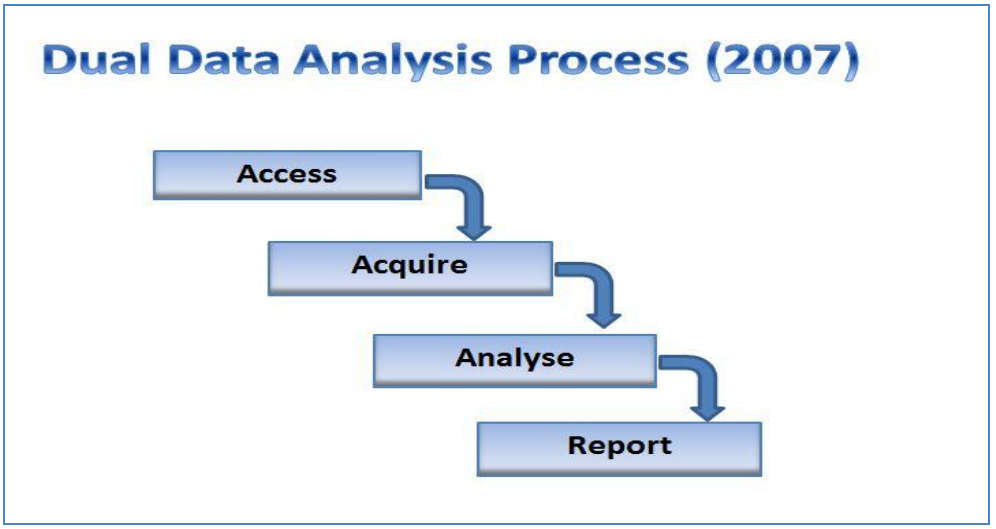
Şekil 1.30. Forensic Process isimli Adli Bilişim Süreci.

F. C. Freiling & B. Schwittay. 2007 yılında **"Common Process Model for Incident and Computer Forensic"** olarak adlandırılan adli bilişim sürecini **3 aşamada** oluşturmuştur. Bu aşamalar **"Pre- Analysis phase - Analysis phase - post-Analysis phase"** olarak belirlenmiştir (Freiling ve Schwittay, 2007).



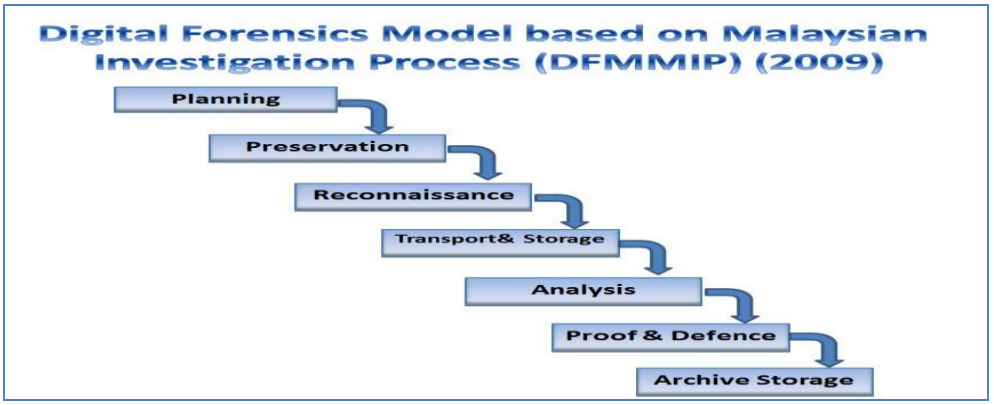
Şekil 1.31. Common Process Model for Incident and Computer Forensic isimli Adli Bilişim Süreci.

D. Bem & E. Huebner. 2007 yılında **"Dual Data Analysis Process"** olarak adlandırılan adli bilişim sürecini **4 aşamada** oluşturmuştur. Bu aşamalar **"Access – Acquire – Analyse - Report"** olarak belirlenmiştir (Bem ve Huebner, 2007).



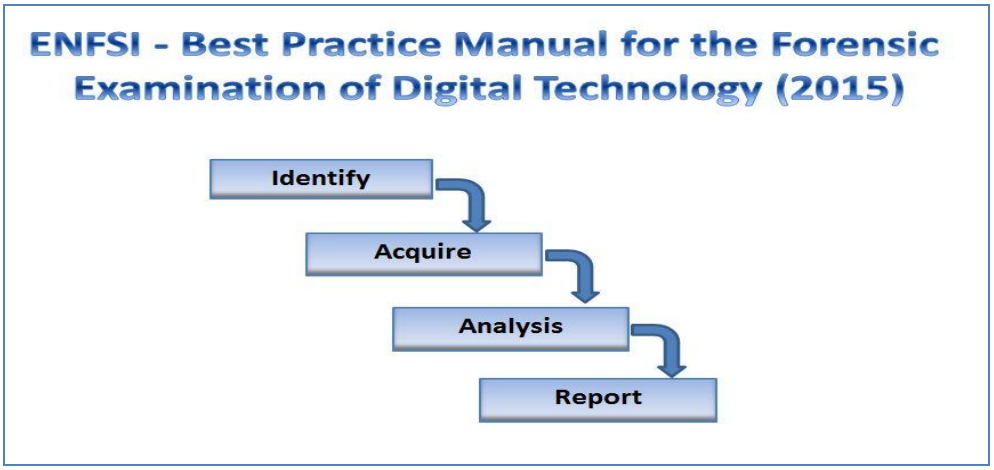
Şekil 1.32. Dual Data Analysis Process isimli Adli Bilişim Süreci.

Perumal, S.. 2009 yılında **"Digital Forensics Model based on Malaysian Investigation Process (DFMMIP)"** olarak adlandırılan adli bilişim sürecini **7 aşamada** oluşturmuştur. Bu aşamalar **"Planning**, **Identification**, **Reconnaissance Transport & Storage**, **Analysis Proof & Defense** ve **Archive Storage** olarak belirlenmiştir (Sundresan, 2009).



Şekil 1.33. Digital Forensics Model based on Malaysian Investigation Process isimli Adli Bilişim Süreci.

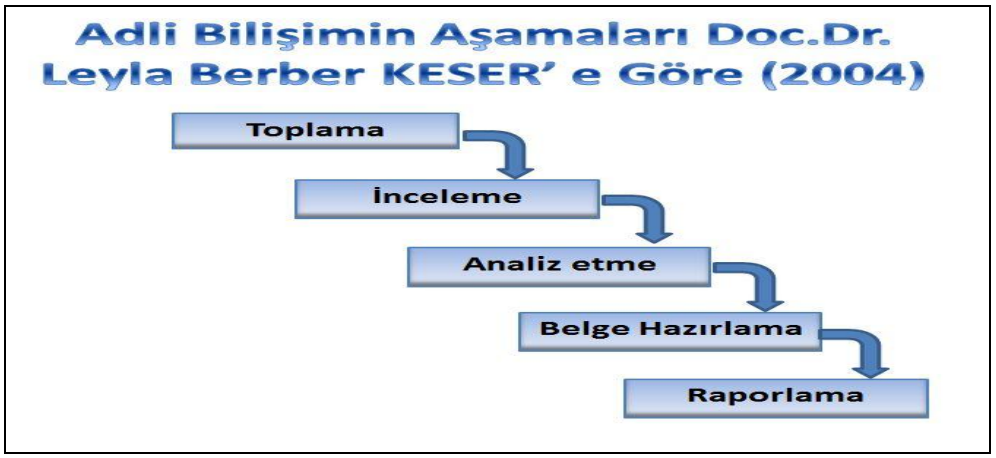
European Network of Forensic Science Institutes (ENFSI) 2015 yılında **"Best Practice Manual for the Forensic Examination of Digital Technology"** isimli çalışmasında belirlediği adli bilişim sürecini **4 aşamada** oluşturmuştur. Bu aşamalar **"Identify- Acquire – Analysis - Report** olarak belirlenmiştir (ENFSI, 2015).



Şekil 1.34. Best Practice Manual for the Forensic Examination of Digital Technology isimli Adli Bilişim Süreci.

1.7.2. Yurt İçi Adli Bilişim İnceleme Süreçleri

Doç.Dr. Leyla Berber Keser 2004 yılında adli bilişim sürecini **5 aşamada** oluşturmuştur. Bu aşamalar **"Toplama – İnceleme – Analiz Etme – Belge Hazırlama – Raporlama"** olarak belirlenmiştir (Keser, 2004 s.:45).

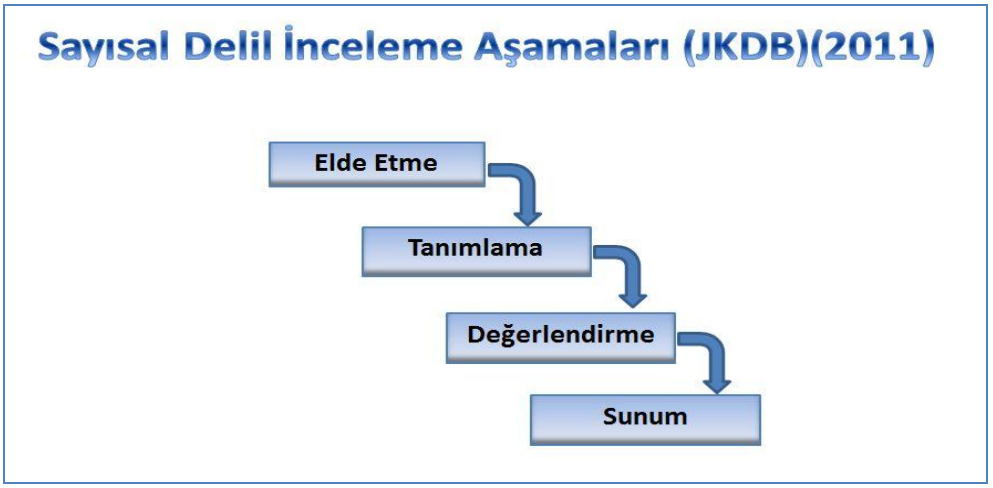


Şekil 1.35. Doç.Dr. Leyla Berber Keser'e Göre Adli Bilişim Süreci.

Doç.Dr. Ahmet Koltuksuz 2010 yılında adli bilişim sürecini **5 aşamada** oluşturmuştur. Bu aşamalar **"Tanımlama – Elde Etme – Saklanması – İnceleme – Mahkemeye Sunum"** olarak belirlenmiştir (Koltuksuz, 2010).

Şekil 1.36. Doç.Dr. Ahmet Koltuksuz'a Göre Adli Bilişim Süreci.

Jandarma Genel Komutanlığı/Kriminal Daire Başkanlığı adli bilişim sürecini **4 aşamada** oluşturmuştur. Bu aşamalar **"Elde Etme – Tanımlama – Değerlendirme - Sunum"** olarak belirlenmiştir (JKDB, 2011 s.:158).

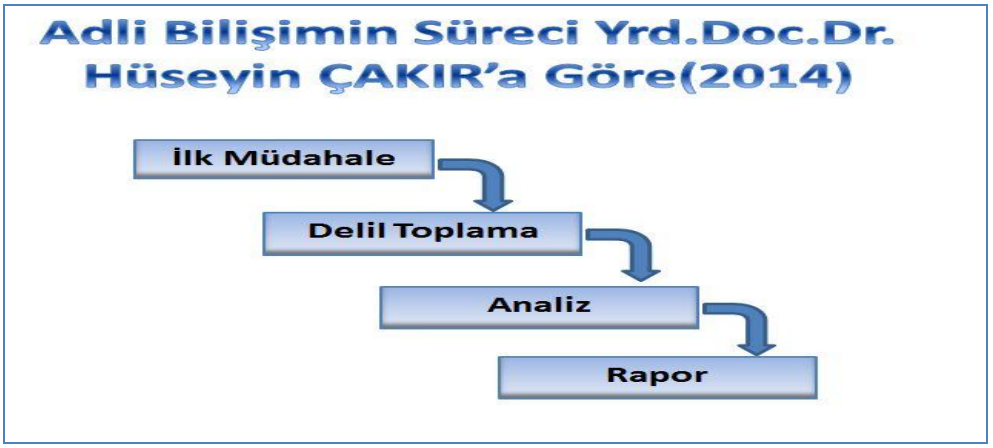


Şekil 1.37. Jandarma Genel Komutanlığı/Kriminal Daire Başkanlığı'na Göre Adli Bilişim Süreci**.**

Yrd.Doç.Dr. Türkay HENKOĞLU 2011 yılında adli bilişim sürecini **3 aşamada** oluşturmuştur. Bu aşamalar **"Delillerin tespit edilmesi, toplanması ve muhafazası - Delilleri açığa çıkartma, inceleme ve analiz yapılması – Delillerin raporlanması"** olarak belirlenmiştir (Henkoğlu, 2011 s.:17).

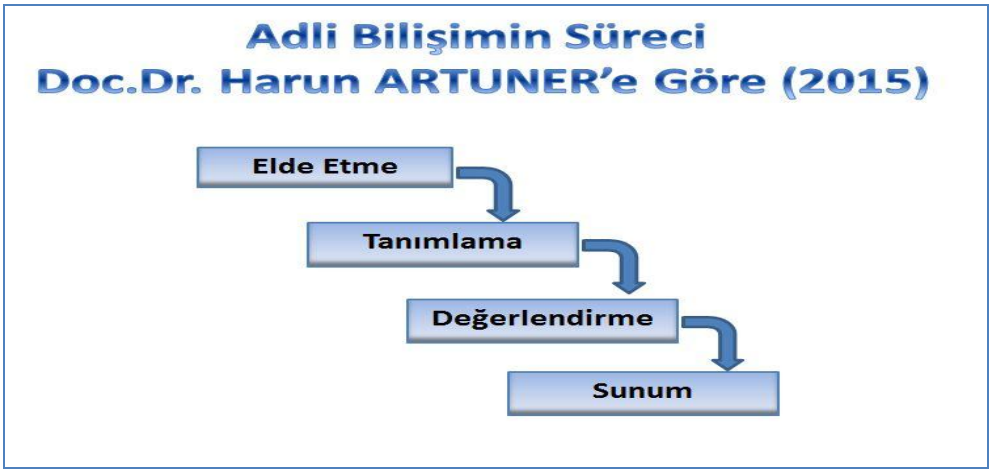
Şekil 1.38. Yrd.Doç.Dr. Türkay HENKOĞLU'na Göre Adli Bilişim Süreci.

Yrd.Doç.Dr. Hüseyin ÇAKIR 2014 yılında adli bilişim sürecini **4 aşamada** oluşturmuştur. Bu aşamalar **"İlk Müdahale – Delil Toplama – Analiz- Rapor"** olarak belirlenmiştir (Çakır ve Kılıç 2014 s.:199).



Şekil 1.39. Yrd.Doç.Dr. Hüseyin ÇAKIR'a Göre Adli Bilişim Süreci.

Doç.Dr. Harun ARTUNER 2015 yılında adli bilişim sürecini **4 aşamada** oluşturmuştur. Bu aşamalar **"Elde Etme – Tanımlama – Değerlendirme - Sunum"** olarak belirlenmiştir (Artuner, 2015 s.:3).



Şekil 1.40. Doç.Dr. Harun ARTUNER'e Göre Adli Bilişim Süreci.

Çizelge 1.1. Yurt Dışı Adli Bilişim İnceleme Süreçleri.

SÜREÇ KİMLİK NO	YIL	İNCELEME SÜRECİNİN İSMİ
S1	1995	Computer Forensic Investigative Process
S2	2001	Digital Forensics Research Workshop (DFRWS)
S3	2001	Scientific Crime Scene Investigation Model
S4	2002	Abstract Digital Forensics Model(ADFM)
S5	2003	Integrated Digital Investigation Process (IDIP)
S6	2003	End to End Digital Investigation
S7	2004	Extended Model of Cybercrime Investigations
S8	2004	Event-based Digital Forensic Investigation Framework
S9	2004	Enhanced Digital Investigation Process Model
S10	2004	Hierarchical, Objective-Based Framework for the Digital Investigations Process
S11	2006	Framework for a Digital Forensic Investigation
S12	2006	The Computer Forensic Field Triage Process Model (CFFTPM)
S13	2006	Forensic Process (NIST) (National Instute of Standards and Technology)
S14	2004	Common Process Model for Incident and Computer Forensics
S15	2007	Dual Data Analysis Process
S16	2009	Digital Forensics Model based on Malaysian Investigation Process (DFMMIP)
S17	2015	European Network of Forensic Science Institutes (ENFSI)-Best Practice Manual for the Forensic Examination of Digital Technology

Çizelge 1.2. Yurt İçi Adli Bilişim İnceleme Süreçleri.

SÜREÇ KİMLİK NO	YIL	İNCELEME SÜRECİNİN İSMİ
S18	2004	Adli Bilişim Aşamaları -Doç.Dr. Leyla Berber KESER'e Göre
S19	2010	Adli Bilişim Aşamaları -Doç.Dr. Ahmet KOLTUKSUZ'a Göre
S20	2011	Sayısal Delil İnceleme Aşamaları - JKDB
S21	2011	Adli Bilişim Aşamaları -Yrd.Doç.Dr. Türkay HENKOĞLU'na Göre
S22	2014	Adli Bilişim Süreci-Yrd.Doç.Dr. Hüseyin ÇAKIR'a Göre
S23	2015	Adli Bilişim Süreci Doç.Dr.Harun ARTUNER'e Göre

Çizelge 1.3. Yurt Dışı Adli Bilişim İnceleme Süreçlerinin Aşamaları.

KİMLİK NO	AŞAMA İSMİ	SÜREÇ KİMLİK NO
K1	Acquisition	S1, S15, S17
K2	Access	S15
K3	Admission	S1,
K4	Analyse	S15
K5	Analysis	S2, S4, S13, S16, S17
K6	Analysis of Individual events	S6
K7	Analysis Phase	S14
K8	Approach Strategy	S4
K9	Archive Storage	S16
K10	Authorization	S7
K11	Awareness	S7
K12	case specific evidence	S12
K13	Chain of evidence Construction	S6
K14	chronology/timeline	S12
K15	Collecting Evidence	S6
K16	Collection	S2, S4, S7, S13
K17	Corroboration	S6
K18	Data Analysis	S10
K19	Data Collection	S10
K20	Decision	S2
K21	Deployment	S5, S9
K22	Digital Crime Investigation	S5
K23	Dissemination	S7
K24	Dynamite	S9

Çizelge 1.3. Devam Yurt Dışı Adli Bilişim İnceleme Süreçlerinin Aşamaları.

KİMLİK NO	AŞAMA İSMİ	SÜREÇ KİMLİK NO
K25	Evaluation	S1,
K26	Event Deconfliction	S6
K27	Event Normaization	S6
K28	Examination	S2, S4, S7, S13
K29	Hypotheses	S7
K30	Identification	S1, S2, S3, S4, S17
K31	Incident Closure	S10
K32	Incident Response	S10
K33	Individualization	S3
K34	Investigation	S11
K35	Internet activity	S12
K36	Notification	S7
K37	Physical Crime Investigation	S5
K38	Planning	S7, S12, S16
K39	Post-Analysis Phase	S14
K40	Pre-Analysis Phase	S14
K41	Preliminary Correlation	S6
K42	Preparation	S4, S10, S11
K43	Presentation	S4, S7, S11
K44	Presentation of Findings	S10
K45	Preservation	S2, S4, S8, S16
K46	Proof & Defence	S7, S16
K47	Readiness	S5, S9
K48	Recognition	S3
K49	Reconnaissance	S16
K50	Reconstruction	S3, S8
K51	Report	S15, S17
K52	Reporting	S13
K53	Returning Evidence	S4
K54	Review	S5, S9
K55	Search	S8
K56	Search and Identify	S7
K57	Second Level Correlation	S6
K58	Storage	S7
K59	Timeline Analysis	S6
K60	Traceback	S9
K61	Transport	S7
K62	Transport& Storage	S16
K63	Triage	S12
K64	Usage/User profiles	S12

Çizelge 1.4. Yurt İçi Adli Bilişim İnceleme Süreçlerinin Aşamaları.

KİMLİK NO	AŞAMA İSMİ	SÜREÇ KİMLİK NO
K65	Toplama	S18
K66	İnceleme	S18
K67	Analiz Etme	S18
K68	Belge Hazırlama	S18
K69	Raporlama	S18
K70	Tanımlama	S19, S20, S23
K71	Elde Etme	S19, S20, S23
K72	Saklanması	S19
K73	İnceleme	S19
K74	Mahkemeye Sunum	S19
K75	Değerlendirme	S20, S23
K76	Sunum	S20, S23
K77	Delillerin tespit edilmesi, toplanması ve muhafazası	S21
K78	Delilleri açığa çıkartma, inceleme ve analiz yapılması	S21
K79	Delillerin raporlanması	S21
K80	İlk Müdahale	S22
K81	Delil Toplama	S22
K82	Analiz	S22
K83	Rapor	S22

1.8. İdeal Bir Adli Bilişim İnceleme Sürecinin Tasarlanması

Tasarlanan adli bilişim inceleme sürecinde, 20 yıllık (1995-2015) süre içerisinindeki yurt dışı ve yurt içerisindeki toplam 23 inceleme süreçleri analiz edilmiş ve mevcut hukuk sistemimizde dikkate alınarak sürecin **4 AŞAMADAN** oluşması gerektiği değerlendirilmiştir. Bu aşamalar içerisinde yurt dışındaki süreçlerde belirtilen fakat yurt içerisindeki süreçlerde bahsedilmeyen **2 YENİ AŞAMA** eklenmiştir. Bu iki yeni aşamadan ilki **HAZIRLIK AŞAMASI'dır.** Hazırlık aşaması 2 yönlü olarak değerlendirilmiştir.

Birincisi hukuki hazırlıktır. Biraz açmak gerekirse, öncelikle olay yerinde bilişim delillerinin toplanması için gerekli olan yasal izinlerin alınması gerekmektedir. Gerekli yasal izni olmayan bir delile teknik açıdan doğru müdahale edilse bile mahkeme tarafından delil olarak kabul edilmeyecektir (6100 sayılı HMK'nın 189/2. maddesi gereği hukuka aykırı olarak elde edilmiş olan deliller mahkeme tarafından bir vakanın ispatında dikkate alınmaz hükmü yer almaktadır.).

Bir diğeri ise gerekli teknik alt yapının hazır halde olması gerekliliğidir. Yeterli ve gerekli teknik bilgisi olmayan veya gerekli teknik donanımı yetersiz olan bir kolluk görevlisinin delile müdahalesi geriye döndürülemeyecek sakatlıklara yol açacak ve bir sonraki aşamada inceleme yapan uzman/bilirkişilerin incelemelerine olumsuz bir etki yapacaktır.

Bu yeni aşamanın ikincisi ise yine yurt dışındaki **"Abstract Digital Forensics Model (ADFM)"** isimli sürecin son aşamasında belirtilen **(Returning Evidence)** fakat yurt içerisindeki süreçlerde bahsedilmeyen **"…DELİLLERİN İADESİ AŞAMASI" dır.** Delillerin iadesi konusunun tarafımızca çok önemli bir aşama olduğu değerlendirilmektedir. Çünkü adli bir incelemenin tamamlanması ve raporunun düzenlenmesi ile birlikte ihtimal dâhilindedir ki incelemeyi yapan kişi/kurum tarafından inceleme son bulmuş olabilir, beri tarafından bir incelemenin sonu başka bir incelemenin başlangıç olabilecektir. Sağlıklı bir incelemenin yapılabilmesi için en başta delilin sağlam (incelenebilir) olması gerekmektedir. Delilin süreç içerisinde hasar görmesi durumunda üzerinde herhangi bir inceleme yapılamayacaktır. Bu nedenle inceleme süreçleri tasarlanırken **kesinlikle delilin iadesi, sürecin bir aşaması olarak değerlendirilmesi gerekmektedir.**

Süreç bir bilişim deliline müdahale aşamalarının tümünü kapsayacak şekilde tasarlanmıştır. Bundan amaç delile ilk müdahaleden, iadesi aşamasına kadar, sağlıklı bir zincir oluşturacak bir süreç tasarımı oluşturmaktır.

İdeal Bir Adli Bilişim Süreci;

1- Hazırlık Aşaması
2- Delillerin Tespit Edilmesi, Toplanması, Muhafazası ve Laboratuvara Gönderilmesi Aşaması
3- Deliller Üzerinde Gerekli İnceleme ve Analiz Faaliyetleri Aşaması
4- İnceleme Sonucu Raporlama ve Delillerin İadesi Aşaması olarak tanımlanmıştır.

Çizelge 1.5. İdeal Bir Adli Bilişim İnceleme Süreci.

S.No	Aşamalar	Mevcut Süreç Kimlik No
1	Hazırlık Aşaması	K8, K10, K11, K36, K38, K40, K42, K47, K48,
2	Delillerin Tespit Edilmesi, Toplanması, Muhafazası ve Laboratuvara Gönderilmesi Aşaması	K1, K2, K13, K15, K16, K19, K21, K30, K41, K45, K55, K56, K58, K61, K62, K65, K70, K71, K72, K77, K80, K81
3	Deliller Üzerinde Gerekli İnceleme ve Analiz Faaliyetleri Aşaması	K4, K5, K6, K7, K12, K14, K18, K22, K24, K25, K26, K27, K28, K29, K33, K34, K35, K37, K49, K50, K57, K59, K60, K63, K64, K66, K67, K73, K78, K82
4	İnceleme Sonucu Raporlama ve Delillerin İadesi Aşaması	K3, K9, K17, K20, K23, K31, K32, K39, K43, K44, K46, K51, K52, K53, K54, K68, K69, K74, K75, K76, K79, K83

Şekil 1.41. Adli Bilişim İnceleme Süreci.

Tasarlanan İdeal Adli Bilişim İnceleme Süreci;

1.8.1. Hazırlık Aşaması;

✓ Hazırlık aşamasında sorumluluk bölgesinde meydana gelen bir olaya müdahale edecek olan kolluk kuvvetleri gerekli olan olay yeri incelemesini yapabilmesi için öncelikle gerekli yasal izinlerini alması gerekmektedir (CMK md.161). Ya da şüpheli şahısların üstü, eşyası, konutu, işyeri veya ona ait diğer yerlerde bir arama yapacaksa eğer bununla ilgili olarak ta gerekli arama ve el koyma kararlarını alması gerekmektedir (CMK md.119).

✓ Eğer yapılacak olan olay yeri incelemesi veya ev/işyeri vb. aramalarında adli bilişim delillerinin bulunabileceği değerlendiriliyorsa bununla ilgili gerekli tedbirlerin alınması gerekmektedir (Örneğin, açık olan bir bilgisayara müdahale edilecekse bir dizüstü bilgisayar, portable çalışabilen imaj alma yazılımları, sabit diskinin imajının alınabilmesi amacıyla imaj alma donanımları ve büyük kapasiteli taşınabilir diskler temin edilmelidir). Böyle bir olaya müdahale edecek kişinin de bu konuda özel eğitim almış olması gerekmektedir.

✓ Ayrıca yine olay yeri incelemelerinde kullanılan video kamera, fotoğraf makinesi ve olay yeri inceleme faaliyetleri esnasında kullanılan çeşitli ekipmanlar hazır bulunmalıdır.

1.8.2. Delillerin Tespit Edilmesi, Toplanması, Muhafazası ve Laboratuvara Gönderilmesi Aşaması

1.8.2.1.Delillerin Tespit Edilmesi;

Adli bilişimin başladığı nokta, el koymanın başladığı noktadır. Dolayısıyla, sürecin başladığı yer olan olay yerinde (içinde delillerin bulunduğu alan) yapılan incelemede yapılan hatalar, delillerin gerçekliğine ve güvenirliliğine gölge düşüreceği için tüm süreci sekteye uğratabilir (Henkoğlu, 2014 s.:17).

Bu nedenle sağlıklı bir olay yeri incelemesi yapılabilmesi amacıyla aşağıda belirtilen hususlara dikkat edilmelidir.

- ✓ Delillerin değişmesine ya da bozulmasına imkan tanımamak amacıyla olay yerinin güvenliği sağlanmalıdır. Çevre güvenliğinin asıl amacı delilleri korumaktır. Bu aşamada olay yerine giriş kontrol altına alınmalı, giren ve çıkan kişilerin kaydı tutulmalı ve amaçsız bir şekilde olay mahallinde bulunulmasına izin verilmemelidir. Özellikle dışarıya çıkan kişilerin üzerinde herhangi bir materyalin bulunmadığından emin olunmalıdır (Henkoğlu, 2014 s.:19).

- ✓ Olay yerinde incelemesi esnasında oda içindeki konumlarını da gösterecek şekilde olay yerinde kullanılan tüm materyaller (yazıcı, tarayıcı, monitör vb.) bilgisayar ekranında görülen bilgiler ve tüm bağlantı kabloları (yükseltilmiş zemin veya asma tavan mevcut ise, bu durumu da gözden kaçırmadan) fotoğraflanmalıdır (Henkoğlu, 2014 s.:19).

✓ Olay yerinde bulunan ve delil olarak değerlendirilen tüm bulgular numaratör vasıtasıyla belirlenmeli ve tespit edilen tüm bulguların ayrıntılı bir tanımı yapılmalıdır. Bulguların fiziki durumu açık bir şekilde belirlenerek bulgu tespit formuna kaydedilmelidir (Seri numarası, marka, model ve üzerinde bulunan yanık, kırık, çizik gibi kusurlar vs.).

✓ Olay yeri inceleme sürecinin başladığı andan, son ana kadar yapılan her işlem mutlaka olay yerinde tutulan dokümanlara kaydedilmelidir (Henkoğlu, 2014 s.:20).

✓ Bilgisayarlara uzaktan erişim amacıyla erişilmeyi sağlayan cihaz (faks vb.) ve bağlantılan öncelikle tespit edilmeli ve sökülmeden etiketlenmelidir. Şayet olay yerine ulaşıldığında bilgisayar açık ve uzaktan erişim mevcutsa (aktif haldeki modem, iletişim alma-gönderme ışıklarının yanma ve sönmesinden anlaşılabilir) bu durumda bağlantı iptal edilmeli ve mutlaka kayda geçirilmelidir. Benzer şekilde, bilgisayarların başka bilgisayarlar ya da bilgisayar ağları ile haberleşmesinde kullanılan tüm bağlantılar (Ethernet, kızılötesi, GPRS, fireware, kablosuz ağ) etilektenmelidir (Henkoğlu, 2014 s.:20).

✓ Olay yerinde yapılan incelemeler esnasında bilgisayar (masaüstü/dizüstü) mevcut ve açık konumda bulunuyorsa bilgisayar üzerinde hiçbir işlem yapılmadan açık bilgisayarlardan canlı inceleme esaslarına göre (MacLockPick, Belksoft Live RAM, Encase Portable, Live Response, SIW, Helix 3 Pro gibi canlı inceleme yazılımları kullanılmak suretiyle) hareket edilmelidir.

✓ Bilgisayar ya da çalışma masası etrafında bulunan notlar kaydedilmeli ve aynı zamanda fotoğrafları çekilmelidir. Bu tür notlarda analiz aşamasında ihtiyaç duyulabilecek şifre ve kullanıcı kayıt bilgileri yer alabilmektedir (Henkoğlu, 2014 s.:21).

✓ Bilgisayarın kasası üzerinde ve CD/DVD sürücüsünde herhangi bir harici veri depolama biriminin (USB bellek, SD hafıza kartı, CD/DVD) olup olmadığı kontrol edilir.

✓ Olay yerinde bulunan ve üzerinde veri depolama ünitesi olabileceği değerlendirilen her türlü cihaz dikkate alınmalı ve hassasiyetle incelenmelidir. Görünüşte sıradan bir daktilo gibi görünen, fakat incelendiğinde gerçekte bir bilgisayar olduğu saptanan durumlarla (Henkoğlu, 2014, s.:21) ya da bir kalem gibi görünen ama gerçekte bir kalem kamera/ses kayıt cihazı olduğu saptanan durumlarla karşılaşmak mümkündür.

1.8.2.2.Delillerin Toplanması

✓ Toplanacak bulgu ve deliller üzerinde başka bir bulgu ve delilin de bulunabileceği düşünülerek (CD üzerinde parmak izi veya kan lekesinin bulunabileceği) hareket edilmelidir ve bu bulgulara da zarar vermeden müdahale edilmeye özen gösterilir. Gerekirse elektronik cihaz ve veri depolama üniteleri (CD/DVD gibi) üzerindeki parmak izi araştırması gibi kriminal işlemler ilk aşamada dijital delillerin toplanması işlemi ile birlikte yürütülür (örneğin klavye, bilgisayar kasası vb. deliller üzerinde tespit edilen parmak izi gibi delillerin öncelikli olarak toplanması gibi).

✓ Dijital delillere zarar verebileceği için, dijital deliller toplanmadan gizli izleri elde etmek amacıyla olay yerinde kimyasal maddeler kullanılmamalıdır (Henkoğlu, 2014 s.:20).

✓ Olay yeri incelemesinde gereken genel kurallar çerçevesinde, öncelikle çalışan sistemler tespit edilmeli ve uçucu delillerin analizi ile ilgili açık bilgisayarlardan canlı inceleme esaslarına göre hareket edilmelidir.

✓ Olay yerinde açık bulunan bilgisayarlar üzerindeki Trucrypt ve Bitlocker gibi dosya/disk şifreleme programlarının varlığı araştırılmalı, söz konusu programlar ile şifrelenmiş dosya veya disk bölümlerinin tespit edilmesi durumunda açık bilgisayarlardan canlı inceleme esaslarına göre gerekli incelemeler yapılır.

✓ Olay yerindeki açık bilgisayarların kapatma işlemi esnasında öncelikli olarak bilgisayara bağlı vaziyette güç kaynağı var ise bilgisayar ile bağlantısı kesilir. Bazı dizüstü bilgisayarlarda disket veya CD sürücü bölümüne yerleştirilmiş ikinci bataryanın olabileceği de unutulmamalıdır. Sonraki aşamada ise bilgisayarın işletim sisteminin durumu göz önünde bulundurularak kapatma işleminin yapılması gerekir. Bunun nedeni ise Windows işletim sistemleri (WinNT, WinXP, Vista, Win7, Win8) bilgisayarın fişini çekmek suretiyle kapatılırken(örneğin normal kapatma işlemi yapılması durumunda, bilgisayarın kayıt defteri veri tabanında adli bilişim açısından önem arz eden pagefile.sys dosyası bilgisayar her kapandığında içeriğindeki bilgileri temizle komutu aktif halde ise içerisindeki bilgiler silinir, bunun önüne geçmek amacıyla bilgisayarın güç kaynağının fişini çekme işlemi yapılır.), Windows sunucuları, Linux ve Macintosh bilgisayarlar normal kapatma işlemi (Bilgisayarı kapat-Shutdown) uygulanarak kapatılmalıdır. Sistem veri tabanının zarar görmesini

önlemek maksadıyla dizüstü bilgisayarlar kapatılırken, işletim sistemine bağlı olarak aynı yöntemler uygulanmakla birlikte, bataryanın da çıkarılması gerekmektedir.

✓ Olay yerinde internet sağlayıcı olarak açık vaziyette bir modem bulunuyorsa, modemin elektrik bağlantısı kesilmeden üzerinde bulunan uçucu veriler toplanmalıdır.

✓ Kapalı konumda bulunan bilgisayarın diski bağlantılarından sökülerek birebir kopyasının alınması işlemi yapılırken, tek yönlü yazma işlemi yapabilen birebir kopyalama cihazı ile kullanma talimatına göre hareket edilerek hedef diske birebir kopya alınmalıdır.

✓ Veri depolama ünitelerine ait alınan birebir kopyaların kapasitesi, hatalı sektörleri ile MD5 ve SHA hash değerlerini kapsayacak şekilde birebir kopya alma tutanağı tanzim edilmelidir. Tanzim edilen tutanağa birebir kopyalama cihazı tarafından üretilen log kayıtları da eklenmelidir.

✓ Sabit diskin birebir kopyası CMK. 134. maddesi gereği iki kopya olarak alınır. Alınan kopyalardan birine incelenmek üzere el konulur, diğerine ise şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınmalıdır.

✓ Birebir kopyası alınacak sabit diskin Solid State Disk olması durumunda bu disklerin üretilme teknolojileri gereği her alınan birebir kopyada farklı MD5 ve SHA hash değerleri üretme ihtimalinin bulunabilmesinden (Wear Levelling) dolayı diskin aynı anda iki ayrı birebir kopya oluşturabilen (Tableau TD2u gibi) donanımlarla kopyasının alınması gerekmekte böyle bir imkânın bulunmaması durumunda ise sabit diskin kopyası alındıktan sonra alınan birebir kopya başka bir diske kopyalanmak suretiyle şüpheliye veya vekiline verilmek suretiyle Solid State Diskin farklı hash değeri üretmesi ihtimali ortadan kaldırılmış olur ve bu husus tutanağa geçirilerek imza altına alınmalıdır.

✓ Güvenlik kamera kayıt cihazları üzerinde inceleme yapılması durumunda öncelikli olarak güvenlik kamera kayıt cihazının, diskleri ve kurulum CD'leri ile birlikte laboratuvara gönderilmesi gerekmektedir. Bunun mümkün olmadığı durumlarda kayıt cihazının içerisinde bulunan disk/diskler ile birlikte, cihazın marka model bilgileri, cihazın tarih saat dilimi ve tarih/saat ayarları tespit edilerek incelenmek üzere gönderilmesi gerekmektedir.

✓ Olay yerinde, açık vaziyette bulunan cep telefonları öncelikli olarak bataryası çıkarılmak suretiyle kapatılmalı, cep telefonunun bataryasının çıkarılamaması durumunda açma-kapama düğmesine basılarak kapatılmalı, kapalı olan cep telefonları açılmamalıdır.

✓ Olay yerinde sıvı içerisinde bulunan bulgular dışarı çıkarıldığında hava ile temas ederek oksitlenmesi ihtimaline karşı içerisinde bulunduğu su ile birlikte gönderilmelidir.

✓ Cep telefonları, kullanım sırasında üzerinde takılı olan SIM karttan farklı bir SIM kart takılarak açıldığında belleğinde bulunan arama kayıtları silinebilmektedir. Bu nedenle özellikle çift sim kart özelliğine sahip cep telefonları içerisinde tespit edilen SIM kartlarının hangi yuvadan çıkarıldığı kesinlikle belirtilir. Çıkarılan SIM kartlar bilgilerinin tespitinden sonra çıkarıldıkları yuvalara takılarak gönderilmelidir.

✓ El konulan bulgular kesinlikle kullanılmamalıdır (Cep telefonu ile arama yapılmamalı, bilgisayar vb. açılmamalı).

✓ İncelenmek üzere gönderilecek delillerin şifrelerinin (SIM kart PIN kodu, cep telefonu güvenlik kilidi, TrueCrypt, BitLocker şifresi vb.) mümkün olması durumunda tespit edilerek inceleme talep yazısında belirtilmelidir.

1.8.2.3. Delilerin Muhafazası

✓ Birden fazla bilgisayara el konulması halinde, sistem bütünlüğünün bozulmamasına ve etiketlendirmeye özen gösterilmelidir. Her bilgisayar sisteminin sahip olduğu yardımcı donanım birimleri(klavye, fare vb.), kendi grubu içinde (örneğin sabit disk, CD/DVD, USB bellek vb.) etiketlendirilmelidir (Henkoğlu, 2014 s.:25).

✓ CD/DVD ve yedekleme ünitelerinde kullanılan kasetlerin hassas veri depolama birimleri oldukları unutulmamalı, bu veri depolama birimlerinin çizilmemesi, bükülmemesi, kırılmaması ve manyetik ortamlara girmemesi için özen gösterilir (Henkoğlu, 2014 s.:25).

✓ Delillerin taşınma işlemleri uygun şekillerde yapılmalıdır. Dijital delillerin statik elektrik ve bazı cihazların oluşturduğu manyetik alanlardan zarar görme riski yüksek olmasından dolayı paketlenmesinde anti statik poşetler kullanılmalıdır (Henkoğlu, 2014 s.:25).

✓ Muhafaza altına alınan bilgisayarlar kesinlikle açılmamalı ve kuru, tozsuz ortamlarda muhafaza edilmeli; sabit disk, disket, USB bellek, CD/DVD vb. medyalar üzerinde herhangi bir işlem yapılmamalıdır.

1.8.2.4.Delillerin Laboratuvara Gönderilmesi

✓ Deliller laboratuvara deliller gönderilirken inceleme istemi yazısı, Cumhuriyet Savcısının onayı veya ilgili mahkemenin karar yazısı ile birlikte gönderilmelidir.

✓ Dıştaki paket üzerine "DİKKAT, ELEKTRONİK MALZEME" ve "MIKNATIS veya MANYETİK ALANLARDAN UZAK TUTUNUZ" uyarıları yazılmalıdır.

✓ Kasalar dik duracak şekilde paketlenerek gönderilmelidir. Dıştaki paketin üzerine "BURASI YUKARI GELECEK ŞEKİLDE TAŞIYINIZ" ifadesi yazılmalıdır.

✓ Bulgular ambalajlanırken manyetik alanlardan ve dış darbelerden korunacak şekilde rutubete maruz kalmayacak şekilde ambalajlanmalıdır (JKDB, 2011 s: 161).

✓ Bilgisayar kasası ve harici veri saklama medyaları gönderilirken mukavva, dayanıklı kartondan yapılmış bir kutu ya da koli kullanılmalıdır. Mümkünse parçaların kendilerine uygun olarak üretilmiş orijinal paketleri kullanılmalıdır. Ambalajlama malzemesi olarak iri plastik kabarcıklı paketleme materyali ya da sünger petler kullanılır.

✓ Bulgular birbirine temas etmeyecek şekilde ayrı ayrı ambalajlanmalı, CD ve DVD gibi nesnelerin veri yazılan yüzeylerinin deformasyona uğramaması için gerekli tedbirler alınmalıdır (JKDB, 2011 s: 161).

- ✓ Dijital deliller anti-statik torbalarda muhafaza edilerek gönderilmelidir.

- ✓ Bulguların, özellikle sabit disklerin izole edilmemiş kısımlarına çıplak elle dokunulmamalıdır (Elektronik devre kartı elemanları vb.).

- ✓ Üzerinde veri tutabilen tüm materyaller gönderilmelidir (sabit disk, USB bellek, cep telefonu, hafıza kartı, SIM kartlar, yazıcı vb.).

- ✓ Masaüstü bilgisayar kasaları ile sabit diskler dışındaki; gönderilen diğer bulgulara ait bataryalar ve şarj cihazları ile bağlantı kabloları gönderilmelidir.

- ✓ Gönderilen bulgu ve delillerin varsa programları ile birlikte gönderilmelidir (Örneğin kalem ses kayıt cihazının incelenmek üzere gönderilmesi durumunda varsa kurulum CD/DVD'si ile birlikte gönderilmelidir.).

- ✓ Bilgisayar kasası ve kamera kayıt cihazının içerisindeki diskler ile birlikte gönderilmesi durumunda içerisinde bulunan sabit diskler hareket etmeyecek şekilde sabitlenmiş olması gerekmektedir. Aksi halde bulgu veya delillerin nakli sırasında kasa içerisindeki sabit diskler hareket ettiğinden dolayı hasar görebilmektedir.

✓ Olay yerinde sıvıya maruz kalmış olan elektronik cihazlar varsa güç bağlantısı sökülmeli/çıkarılmalıdır. Deliller oda sıcaklığında kurutularak gönderilmelidir (Örneğin ıslak halde bulunan cep telefonunun bataryasının çıkarılması gibi).

✓ Birebir kopya alınma ihtimali yoksa, bilgisayar kasası göndermek yerine imkanlar dahilinde bu kasalarda bağlantılı vaziyette bulunan sabit diskler sökülerek gönderilmeli ve bu hususlar kayıtlarda açıkça belirtilmelidir (JKDB, 2011 s: 161).

✓ Masaüstü ve dizüstü bilgisayarlara el konulduğunda sabit diskinin bulunup bulunmadığı kontrol edilmelidir (JKDB, 2011 s: 161).

✓ İnceleme istek formlarında gönderilen bulguların kime ait olduğu ile özellikleri belirtilmeli, ambalajlanan bulguların üzerine "Gönderilen Deliller" bölümündeki sıra numarası yazılmalıdır (JKDB, 2011 s: 161).

✓ İnceleme istek formunda olayın konusu, tarihi ve olayla ilgili isimler, gönderilen bulgu ve deliller üzerinde anahtar kelime olarak aratıldığından dolayı açık olarak belirtilmelidir (Örneğin tehdit olayında tehdit ettiği metnin açık olarak belirtilmesi).

✓ Bulgu olay yerinden toplandıktan sonra içeriğine erişilmeden laboratuvara gönderilmelidir. Adli makamların talimatı ile delilin içeriğine erişilmesi gerektiğinde durum tutanakla belirlenmelidir.

✓ Olay yerinden elde edilen bulgu ve deliller arızalı halde bulunsa dahi durum tutanakta belirtilerek laboratuvara gönderilmelidir.

✓ Cep telefonu ve mobil cihazlar içerisine takılı vaziyette bulunan SIM kart, hafıza kartı ve bataryaları takılı vaziyette gönderilmelidir.

1.8.3. Deliller Üzerinde Gerekli İnceleme ve Analiz Faaliyetleri Aşaması

✓ İncelenmek üzere gönderilen deliller açılmadan önce delilin paketlemesi/ambalajlaması üzerinde bir hasar (açılma/yırtık/ezik vs.) olup olmadığı kontrol edilmelidir.

✓ Delille ilgili olarak gönderilen evrak kontol edilmeli, evrakın ilgili kuruma ve yetkili kişinin imzasıyla gönderildiği kontrol edilmelidir.

✓ Delil açma işlemleri heyet huzurunda yapılmalı ve yapılan işlemler kamera/fotoğraf makinesi gibi cihazlarla kayıt altına alınmalıdır.

✓ Açma işlemi esnasında delilin tanımlayıcı bilgileri (Seri numarası/IMEI numarası/Barkod numarası/üzerindeki tanımlama bilgileri vs.) belirtilmelidir. Ayrıca delilin üzerinde bir hasar mevcut ise bu durum ayrıntılı bir şeklide kayda geçirilmelidir (kırık, ezik, çizik vs).

✓ Delilin açma ve tanımlama işlemi yapıldıktan sonra ilgili evrakta belirtlien delil ile aynı olup olmadığı kontrol edilmelidir. Farklılık tespit edilmesi durumunda durum açma tutanağında belirtilmeli ve talep makamı ile irtibata geçilmek suretiyle hatanın resmi yazı ile düzeltilmesi talep edilmelidir. Düzeltme talebinin yerine getirilmemesi durumunda delil inceleme aşamasına geçilmeden iade edilmelidir.

✓ Delilin kabul işlemi gerçekleştikten sonra inceleme aşamasına geçilmelidir. İnceleme aşaması mevzuatımıza göre (CMK Madde 66) delilin kabul tarihinden itibaren 3 aylık bir süreyi kapsamaktadır. İncelemenin tamamlanamaması durumunda süre bir defaya mahsus olmak üzere 3 ay daha uzatılabilir. İncelemenin bu süre içerisinde tamamlanamaması durumunda, bilirkişi değiştirilebilir. Bilirkişi, incelemenin sona ermesinin sebeplerini belirten bir rapor hazırlar ve delilleri ile birlikte ilgili makama iade eder.

✓ İnceleme/analiz faaliyetleri talep edilen inceleme isteği doğruldusunda yapılır.

1.8.4 İnceleme Sonucu Raporlama ve Delillerin İadesi Aşaması

✓ "Adli bilişim incelemesinin son aşaması sunumdur. Tespit edilen ve değerlendirmesi yapılmış olan veriler, talep eden makama sunulmak üzere anlaşılabilir bir dilde raporlanır." (Brown, 2010).

✓ Adlî makamlara sunulan raporlarda teknik bilgilere çok fazla yer verilmemelidir. Zorunlu olarak yer verilen teknik bilgiler açıklayıcı bir biçimde sunulmalıdır. Sunulan rapor ayrıntılı ve anlaşılabilir olmalıdır. Raporlamada aşağıdaki hususlara dikkat edilmelidir (JKDB, 2011 s: 172).

✓ Raporun dili ve içeriği teknik bilgisi olmayan insanlar tarafından bile anlaşılabilir olmalıdır (JKDB, 2011 s: 172).

✓ İnceleme isteğinde talep edilen hususlar inceleme konusu olmalı, ancak inceleme isteğinde belirtilmeyen bir konuda tespitte bulunulması durumunda inceleme isteğini yapan makamla derhal irtibata geçilerek, gelişen durum hakkında bilgi verilmelidir. Örneğin, tarihi eser kaçakçılığı ile ilgili resim dosyalarının tespit edilmesine yönelik yapılan inceleme esnasında çocuk pornografisi suçu olabilecek dosyaların tespit edilmesi durumunda derhal inceleme isteğinde bulunan makamla irtibata geçilmeli ve gerekirse yeni gelişen durumla ilgili yeni bir inceleme isteğinde bulunulması konusunda bilgi verilmelidir (JKDB, 2011 s: 172).

✓ Teknik terimler olduğunca az kullanılmalı, kullanılanlar ise detaylı şekilde açıklanmalıdır (JKDB, 2011 s: 172).

✓ Raporda, incelenen delillerin hangi adli bilişim metotları ile incelendiği, delillerin cinsleri ve özellikleri (markası, modeli, seri numarası, toplam kapasitesi, algoritma ve doğrulanmış algoritma imzaları varsa kullanıcı isimleri vb.) mutlaka belirtilmelidir (JKDB, 2011 s: 172).

✓ İnceleme başlangıcı algoritma imzası ile inceleme sonrası algoritma imzalarının birbirleri ile aynı olduklarının dolayısıyla delil üzerinde herhangi bir değişiklik meydana gelmediğinin raporda belirtilmesi gerekmektedir. Algoritma imzasının, bilimsel açıdan kesinlik ifade edebilmesi için MD5 ve SHA-1 veya SHA-256 türünde belirtilmesi gereklidir (JKDB, 2011 s: 172).

✓ Eğer incelenmek üzere, olay yerinde alınan bir **birebir** kopya gönderilmesi halinde, olay yerinde kopyalama esnasında alınan algoritma imzası ile kopyanın laboratuvara geldiği haliyle alınan algoritma imzası karşılaştırılmalıdır. Bunun nedeni, olay yeri incelemesi esnasında alınan kopya ile incelenen kopyanın aynı delile ait olduğunun ortaya konulması gerekliliğidir (JKDB, 2011 s: 172).

✓ Delile ait üzerinde inceleme yapılan birebir kopya, gerektiğinde tekrar inceleme yapılabilmesi maksadıyla rapor ile birlikte talep makamına gönderilmelidir. Bu kapsamda adli bilişim yazılım ve donanımları kullanılarak alınan birebir kopyaların herhangi bir bilgisayarda açılamayacağı ancak yine adli bilişim yazılım ve donanımları ile açılabileceği belirtilmelidir (JKDB, 2011 s: 172).

✓ Delillerin iadesi aşaması genellikle göz ardı edilen ve önemsenmeyen bir aşama olarak düşünülmektedir. Deliller üzerinde bilirkişi incelemesi yapıldıktan sonra inceleme sonuçları talep makamına deliller ile birlikte iade edilmektedir. Delilleri ve inceleme sonuçlarını teslim alan makamlar belirli bir süre sonra inceleme sonuçlarının bulunduğu sabit/taşınabilir diskin içeriğine erişemediğini beyan etmektedirler (iade edilen delillerin ve inceleme sonuçlarının iade sürecinde ve sonrasında hasar görmesi nedeniyle).

✓ İncelemesi biten bir delil sanki bir daha incelenmeyecekmiş gibi düşünülüp önemini yitirmektedir. Fakat delilin bir inceleme sürecinde delilin iadesi son aşamayı oluşturmakta iken, yeni başlayacak olan bir inceleme sürecinin de ilk aşamasını oluşturmaktadır. Bu nedenle düzenlenen uzmanlık raporu ile birlikte iade edilen deliller, aynı deliller laboratuvara gönderiliyormuş gibi davranılmalı ve o aşamada dikkat edilmesi gereken hususlara bu aşamada da riayet edilmelidir.

✓ Bu kapsamda, bu tezin yapılmasındaki amaç her geçen gün daha da zorlu bir hal alan adli bilişim incelemelerini standartlaştırmak ve süreç içerisinde eksik kalan bir hususun olmaması adına kapsamlı bir Adli Bilişim İnceleme Süreci tasarlanmasıdır.

2. GEREÇ VE YÖNTEM

2.1. Gereçler

2.1.1. İncelemede Kullanılan Donanım ve Yazılımlar

✓ İnceleme Bilgisayarı (Tüm inceleme faaliyetlerinin yapıldığı bilgisayar)

✓ Tableu TD2u birebir kopya (İmaj) alma donanımı (Sabit diskin birebir kopyasının alınmasında kullanılan)

✓ 2 adet, birebir kopyanın alındığı sabit disk (Şüpheli sabit diskin birebir kopyalarının alındığı sabit diskler)

✓ Mobiledit Forensic Express Mobil Adli Bilişim Yazılımı (Cep telefonunun kopyasının alınmasında ve incelemesinin yapılmasında kullanılan)

✓ Encase Forensic Adli Bilişim Yazılımı (Sabit diskin incelemesinde kullanılan)

✓ Exiftool 9.74 Yazılımı (Fotoğraf ve Video dosyalarının EXIF bilgilerinin incelenmesinde kullanılan)

✓ Photorec 7.1 Yazılımı (Sabit Disk içerisinden dosya kurtarma işlemi için kullanılan)

✓ EMFSpoolViewer.exe Yazılımı (Sabit Disk içerisinde bulunan spool dosyalarını incelemek için kullanılan)

✓ Reg ripper v2.8 Yazılımı (Sabit Disk içerisinde bulunan kayıt defteri veri tabanı dosyalaını incelemek için kullanılan)

2.1.2. İncelemede Kullanılan Araç ve Gereçler

✓ Acer Marka Dizüstü Bilgisayar ve bilgisayara takılı vaziyette sabit disk (Windows 7 İşletim Sistemine Sahip) (Delil olarak kullanılan)

✓ Sony Marka Cep Telefonu (Android İşletim Sistemine Sahip) (Delil olarak kullanılan)

✓ Turk Telekom Marka SIM Kart. (Delil olarak kullanılan)

✓ Canon marka Yazıcı (Delil olarak kullanılan)

✓ DVD+R (Delil olarak kullanılan)

✓ Nikon marka Dijital Fotoğraf Makinesi (Olay yeri fotoğraf çekimi işlemleri için kullanılan)

✓ Numaratör 1-2-3 (Olay yerinde bulunan delillerin tespiti için kullanılan)

✓ Delil Muhafaza Kabı/Köpük (Olay yerinde bulunan delillerin ambalajlanması için kullanılan)

2.2. Yöntem

Çalışma iki bölümden oluşmaktadır. İlk bölümde yurt dışı ve yurt içinde tasarlanan adli bilişim inceleme süreçleri analiz edilmiş ve Türk Hukuk sistemine uygun yeni bir adli bilişim inceleme süreci tasarlanmıştır. İkinci bölümde ise tasarlanan adli bilişim inceleme süreçinin tüm aşamalarını gösterecek bir örnek olay tasarlanmıştır. Tasarlanan örnek olay içerisinde adli bilişim incelemelerinde sıkça karşılaşılan delil türlerinden **bilgisayar**(Windows 7 işletim sistemine sahip sabit diski mevcut), **cep telefonu** (Android işletim sistemine sahip) ve **SIM kart**, **yazıcı** ve **DVD+R** üzerinde incelemeler yapılmak suretiyle içerisinden elde edilebilecek veri türlerinin çeşitleri ortaya konulmuştur. İncelemeler sonucunda adli bilişim delilin ilk müdahale aşamasından, kriminal laboratuvarda incelemesinin tamamlanmasına müteakip iade aşamasına kadar ki sürecin ayrıntılı bir şekilde planlanması yapılmıştır.

3. BULGULAR

3.1. Tasarlanan Adli Bilişim İnceleme Sürecinin Örnek Olay Üzerinden Gösterilmesi ve Tespitler

ÖRNEK OLAY (KASTEN YARALAMA VE TEHDİT SUÇU)

23.12.2017 günü saat 12.30 sıralarında Ankara İli, Gölbaşı İlçesi, Taşpınar Köyü girişinde Şüpheli H.U.S. alacak verecek meselesi yüzünden mağdur M.E.'nin üzerindeki kıyafetleri çıkararak mağdura şiddet uyguluyor ve olay anını cep telefonu ile fotoğraf ve video çekimi yaptırtıyor (Temsili olarak uygulanması).

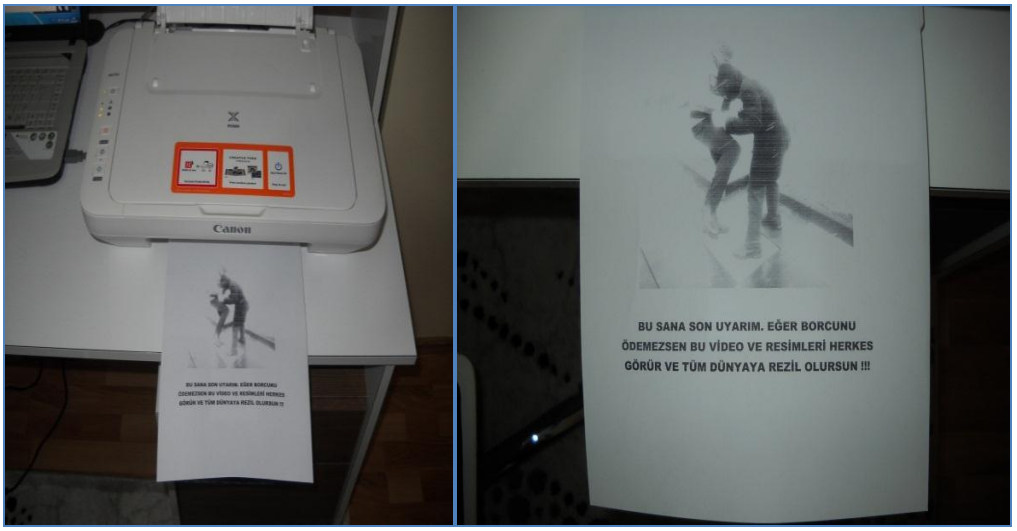
Şekil 3.1. Olay Anında Çekilen Fotoğraf Kaydı.

Şekil 3.2. Olay Anında Çekilen Video Kaydı.

24.12.2017 tarihinde şüpheli H.U.S. kendi cep telefonu ile çektirmiş olduğu video ve resim dosyalarını evinde bulunan bilgisayara kopyaladı.

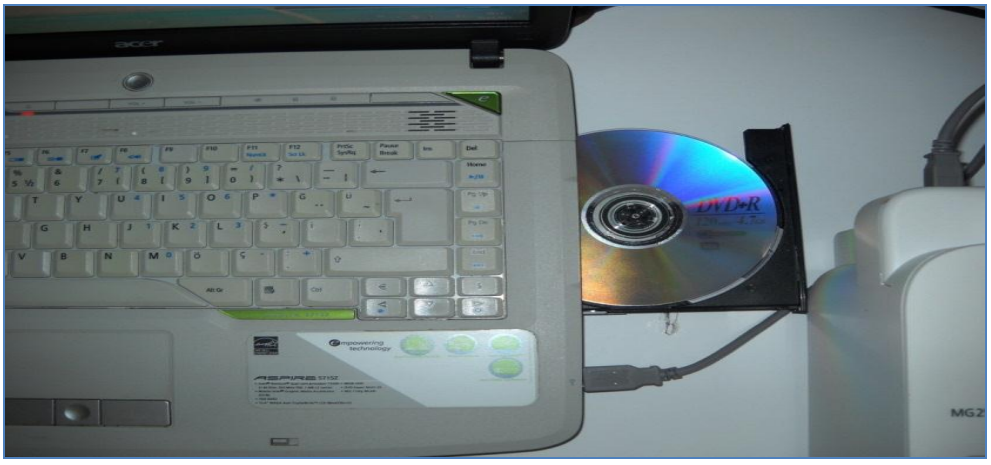
Şekil 3.3. Cep Telefonundan Yapılan Kopyalama İşlemi.

Şüpheli H.U.S. bilgisayar üzerinde bir Microsoft Word Belgesine çekmiş olduğu resmi ekledi ve altına "**BU SANA SON UYARIM. EĞER BORCUNU ÖDEMEZSEN BU VİDEO VE RESİMLERİ HERKES GÖRÜR VE TÜM DÜNYAYA REZİL OLURSUN !!!"** mesajını yazmak suretiyle bilgisayara bağlı bulunan yazıcıdan çıktı aldı. *(Yazıcının yazdırılan belgeleri tut ayarı açık vaziyette)*



Şekil 3.4. Tehdit Metninin Yazıcıdan Çıktı Alınması.

Ayrıca olay anında çekilen videoyu da bilgisayarından DVD'ye yazdırdı ve DVD'yi yazıcı çıktısı ile birlikte M.E'ye tehdit amacıyla gönderdi.



Şekil 3.5. Tehdit İçerikli Videonun DVD+R'ye yazdırılması.

DVD ve yazıcı çıktısı eline geçen Mağdur M.E., şüpheli H.U.S. hakkında kolluk kuvvetlerine suç duyurusunda bulundu.

ADLİ BİLİŞİM İNCELEME SÜRECİ

Birinci bölümde belirttilen ve 4 aşamadan oluşan adli bilişim inceleme sürecinin uygulanabilirliği, tasarlanan örnek olay içerisinde tüm aşamalarını kapsayacak şekilde gösterilmiştir.

Çizelge 2.1. Adli Bilişim İnceleme Süreci.

S.No	Aşamalar
1	Hazırlık Aşaması
2	Delillerin Tespit Edilmesi, Toplanması, Muhafazası ve Laboratuvara Gönderilmesi Aşaması
3	Deliller Üzerinde Gerekli İnceleme ve Analiz Faaliyetleri Aşaması
4	İnceleme Sonucu Raporlama ve Delillerin İadesi Aşaması

1- Hazırlık Aşaması

İhbarı alan kolluk kuvvetlerine bağlı Adli Kolluk Görevlileri durumu Gölbaşı Cumhuriyet Başsavcılığına bildirdi. Gölbaşı Cumhuriyet Savcılığının talebi üzerine 26.12.2017 günü Gölbaşı Sulh Ceza Hakimliği şüphelinin evinde ve üzerinde 1 defaya mahsus arama yapılmasına ve suç unsurlarına el konulmasına karar verdi. (CMK md.119) (Hukuki hazırlık)

Kararda ayrıca el konulan deliller üzerinde;

✓ Darp anını gösterir videonun ve tehdit metninin (BU SANA SON UYARIM. EĞER BORCUNU ÖDEMEZSEN BU VİDEO VE RESİMLERİ HERKES GÖRÜR VE TÜM DÜNYAYA REZİL OLURSUN !!!) bulunup bulunmadığı,

✓ Dosya ve kayıtlar silinmiş ise gerekli kurtarma işlemlerinin yapılması,

✓ Videonun oluşturulduğu konuma ait bilgilerin tespit edilmesi talebinde bulunuldu.

Ayrıca kolluk kuvvetlerine bağlı Olay Yeri İnceleme Ekipleri (Ekip bünyesinde konunun uzmanı personel de bulunmaktadır.), olay yerinde bulunan sayısal delillerin kopyasını almak amacıyla TD2u birebir kopyalama cihazı, canlı inceleme yazılımları ve birebir kopyaların alınabileceği sabit diskler temin etti (Teknik hazırlık).

2- Delillerin Tespit Edilmesi, Toplanması, Muhafazası ve Laboratuvara Gönderilmesi Aşaması

İlgili mahkeme tarafından verilen arama ve el koyma kararına istinaden kolluk kuvvetlerine tarafından 26.12.2017 günü saat:14.00'de şüpheli H.U.S.'un Gölbaşı ilçesinde bulunan evinde arama yaptı. Arama ve el koyma faaliyetleri esnasında fotoğraf çekimi, kroki çizimi ve not tutulması işlemleri de genel olay yeri inceleme safhalarına göre yapıldı.

a. Delillerin Tespit Edilmesi

Şüpheli H.U.S.'un evinde yapılan aramada, çocuk odasında çalışma masası üzerinde Acer marka dizüstü bilgisayar **(Delil-1)** ile bilgisayara takılı vaziyette Canon marka yazıcı **(Delil-2)** tespit edildi.

Şekil 3.6. Çocuk Odasında Bulunan Dizüstü Bilgisayar **(Delil-1)**.

Şekil 3.7. Çocuk Odasında Bulunan Yazıcı **(Delil-2)**.

Şekil 3.8. Delillerin Genel Görünümü.

Şekil 3.9. Delillerin Genel Görünümü.

Ayrıca mutfak bölümünde girişte sol tarafta bulunan beyaz renkli çekmeceli dolap üzerinde şarja takılı vaziyette 1 adet Sony marka cep telefonu **(Delil-3)** tespit edildi. Cep telefonunun açık vaziyette olduğu üzerinde güvenlik kilidinin bulunduğu tespit edildi. Şüpheliden güvenlik kilidinin **"1>4>7>8>9"** olduğu öğrenildi.

Şekil 3.10. Mutfakta Bulunan Cep Telefonu **(Delil-3)**.

b. Toplanması, Muhafazası ve Laboratuvara Gönderilmesi Aşaması

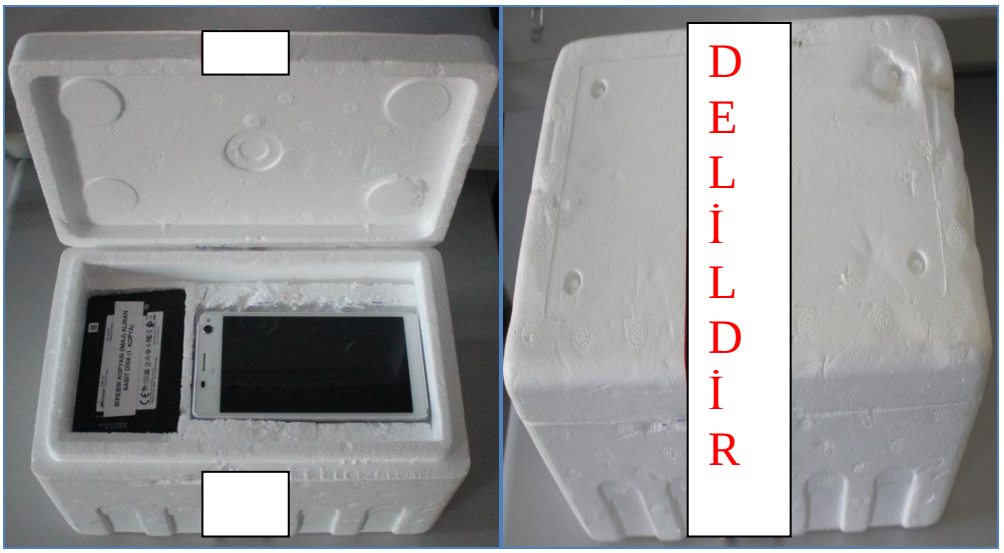
Şüphelinin evinde ele geçirilen Acer marka dizüstü bilgisayara takılı vaziyette bulunan sabit diskinin birebir kopyası Olay Yeri İnceleme Uzmanları tarafından 2 suret olarak alındı. Alınan birebir kopyanın 1 sureti şüpheli şahsa, 1 sureti ise incelenmek üzere teslim alındı. **(CMK md.134).** Birebir kopya alma işlemi tamamlandıktan sonra alınan kopyaya ait MD5 ve SHA1 HASH (Verilerin bütünlüğünü kontrol etmek için kullanılan tek yönlü özetleme algoritması- Çakır, 2014 s.:148) değerlerini belirten Birebir Kopya Alma Tutanağı tanzim edildi.

Şekil 3.11. TD2u Donanımı İle Birebir Kopya (İmaj) Alma İşlemi.

Şüpheli H.U.S.'nin evinde ele geçirilen cep telefonu ile dizüstü bilgisayarın yanında bulunan yazıcının kopyası alınamadığı için el konuldu.

Olay yerinden ele geçirilen deliller gerekli incelemelerin yapılabilmesi amacıyla usulüne uygun olarak paketlendi.

Şekil 3.12. Cep Telefonu ve Sabit Diskin Ambalajlanması.



Şekil 3.13. Cep Telefonu ve Sabit Diskin Ambalajlanması.

Şekil 3.14. Yazıcının Ambalajlanması.

Şüphelinin evinden ele geçirilen;

✓ İçerisinde Acer marka bilgisayara takılı vaziyette bulunan FUJITSU marka, MHW2120BH model, **"NZ1DT732C1FS"** seri numaralı 120 GB sabit diskin birebir kopyasının bulunduğu Samsung marka, SM500DM002 model, **"5452145AB"** seri numaralı sabit disk,

✓ 1 adet Canon marka, PIXMA MG2550 model,**"ASLX52X"** seri numaralı yazıcı,

✓ 1 adet Sony marka, C4 (E5303)model, "**35219407034xxxx**" IMEI numaralı cep telefonu ve Turk Telekom marka, "**899028603943263xxxx**" seri numaralı SIM kart,

ile şüpheli tarafından mağdura gönderildiği bildirilen;

✓ 1 adet Sony marka, **"asl123sacd12"** seri numaralı DVD+R,

✓ 1 adet yazıcı çıktısı.

üzerinde gerekli incelemelerin yapılabilmesi amacıyla uygun şekilde paketlendikten sonra ilgili yazı ile birlikte çuval içerisine konulup mühürleme işlemi yapıldıktan sonra kurye vasıtasıyla Kriminal Laboratuvara gönderildi.

3- Deliller Üzerinde Gerekli İnceleme ve Analiz Faaliyetleri Aşaması

Kriminal Laboratuvarca teslim alınan deliller üzerinde;

1- Talep yazısının kendilerine hitaben ve imzalı olup olmadığı kontrol edildi.

2- Talep yazısında bahsedilen deliler ile gönderilen delillerin aynı olup olmadığı kontrol edildi (eksiklik veya fazlalığın tespit edilmesi durumunda talep makamı ile irtibata geçilerek durum bildirilir ve resmi bir yazı ile sorunun düzeltilmesi talep edilir.).

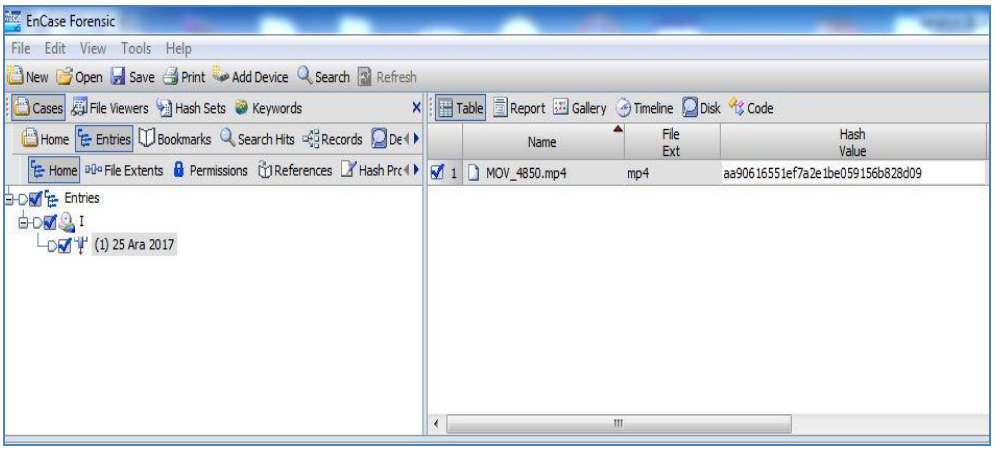
3- Talep yazısında bahsedilen deliller ile gönderilen delillerin aynı olduğunun anlaşılması durumunda deliller üzerinde herhangi bir hasar, kusur ve eksikliğin bulunup bulunmadığı kontrol edildi.

4- Yapılan tüm işlemler kamera sistemi ile kayıt altında olan delil açma odalarında yapıldı.

5- Tüm bu işlemler sorunsuz bir şekilde yapıldıktan sonra deliller üzerinde talep edilen incelemeler gerçekleştirildi.

DVD+R'nin üzerinde yapılan inceleme;

Sony marka, **"asl123sacd12"** seri numaralı DVD+R'nin yapılan incelemesinde; içerisinde 1 adet **"MOV_4850.mp4"** isimli video dosyasının bulunduğu tespit edilmiştir.

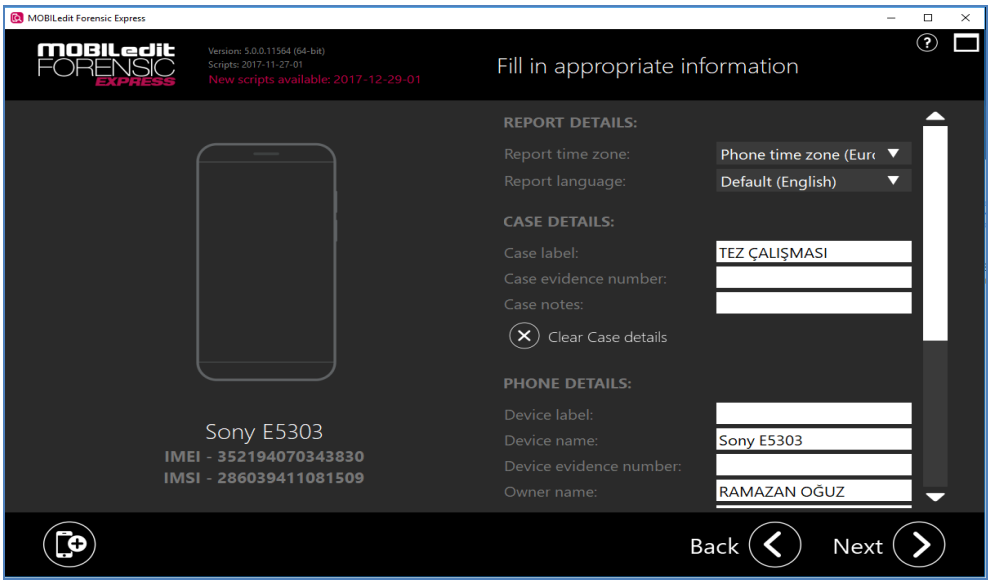


Şekil 3.15. DVD+R'nin İçeriğindeki Video Dosyası.

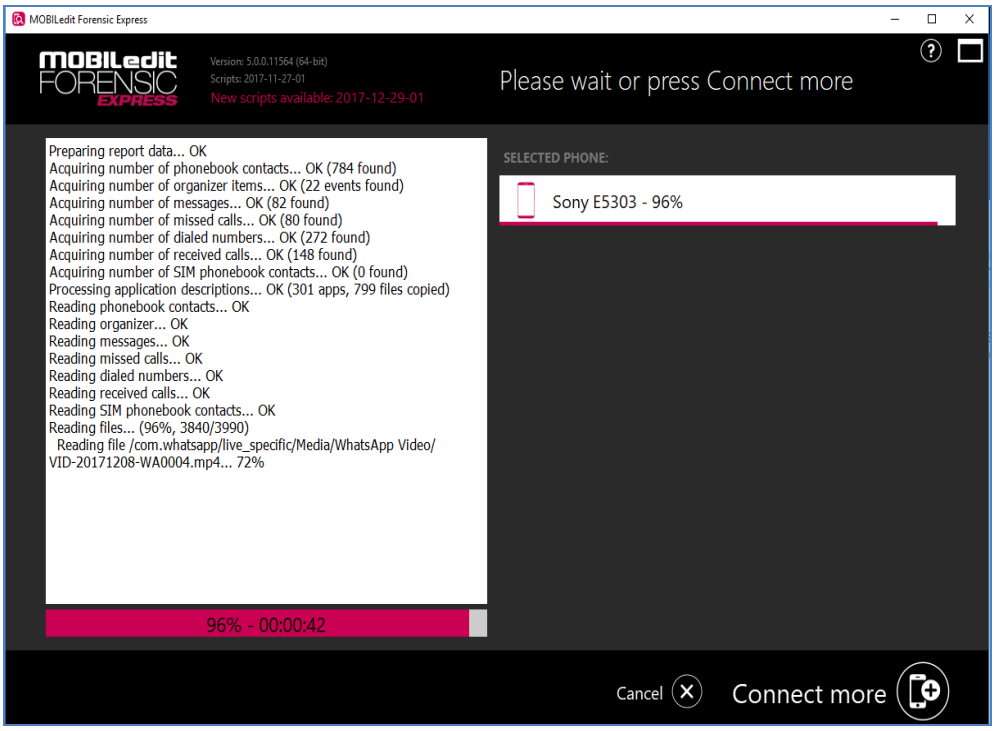
Cep Telefonu üzerinde yapılan İnceleme;

Sony marka, C4 (E5303) model, “35219407034xxxx” IMEI numaralı cep telefonunun kopyası **Mobiledit FORENSIC EXPRESS** mobil adli bilişim yazılımı ile alındı (Bu model için Fiziksel kopya alma desteği bulunmadığı için cep telefonunun silinmiş alanlarındaki verilere kısmen ulaşılmıştır).

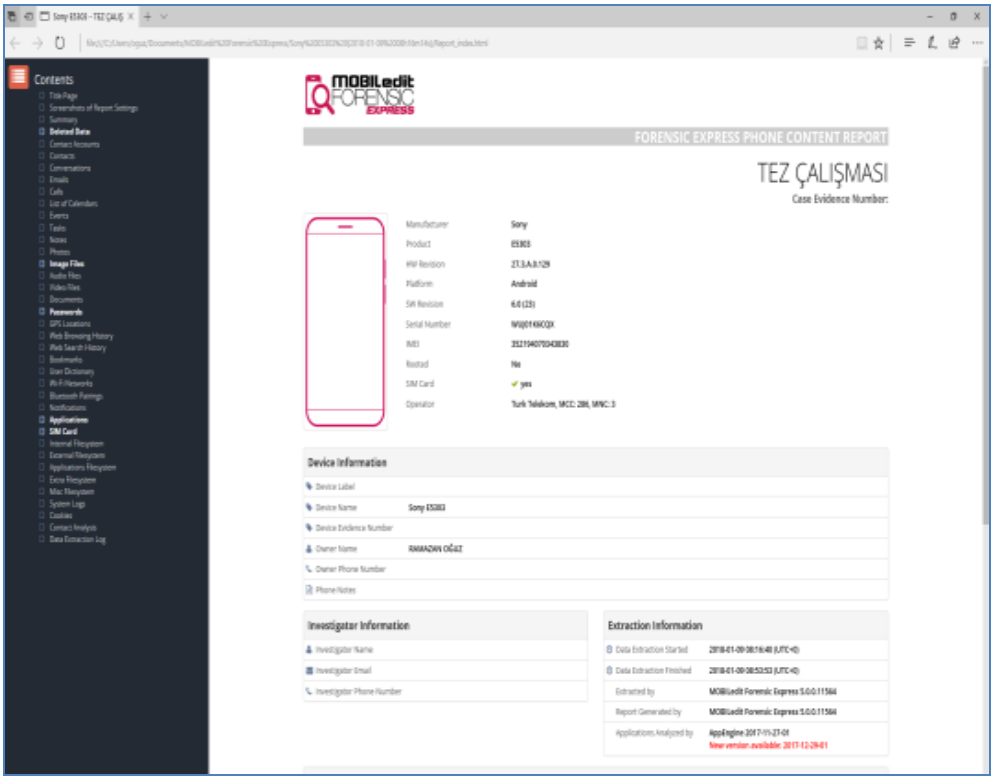
Şekil 3.16. Cep Telefonunun Kopyasının Alınması**.**



Şekil 3.17. Cep Telefonunun Kopyasının Alınması.

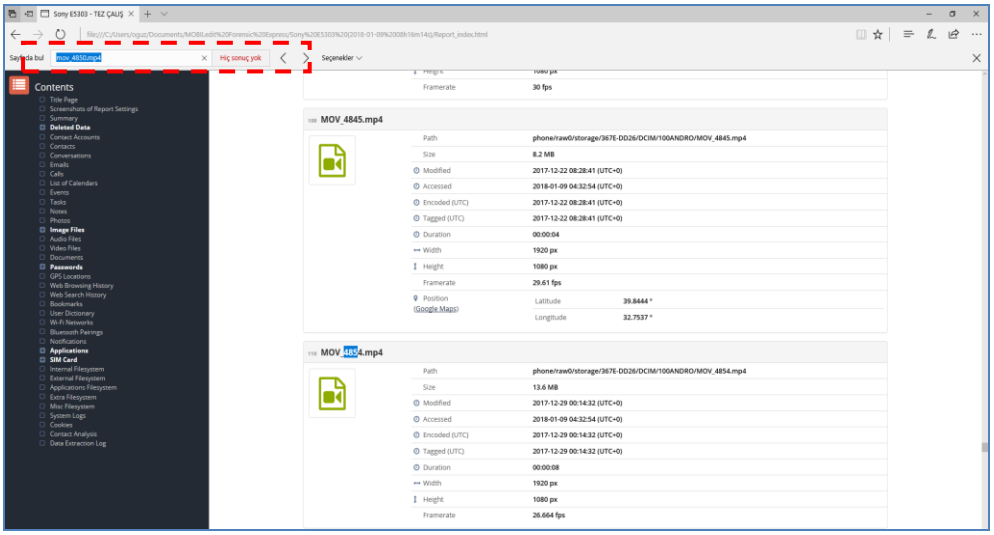


Şekil 3.18. Cep Telefonunun Kopyasının Alınması.



Şekil 3.19. Cep Telefonunun İçeriğinin Raporlanması.

Alınan kopyanın içeriğinde yapılan incelemede; DVD+R içerisinde bulunan **“MOV_4850.mp4”** isimli video dosyasının bulunmadığı tespit edildi. Ayrıca cep telefonunun kopyasının içeriğinde tehdit içerikli belgedeki resim ve tehdit metni de tespit edilemedi (Şüpheli H.U.S. daha sonraki beyanlarında olayla ilgili kayıtları bilgisayara kaydettikten sonra cep telefonundan sildiğini beyan etmiştir.).



Şekil 3.20. Cep Telefonunun İçeriğinde Suç Konusu Video Dosyasının Kaydının Tespit Edilememesi.

SIM kart üzerinde yapılan inceleme;

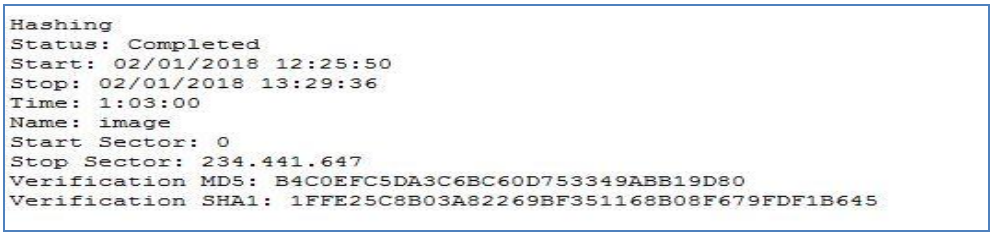
Turk Telekom marka, “899028603943263xxxx” seri numaralı SIM kart üzerinde; arama kaydı, rehber bilgisi, kısa mesaj(SMS) ve SIM kart bilgisi haricinde veri bulunmadığından dolayı, içeriğinde suç konusu olarak belirtilen video dosyası, resim dosyası ve tehdit metnine ulaşılamadı.

Sabit Disk üzerinde yapılan inceleme;

Samsung marka, SM500DM002 model, "5452145AB" seri numaralı sabit disk içerisinde bulunan FUJITSU marka, MHW2120BH model, "NZ1DT732C1FS" seri numaralı 120 GB sabit diskin birebir kopyasına ait MD5 ve SHA1 (HASH) değerleri kontrol edildi (Birebir kopya alma esnasında tutulan tutanakta belirtilen HASH değerleri).

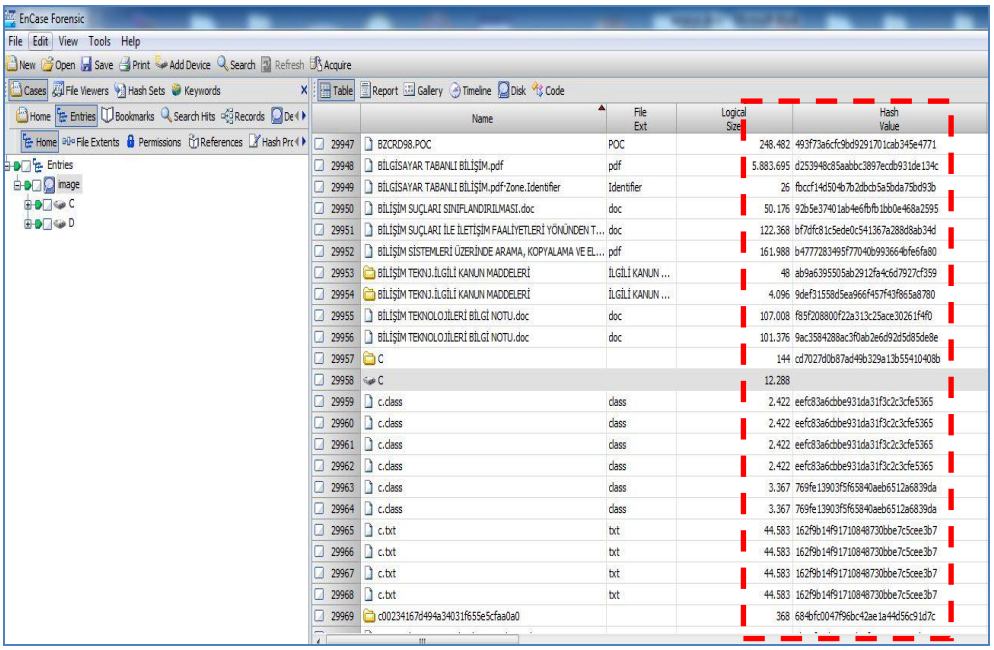
Fotoğraf 3.21. Sabit Diske Ait Alınan Birebir Kopyanın HASH Değerleri.

Alınan birebir kopya **Encase Forensic Adli Bilişim Yazılımı** ile açıldıktan sonra hesaplanan HASH değerleri görülmektedir. HASH değerleri (Birebir kopya alma esnasında tutulan tutanakta belirtilen HASH değerleri*)* aynı olduğu için incelemeye başlanıldı.



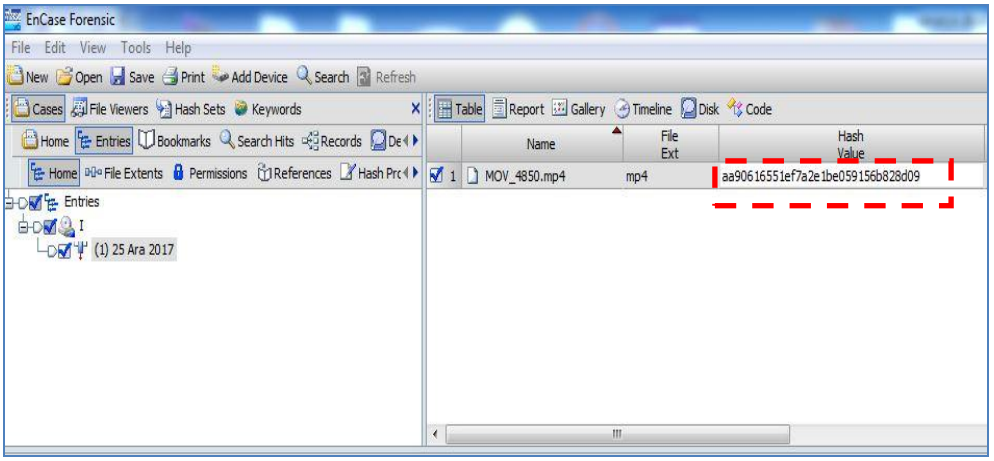
Şekil 3.22. Birebir Kopyanın Encase Yazılımı İle Açıldıktan Sonraki HASH Değerleri**.**

DVD+R içerisinde gönderilen suç konusu video dosyasının sabit disk içerisinde bulunup bulunmadığının tespiti amacıyla sabit disk içerisindeki tüm dosyaların HASH değerleri hesaplandı.



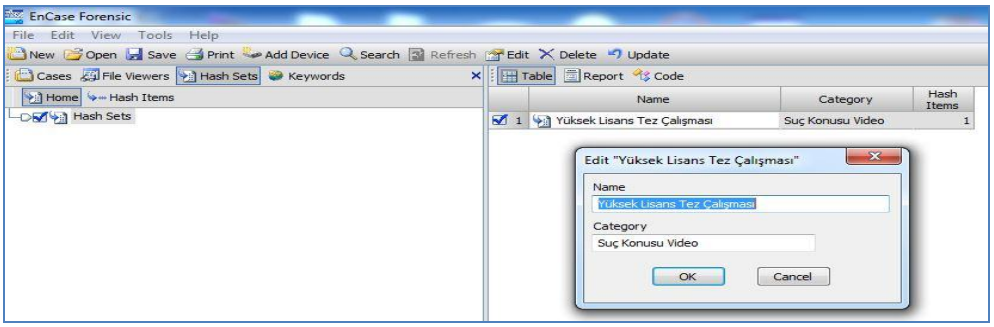
Şekil 3.23. Sabit Disk İçerisinde Tüm Dosyaların HASH Değerleri.

DVD+R içerinde gönderilen suç konusu video dosyasının ***(MOV_4850.mp4*** *isimli)* Hash Değerleri hesaplandı (Söz konusu dosyanın MD5 hash değerinin **"aa906 16551ef7a2e1be059156b828d09"** olduğu tespit edildi).



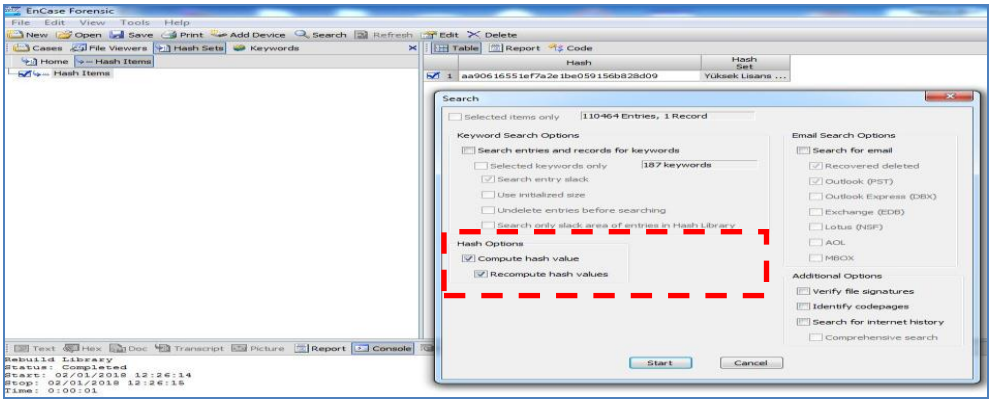
Şekil 3.24. DVD+R İçerisindeki Video Dosyasının HASH Değerleri.

Hesaplanan HASH değeri sabit disk içerisinde bulunan dosyalar ile karşılaştırmasının yapılabilmesi amacıyla HASH kütüphanesine eklendi.



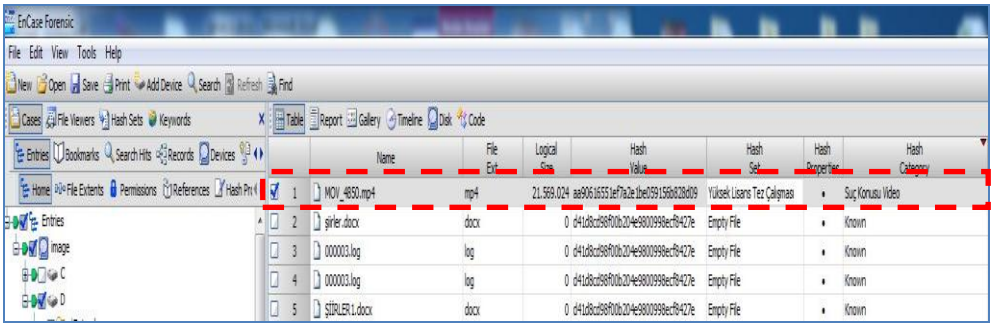
Şekil 3.25. Video Dosyasının HASH Değerinin HASH Kütüphanesine Eklenmesi.

HASH kütüphanesine eklenen suç konusu HASH DEĞERİ sabit disk içerisinde bulunan dosyaların HASH değerleri ile karşılaştırıldı.

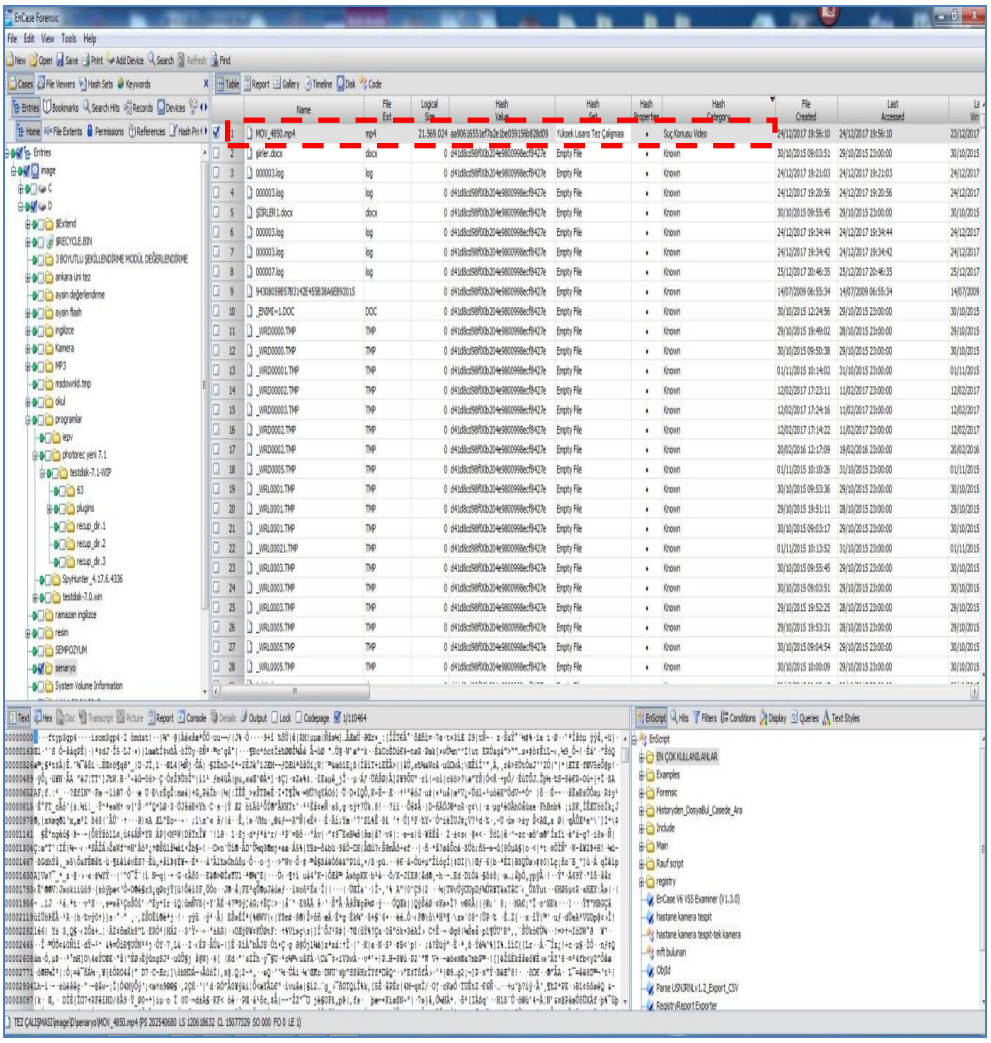


Şekil 3.26. HASH Analizi.

Yapılan analiz neticesinde sabit diskin **"D:\Senaryo"** isimli klasör altında bulunan **"MOV_4850.mp4"** isimli dosya ile HASH değerlerinin aynı olduğu tespit edildi.

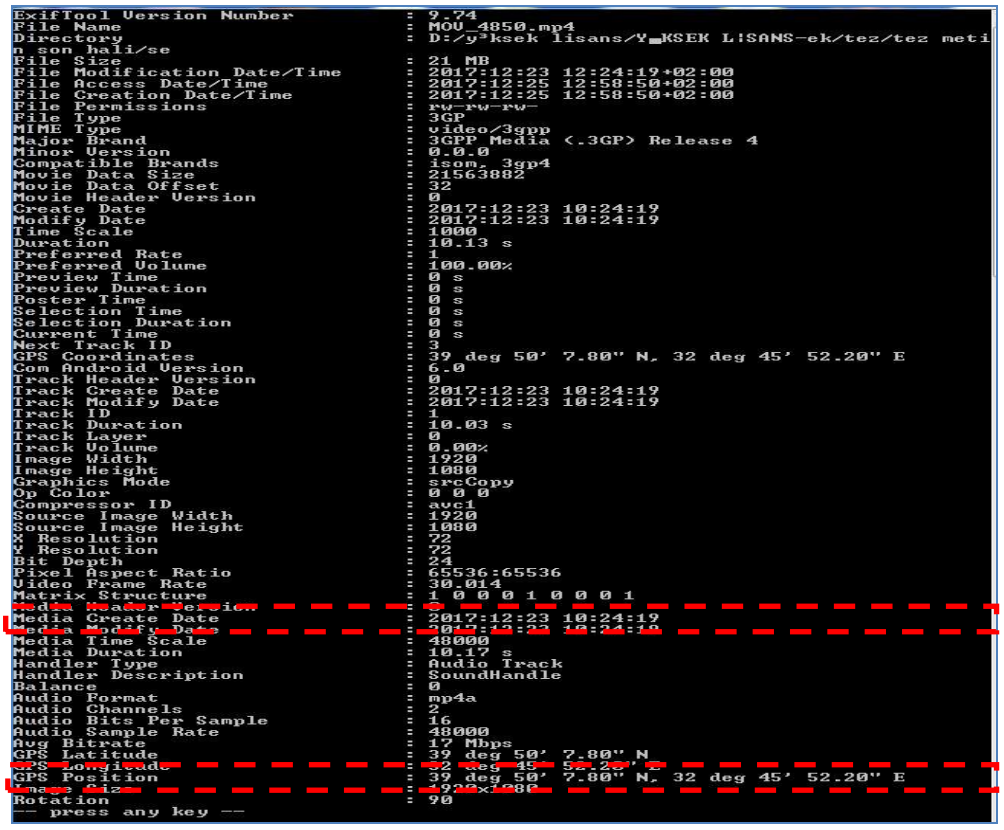


Şekil 3.27. HASH Analizi Sonucu Suç Konusu Video Dosyasının Tespiti.



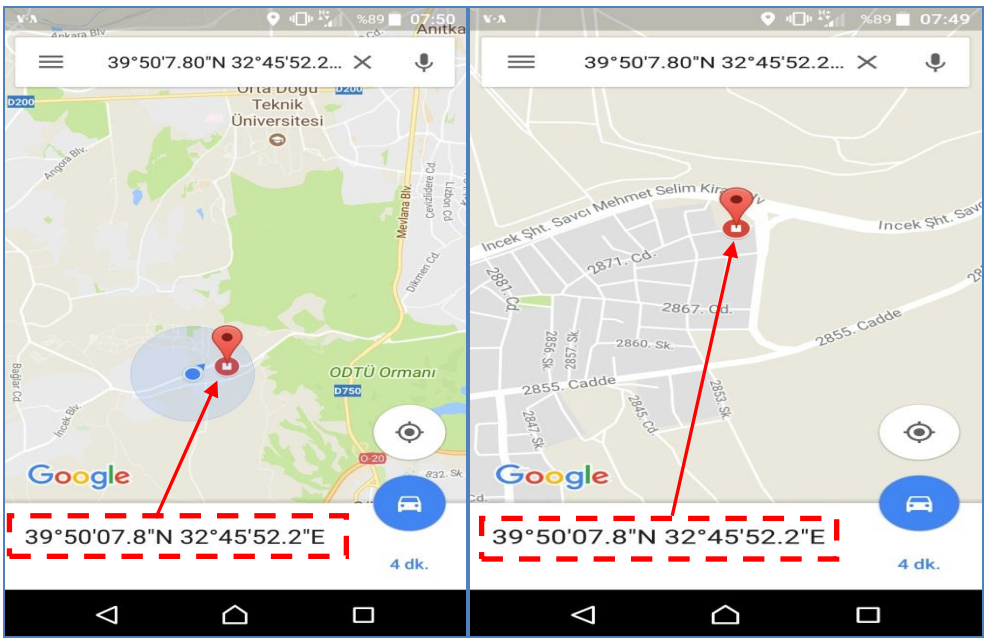
Şekil 3.28. HASH Analizi Sonucu Suç Konusu Video Dosyasının Tespiti.

Sabit disk içerisinde tespit edilen MOV_4850.mp4 isimli video dosyasının meta data (Üst veri bilgileri - kullanıcının doğrudan göremediği, verileri açıklayıcı bilgileri taşıyan sistem bilgileridir - Adli Bilişim ve Elektronik Deliller s.:150) bilgileri **Exiftool 9.74** isimli yazılım ile incelendiğinde; video dosyasının oluşturulma tarihinin **(Media Create Date:2017:12:23 10:24:19 GMT)** olduğu ve video dosyanın çekildiği koordinat bilgisinin **(39 deg 50’ 7.80”N, 32 deg 45’ 52.20” E)** olduğu tespit edildi.



Şekil 3.29. Video Dosyasının Üst Veri Bilgilerinin İncelenmesi.

Tespit edilen koordinat bilgileri **Google Map** üzerinden kontrol edildiğinde suç yeri olarak belirtilen Taşpınar köyü girişi mevkii ile uyumlu olduğu tespit edildi.

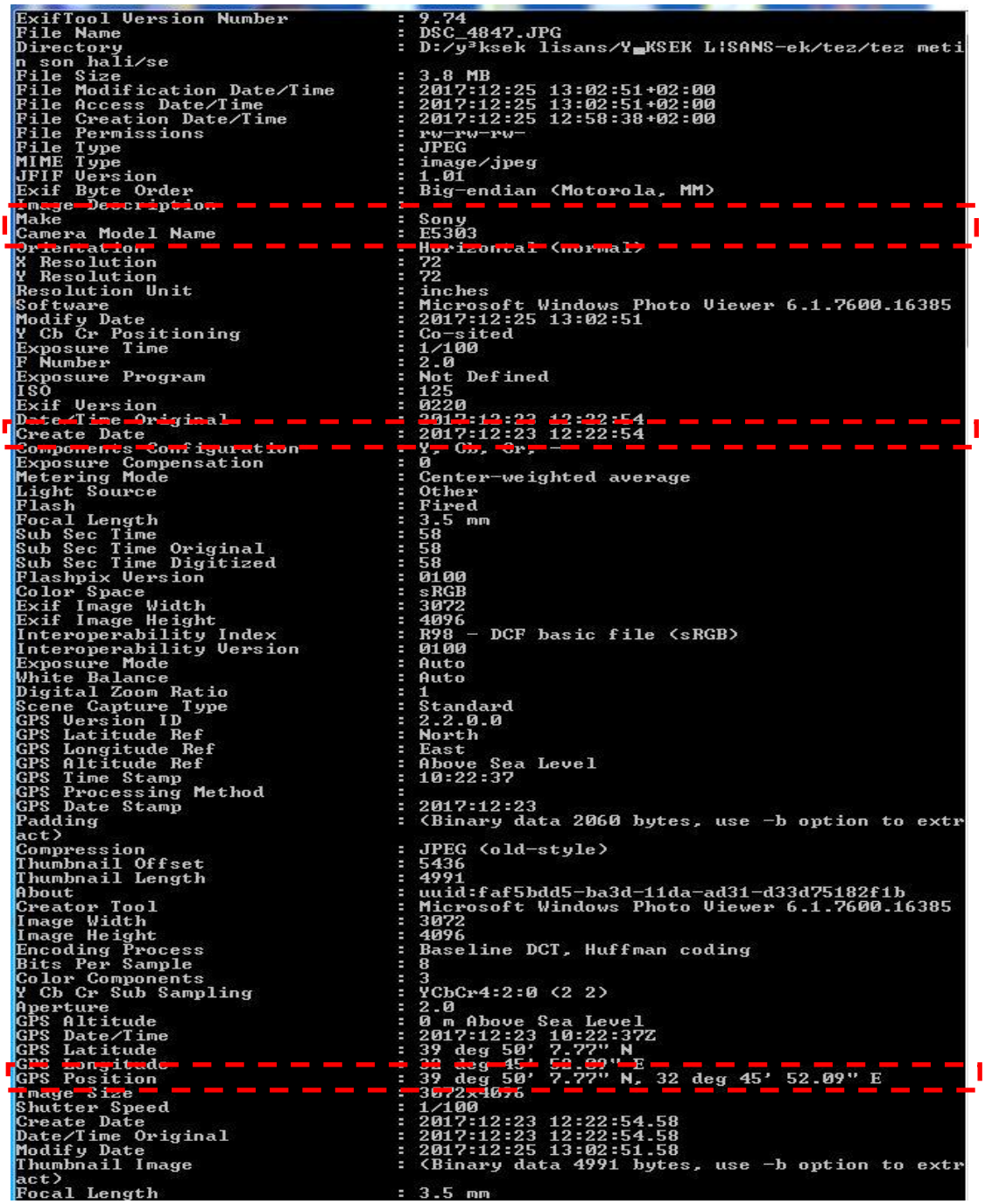


Şekil 3.30. Üst Veri Bilgilerinden Tespit Edilen Video Dosyasına Ait Koordinat Bilgilerinin Harita Üzerinde Gösterimi.

Ayrıca sabit diskin **“D:\Senaryo”** isimli klasör altında **“DSC_4847.JPG”** isimli resim dosyası tespit edilmiştir. Dosyanın tehdit metninin yazılı olduğu kağıt ta belirtilen resimle uyumlu olduğu tespit edilmiştir.

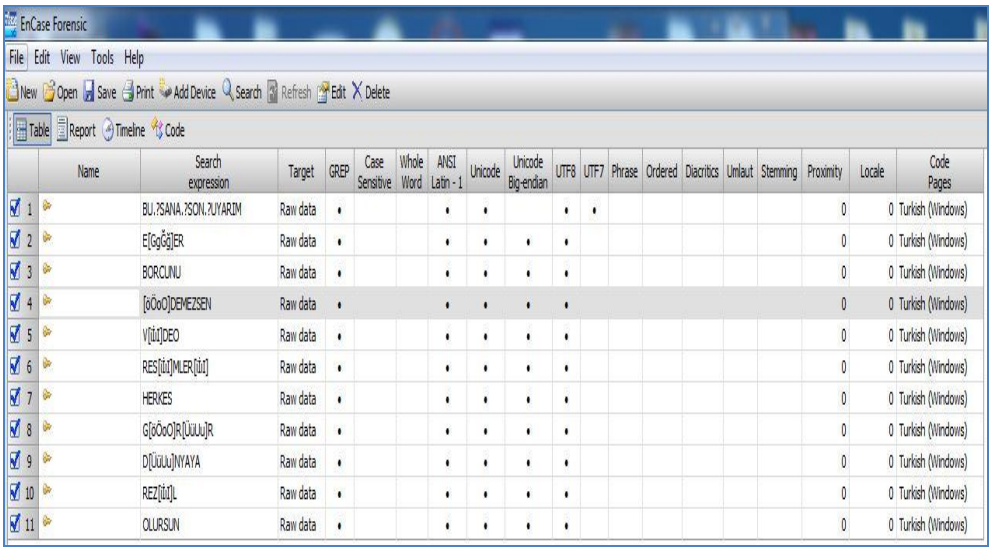
Şekil 3.31. Suç Konusu Resim Dosyasının Görünümü.

“DSC_4847.JPG” isimli resim dosyasının meta data bilgileri **Exiftool 9.74** isimli yazılım ile incelendiğinde; resim dosyasının oluşturulduğu kamera bilgisinin **Sony E5303** *(Şüphelinin cep telefonu ile aynı marka model)* olduğu, oluşturulma tarihi **(Create Date:2017:12:23 12:22:54 GMT+2)** ve resim dosyanın çekildiği koordinat bilgisinin **(39 deg 50’ 7.77”N, 32 deg 45’ 52.09” E)** olduğu tespit edildi. Resim dosyasının koordinat bilgileri ile suç konusu video dosyasının koordinat bilgilerinin aynı bölge içerisinde olduğu tespit edildi.



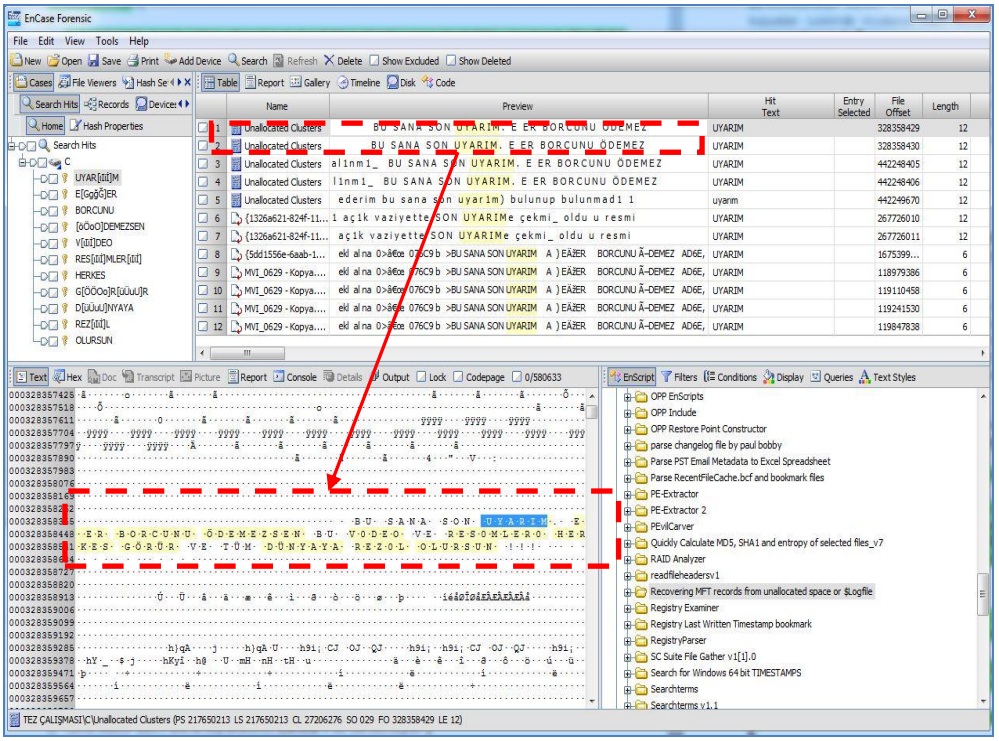
Şekil 3.32. Resim Dosyasının Üst Veri Bilgilerinin İncelenmesi.

Ayrıca sabit disk içerisinde tehdit metni içerisinde geçen ibareler anahtar kelime olarak aratıldı.



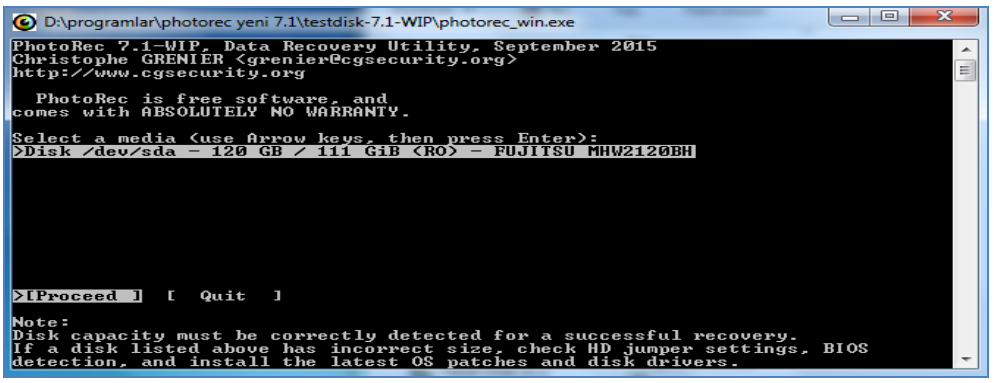
Şekil 3.33. Encase Adli Bilişim Yazılımı İle Anahtar Kelime Arama İşlemi.

Anahtar kelimesi araması neticesinde, sabit diskin silinmiş alanları olarak tabir edilen (Unallocated Clusters) disk bölümü içerisinde suç konusu olarak belirtilen kelimelere ulaşıldı.

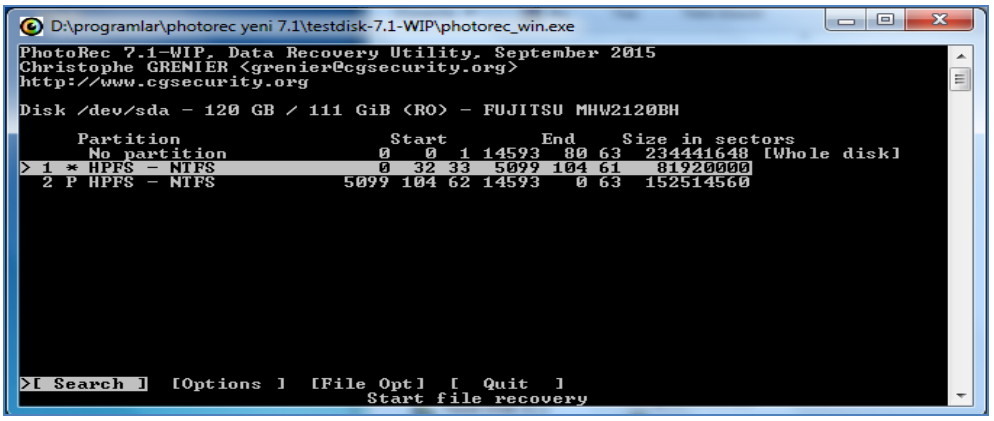


Şekil f 3.34. Encase Adli Bilişim Yazılımı İle Anahtar Kelime Sonuçlarının Analizi.

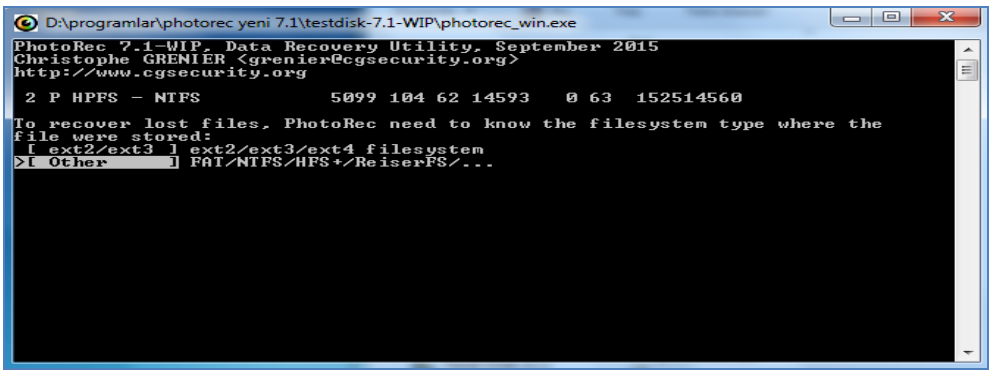
Sabit diskin silinmiş alanları içerisinde; **Photorec 7.1** isimli dosya kurtarma yazılımı ile dosya kurtarma işlemi yapıldı.



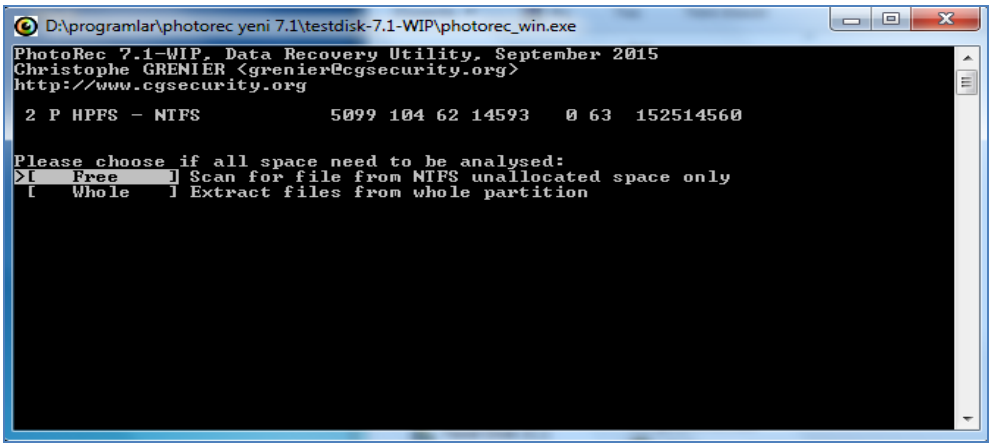
Şekil 3.35. Photorec 7.1 Yazılımı İle Dosya Kurtarma İşlemi.



Şekil 3.36. Photorec 7.1 Yazılımı İle Dosya Kurtarma İşlemi.

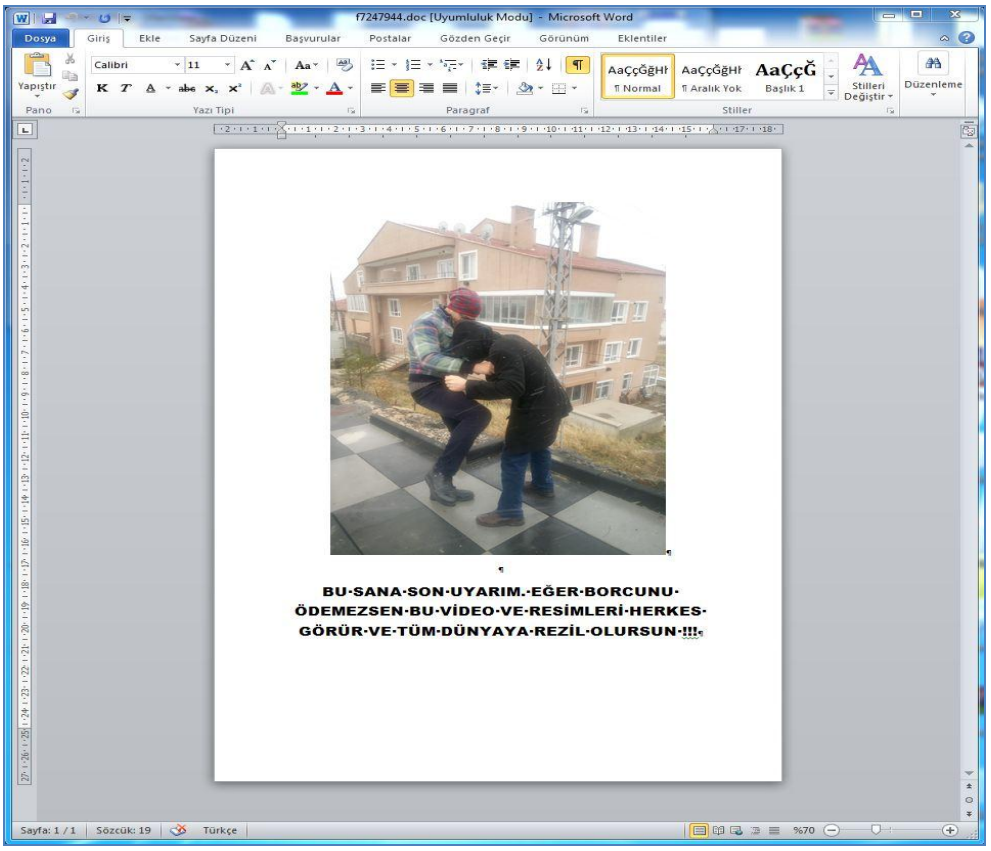


Şekil 3.37. Photorec 7.1 Yazılımı İle Dosya Kurtarma İşlemi.



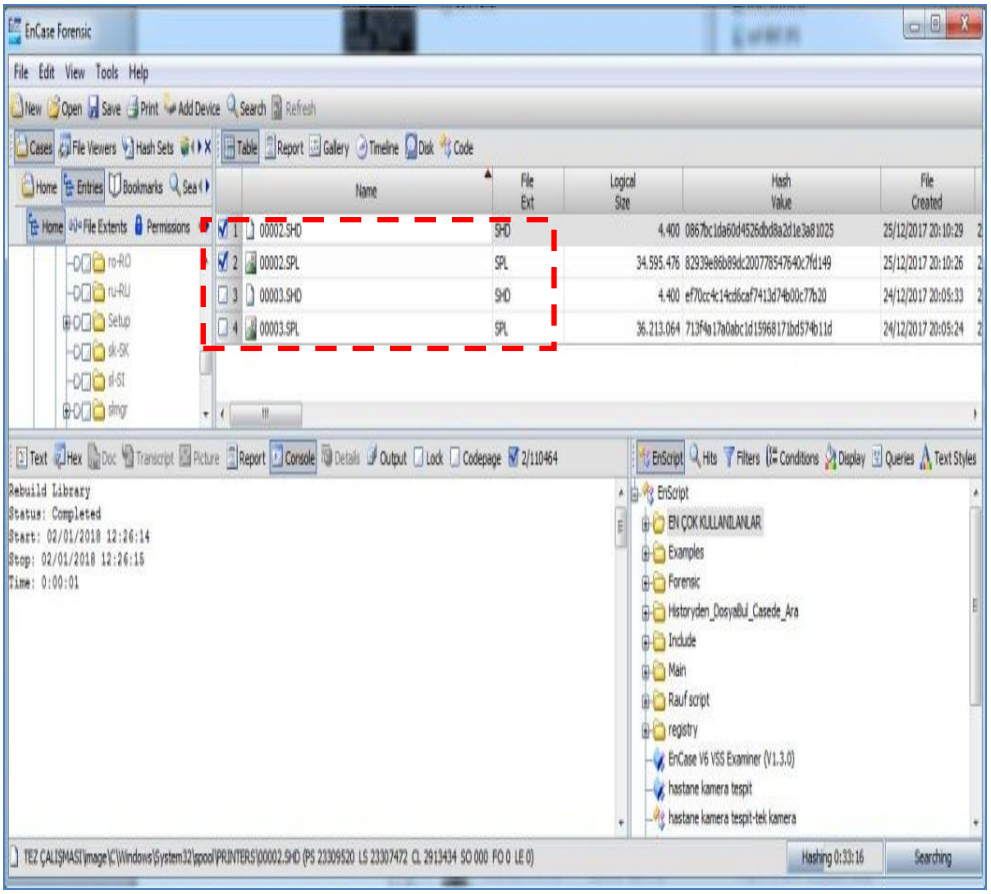
Şekil 3.38. Photorec 7.1 Yazılımı İle Dosya Kurtarma İşlemi.

Dosya kurtarması işlemi neticesinde; kurtarılan tüm dosyalar içerisinde **"f7247944.doc"** isimli Microsoft Word dosyasının *(isim bilgisi kurtarma programı tarafından atanmıştır.)* tehdit suçu ile ilgili olduğu tespit edildi.



Şekil 3.39. Photorec 7.1 Yazılımı İle Kurtarılan Suç Konusu Microsoft Word Dosyası.

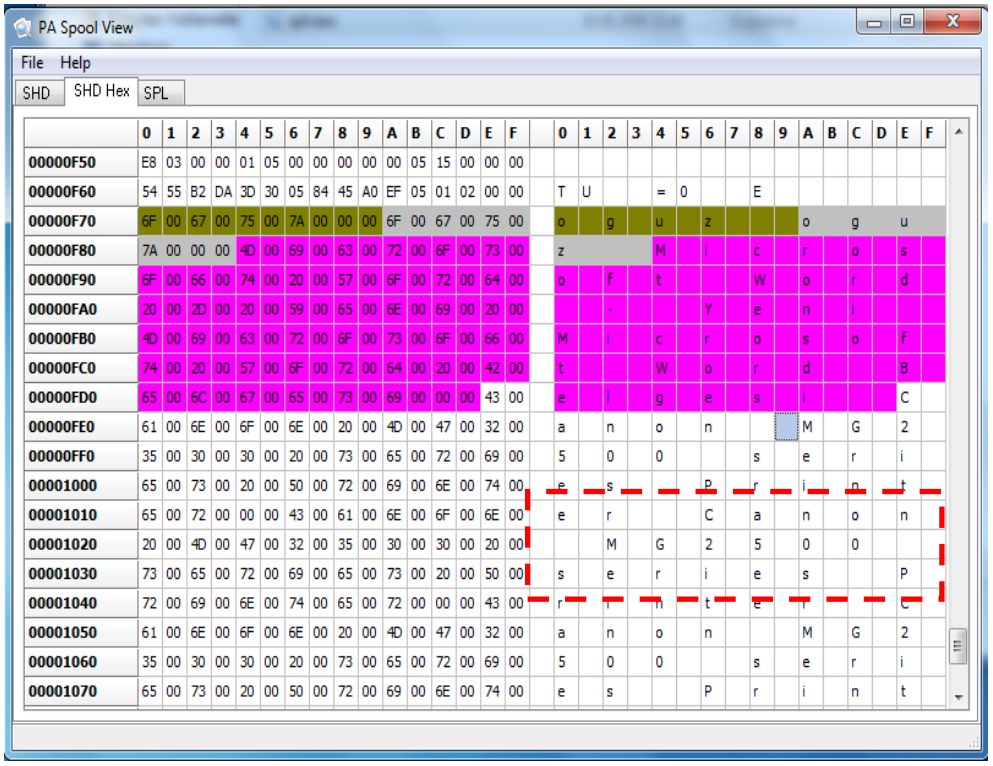
Windows 7 işletim sistemine sahip bir bilgisayarda yazıcıya gönderilen belgelerin kaydı (İki şekilde gerçekleşmektedir. Birincisi yazdırma işleminin tamamlanamadığı durumlarda, ikincisi ilgili kayıt defteri veritabanı içerisinde yazdırılan belgenin kaydını tut ayarının yapılması durumunda) **"C\Windows\System32\Spool\PRINTERS"** isimli klasör dizini altında tutulmaktadır. Bilgisayarın ilgili kaydı incelendiğinde "00002.SPL, 00002.SHD, 00003.SPL ve 00003.SHD" kayıtlarının bulunduğu tespit edildi.



Şekil 3.40. Encase Adli Bilişim Yazılımı İle Yazıcıya Gönderilen Belgelerin İncelenmesi.

Söz konusu kayıtlar **"EMFSpoolViewer.exe"** isimli program ile incelendiğinde; **"00002.spl"** isimli dosyanın içerisinde gönderilen tehdit metnine ait kayıtların bulunduğu, **00002.shd** dosyası içerisinde bilgisayar kullanıcı adı, gönderilen belgenin isim bilgisi ve yazıcıya ait bilgilerin bulunduğu tespit edildi.

Şekil 3.41. EMFSpoolViewer.exe Yazılımı İle Yazıcıya Gönderilen Belgelerin Tespiti.



Şekil 3.42. EMFSpoolViewer.exe Yazılımı İle Yazıcıya Gönderilen Belgelerin Tespiti.

Şüpheliye ait Sony marka, xperia C4(E5303) model cep telefonunun bilgisayara bağlanılıp bağlanmadığının tespiti amacıyla **"reg ripper v2.8"** isimli program ile bilgisayar içerisinde bulunan **system** ve **software** isimli kayıt defteri veritabanı dosyaları incelenmiştir. Yapılan incelemelerde Software isimli veritabanı dosyası içerisinde **Portable Devices** bölümünde bilgisayara bağlanılan cep telefonuna ait isim bilgisi ***(xperia C4)*** ile bağlanma tarihi bilgisi ***(24 Aralık 2017 saat:17:50:21(UTC))*** tespit edilmiştir.

Şekil 3.43. Reg ripper v2.8 Yazılımı İle Bilgisayara Bağlanılan Cep Telefonunun Tespiti.

Yazıcı üzerinde yapılan inceleme;

➢ Canon marka, PIXMA MG2550 model (yazıcı, tarayıcı ve fotokopi makinası ve renkli çıktı alma özelliğine sahip) bir yazıcı olduğu tespit edildi.

➢ Dahili hafızasının bulunmadığı tespit edildi.

➢ Yazıcının sadece veri aktarım kablosu ise bilgisayara bağlanma özelliğinin bulunduğu tespit edildi.

➢ Yazıcının dahili hafızası bulunmadığından dolayı içeriğinde herhangi bir inceleme yapılmamıştır.

4- İnceleme Sonucu Raporlama ve Delillerin İadesi Aşaması

a. İnceleme Sonucu Raporlama

Deliller üzerinde gerekli incelemeler ve tespitler yapıldıktan sonra Adli Bilişim İnceleme Sürecinin son aşaması olan Raporlama ve Delillerin İadesi aşamasına geçildi.

BİLİRKİŞİ RAPORU

Dosya No : 2017/XXX

Gönderen Makam : Gölbaşı İlçe Jandarma Komutanlığı

Olay Yeri ve Tarihi : Ankara İli, Gölbaşı İlçesi, Taşpınar Köyü Girişi - 23.12.2017

Olay Türü : Kasten Yaralama ve Tehdit Suçu

Şüpheli : H.U.S. (TC:12349505xxx)

Mağdur : M.E. (21728291xxx)

Gönderilen Deliller :

1. Samsung marka, SM500DM002 model, **"5452145AB"** seri numaralı, sabit disk (İçerisinde FUJITSU marka, MHW2120BH model, **"NZ1DT732C1FS"** seri numaralı 120 GB sabit diske ait imaj bulunmaktadır).

2. Sony marka, xperia C4 (E5303) model, "**35219407034xxxx"** IMEI numaralı cep telefonu ve bu cep telefonuna takılı vaziyette bulunan Turk Telekom marka **"899028603943263xxxx"** seri numaralı SIM kart.

3. Canon marka, PIXMA MG2550 model, **"ASLX52X"** seri numaralı yazıcı.

4. İçerisinde video görüntüsünün bulunduğu Sony marka **"asl123sacd12"** seri numaralı DVD+R.

5. Üzerinde tehdit metninin bulunduğu A4 ebadında yazıcı çıktısı.

İNCELEMELER SONUCUNDA;

1. Cep telefonunun kopyası üzerinde yapılan incelemede, içerisinde suç konusu video dosyası, resim dosyası ve tehdit içerikli metin belgesi tespit edilememiştir.

2. SIM kartın üzerinde arama kaydı, rehber bilgisi, kısa mesaj(SMS) ve SIM kart bilgisi haricinde veri bulunmadığından dolayı üzerinde inceleme yapılmamıştır.

3. İncelemeye verilen DVD+R'nin içerisinde bulunan suç konusu video dosyasının hesaplanan HASH değerinin sabit disk içerisinde **"D:\Senaryo"** isimli klasör altında bulunan **"MOV_4850.mp4"** isimli dosyanın hash değeri ile aynı olduğu tespit edilmiştir. Video dosyası oynatıcı program ile açıldığında, suç konusu video dosyası ile aynı olduğu tespit edilmiştir.

4. Tespit edilen video dosyasının metadata (Üst veri bilgileri) incelendiğinde; dosyanın oluşturulma tarihi(suç tarihi ile aynı) **(Media Create Date:2017:12:23 10:24:19 UTC)** ve video dosyanın çekildiği koordinat bilgilerine ulaşıldı **(39 deg 50' 7.80"N, 32 deg 45' 52.20" E).**

5. Dosyanın koordinat bilgilerine Google Map isimli uygulama üzerinden bakıldığında, koordinat bilgilerinin suç yeri olarak belirtilen Taşpınar köyü civarı olduğu tespit edildi.

6. Tehdit metni içerisinde geçen ibareler anahtar kelime olarak aratıldığında, sabit diskin silinmiş alanları olarak tabir edilen (Unallocated Clusters) disk bölümü içerisinde bahse konu tehdit mesajına ulaşıldı.

7. Sabit diskin silinmiş alanları içerisinden yapılan kurtarma işleminin sonucunda, tehdit metninin bulunduğu Microsoft Word belgesi kurtarıldı.

8. Bilgisayar içerisinde yazıcıya gönderilen dosyaların kaydının tutulduğu **"C:\Windows\System32\Spool\PRINTERS"** klasör dizini altındaki dosyalar incelendiğinde Canon marka yazıcıya gönderilen tehdit metnine ait kayıtlara ulaşıldı**.**

9. Bilgisayar ile bağlantı kuran aygıtların yapılan incelemesinde Sony marka xperia C4 model cep telefonunun bilgisayara bağlandığına dair veriler tespit edildi.

Sonuç: Elde edilen tespitler ışığında, incelemeye verilen cep telefonunun, dizüstü bilgisayarın ve yazıcının suç konusu elektronik delillerin oluşturulmasında kullanıldığı **tespit edilmiştir**.

b. Delillerin İadesi

Gerekli inceleme ve analiz faaliyetleri tamamlandıktan sonra deliller ile tarafımızca alınan delillerin kopyaları, Bilirkişi Raporu ile birlikte talep makamına iade edildi. İade esnasında delillerin teslim alındığı şekliyle ve dış etkenlerden hasar görmeyecek şekilde muhafazası sağlandı.

4. TARTIŞMA

Elektronik delillerin yapısı, mahkemede kabule şayan bir delil olarak kabul edilebilmeleri için özel bir mücadeleyi gerektirmektedir. Bu mücadeleyi verebilmek için uygun bir adli bilişim prosedürünün izlenmesi gerekmektedir (Berber 2004 S.:45). En uygun adli bilişim sürecinin belirlenmesi amacıyla çeşitli adli bilişim süreçleri analiz edilmiştir.

Yurt dışında tasarlanmış olan adli bilişim inceleme süreçleri incelendiğinde, dünyada ilk dijital verilerin suçu aydınlatmada kullanılması 1984 yılına kadar dayanmaktadır. 1984 yılında FBI (Federal Bureau of Investigation- Federal Soruşturma Bürosu) laboratuvarı ve diğer kolluk kuvvetleri tarafından bilgisayar kalıntılarını incelemek için bir program geliştirmeye başlandı ve bilgisayar incelemeleri için Computer Analysis Response Team (CART) kuruldu. Bu tarihten itibaren müdahale edilen suçlarda dijital delillerin toplanması ve incelenmesi konusunda adli bilişim standardının eksikliği ve bu standartların ihtiyaç olduğu konusunda fikir birliğine varıldı.

1995 yılından itibaren tespit edilen bu eksikliğin giderilmesine yönelik yurt dışında adli bilişim inceleme süreçleri tasarlanmaya başlandı. Yurt dışında o tarihten günümüze kadar yüzlerce süreç tasarlaması yapıldı. Ülkemizde ise 2004 yılında yürürlüğe giren 5137 sayılı CMK'nın 134. maddesinde bilişim suçlarına ait delillerin toplanmasına yönelik düzenleme ile ülke genelinde çeşitli adli bilişim inceleme süreçleri tasarlanmıştır.

Tasarlanan süreçlerden yirmi üçü *(17 yurt dışı, 6 yurt içi)* incelendiğinde, yurt dışı inceleme süreçlerinde;

"Çizelge 1.3 Devam Yurt Dışı Adli Bilişim İnceleme Süreçlerinin Aşamaları" isimli çizelgede **S3, S4, S5, S7, S9, S10, S11, S12, S14** ve **S16 Süreç Kimlik No** ile belirtilen adli bilişim inceleme süreçleri içerisinde **"Approach Strategy, Authorization, Awareness, Notification, Planning, Pre-Analysis Phase, Preparation, Readiness** ve **Recognition"** isimli süreç isimlerinin bulunduğu görülmüştür. Bu süreç isimleri tarafımızca tasarlanan ve yurt içi inceleme süreçlerinde bulunmayan **"HAZIRLIK" aşaması kapsamında değerlendirilmiştir.**

M. Reith, C. Carr & G. Gunsh 2002 yılında **"Abstract Digital Forensics Model (ADFM)"** olarak adlandırdığı Adli Bilişim sürecini **9 aşama** oluşturmuştur. Bu aşamalar **" Identification- Preparation – Approach Strategy- Preservation - Collection – Examination – Analysis – Presentation – Returning Evidence"** olarak belirlenmiştir. Burada son aşamada **"RETURNING EVIDENCE"** (Kanıtların İadesi) aşaması ile süreci tamamlamıştır. Bu süreç aşaması da tarafımızca tasarlanan ve yurt içi inceleme süreçlerinde bulunmayan "**DELİLLERİN İADESİ**" aşaması olarak belirtilmiştir.

Tarafımızca ortaya konan adli bilişim inceleme sürecinin uygulanabilirliğini göstermeye yönelik örnek bir olay tasarlanmıştır. Tasarlanan **"Kasten Yaralama ve Tehdit"** olay içerisinde, şüpheli şahıs elektronik cihazları kullanmak suretiyle işlenen suçun delillerini oluşturmuştur. Elektronik cihazlar içerisinden suç konusu delillerin tespiti esnasında **"HASH Değerleri ve Analizi, Meta Data bilgileri, Anahtar Kelime Arama, Silinmiş Dosyaların Kurtarılması, İşletim Sistemi Dosyaları Analizi** ve **Kayıt Defteri Veri Tabanı Dosyalarının Analizi"** gibi adli bilişim inceleme yöntemleri kullanılmak suretiyle sürecin analiz ve inceleme boyutuna vurgu yapılmıştır. İncelemeler esnasında kullanılan yazılım ve donanımlara bağlı kalmadan da adli bilişim incelemelerinde kullanılan farklı yazılım ve donanımlar ile de aynı sonuçlara ulaşılabileceği unutulmamalıdır.

5. SONUÇ VE ÖNERİLER

Yurt dışında tasarlanan ve inceleme safhalarını oluşturan süreçler içerisinde belirtilen, fakat yurt içi inceleme safhalarını oluşturan süreçlerde belirtilmeyen **"HAZIRLIK"** ile **"DELİLLERİN İADESİ"** aşamalarının, adli bilişim inceleme süreci içerisinde gerekli safhalardan olduğu değerlendirilmiş ve ortaya koyduğumuz akış içerisinde izah edilmiştir.

Tarafımızca ortaya konan adli bilişim inceleme sürecinin uygulanabilir olduğunu açıkça anlatmak amacıyla örnek bir olay tasarlanmıştır. Tasarlanan örnek içerisinde adli bilişim inceleme sürecinin tüm aşamaları ayrıntılı bir şekilde ortaya koymak suretiyle adli bilişim inceleme sürecinin **uygulanabilir olduğu gösterilmiştir**.

Tez çalışması kapsamında ülkemiz mevzuatında bulunan ve konu ile ilgili kanun maddeleri belirtilmiştir. Bunlar arasından 5137 sayılı Ceza Muhakemeleri Kanunu'nun 134. Maddesi; *"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 elkonulabilir. Şifrenin çözümünün yapılması ve* ***gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir****."* şeklinde belirtilmiştir. Fakat gecikme olmaksızın iade edilir ifadesinden suça ilişkin olduğu değerlendirilen bir sabit diskin şüpheliye iade edilmesi durumunda suçun devam edebileceği de değerlendirilerek *(örneğin, kredi kartı dolandırıcılığı yapan şüphelinin imajı alınan sabit diskinin kendisine iade edilmesi neticesinde sabit disk içerisinde bulunan kredi kartı bilgileriyle suç işlemeye devam etmesi gibi)* **iade edilir yerine iade edilip edilemeyeceği hakim kanaatinde olmasının uygun olacağı değerlendirilmektedir.**

Tarafımızca tasarlanan ve adli bilişim safhalarını oluşturan inceleme süreci genel olarak tüm suç türlerini kapsayacak şekilde planlanmıştır. Fakat adli bilişim alanındaki suç türleri gün be gün çeşitlilik arz ettiğinden, bir sonraki çalışmada suç türlerine göre alt inceleme süreçlerinin tasarlanmasının faydalı olacağı değerlendirilmektedir.

ÖZET

Adli Bilişimde İnceleme Süreçleri

Adli Bilişimde İnceleme Süreçleri isimli tez çalışmasının amacı, her geçen gün daha da zorlu bir hal alan adli bilişim incelemelerini standartlaştırmak ve eksik kalan bir hususun önüne geçilmesi adına bir inceleme süreci ortaya koymaktır. Bu sürecin kapsamı oluşturulurken yurt dışında ve yurt içerisinde tasarlanmış olan süreçlerin incelemesi yapılmış ve Türk Hukuk sistemine uygun bir süreç tasarlaması yapılmıştır.

Kapsam olarak adli bilişim inceleme süreci, olay yerinde delilin tespitinden önce yapılacak olan hazırlık aşamasından başlayıp, inceleme ve raporlamanın yapılmasından sonra delilin iade aşamasını da kapsayacak şekilde tüm süreci içerisinde barındırmıştır.

Tasarlanan adli bilişim inceleme sürecinin gerçek hayatta uygulanabilirliğini göstermek adına kurgulanan örnek bir olay üzerinden tüm aşamalar tek tek gösterilmiştir. Örnek olay kurgulanırken adli bilişim incelemelerinde en çok karşılaşılan Dizüstü bilgisayar (sabit disk), cep telefonu, SIM kart, DVD, yazıcı gibi elektronik deliller üzerinde incelemeler gerçekleştirilmiştir. İncelemeler esnasında deliller üzerinde uygulanan yöntemler ile tespit edilebilecek veri türleri ortaya konmuştur. İncelemeler adli bilişim incelemelerinde kullanılan genel kabul görmüş adli bilişim yazılım ve donanımları ile yapılmıştır.

Sonuç olarak tasarlanan adli bilişim inceleme sürecinin uygulanabilirliği gösterilmek suretiyle bu alanda çalışan olay yeri inceleme personellerine ve adli bilişim uzmanlarına katkı sağlayacağı değerlendirilmektedir.

Anahtar Kelimeler: Adli Bilişim, Birebir Kopya, Elektronik Delil, Hash, İnceleme Süreci

SUMMARY

Investigation Processes at Digital Forensics

The Examination Processes in Forensic Computing aims to standardize forensic computation studies, which are becoming more and more challenging each passing day, and to put forward an examination process in order to prevent a missing item. While the scope of this process has been established, the processes designed abroad and in the country have been examined and a process has been designed in accordance with the Turkish legal system.

As a matter of course, the forensic examination process started from the preparatory stage before the detection of the evidence at the scene and after the examination and reporting, it included the whole process including the return stage of the evidence.

All phases are shown one by one through a case that is designed to show the applicability of the designed forensic investigation process in real life. When the case study was conducted, examinations were carried out on electronic evidence such as Laptop computer (hard disk), mobile phone, SIM card, DVD, printer which are most common in forensic examinations. The data types that can be detected by the methods applied on the evidence during the examinations are presented. The reviews were made using generally accepted forensic software and hardware used in forensic science examinations.

As a result, it is evaluated that the designed forensic investigation process will be able to contribute to on-scene investigation personnel and forensic experts working on this area by showing applicability.

Key words: Computer Forensic, Image, Electronic Evidence, Hash, Examination Process

KAYNAKLAR

ARTUNER H (2015). Adli Bilişim Alanında Dijital Delil, Delil Karartma, Delil Toplama

AYDIN E D (1992). Bilişim Suçları ve Hukukuna Giriş, s.:3

AYDOĞAN H (2009). Adli Bilişim'de Yeni Elektronik Delil Elde Etme Yöntemleri Polis Akedemisi Yüksek Lisans Tezi Ankara

BARYAMEREEBA V, TUSHABE F (2004). The Enhanced Digital Investigation Process Model, in Proceeding of Digital Forensic Research Workshop, Baltimore, MD

BAYRAKTAR Y D (2011). Muhakemelerde Delillerin Önemi *Sosyal Bilimler Dergisi*, sayı:25

BEEBE N L, CLARK J G (2004). A Hierarchical, Objective-Based Framework for the Digital Investigations Process, in Proceeding of Digital Forensic Research Workshop (DFRWS), Baltimore, Maryland

BEM D, HUEBNER E (2007). Computer Forensic Analysis in a Virtual Environment, *International Journal of Digital Evidence, **Vol. 6**, no. 2, pp. 1-13.*

BERBER K L (2004). Adli Bilişim (Computer Forensıc)

BROWN C L T (2006). Computer Evıdence: Collectıon and Preservatıon.

BROWN L T C (2010). Computer Evıdence:Collectıon and Preservatıon, 2nd Ed., course technology, a part of cengage learning, USA.

CARRIER B, SPAFFORD E H (2003). Getting Physical with the Digital Investigation Process, *International Journal of Digital Evidence, **Vol. 2**, No. 2*

CARRIER B, SPAFFORD E H (2004). An Event-based Digital Forensic Investigation Framework. Proceedings of Digital Forensics Research Workshop. Baltimore, MD.

CIARDHUAIN S (2004). An Extended Model of Cybercrime Investigation, *International Journal of Digital Evidence, **Vol. 3**, No. 1, pp. 1-22.*

CMK 5271 sayılı Ceza Muhakemesi Kanunu

ÇAKIR H, KILIÇ M S (2014) Adli Bilişim ve Elektronik Deliller

EKİZER A H (2014). Adli Bilişim, Erişim Adresi: [www.ekizer.net]. Erişim Tarihi:18/01/2018.

ENCASE 6.18 Amerika Birleşik Devletlerinde kurulu bulunan Guidance Software firmasının geliştirdiği Adli Bilişim İnceleme yazılımıdır. [www.guidancesoftware.com]

ENFSI (European Network of Forensic Science Institutes)- Best Practice Manual fort he forensc Examination of Digital Technology ENFSI-BPM-FIT- Version 01- November 2015 sayfa 17

FREILING F C, SCHWITTAY B (2007). Common Process Model for Incident and Computer Forensics, in Proceedings of Conference on IT Incident Management and IT Forensics, Stuttgard,Germany, pp. 19-40

GÖKSU M. (2010); Hukuk yargılamasında Elektronik Delil, Ankara Üniversitesi Doktora Tezi, Ankara.

HENKOĞLU T (2014). Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi 2. Baskı.

JKDB(Jandarma Kriminal Daire Başkanlığı) (2011)Adli Bilimler II

KOHN M, ELOFF J H P, OLIVIER M S (2006). Framework for a Digital Forensic Investigation

KOLTUKSUZ A (2010). Adli Bilişime Giriş s.:43, Adli Bilişim Günü, Yaşar Üniversitesi, 7 Haziran 2010, İzmir

KRUISE W G, HEISER J G (2002). Computer Forensıcs Incıdent Response Essentıals

Mobiledit FORENSIC EXPRESS v5.0.0.11564 Mobil cihazların incelemelerinde kullanılan adli bilişim yazılımıdır. [http://www.mobiledit.com]

NIST (National Instute of Standards and Technology) (2006) *Guide to Integrating Forensic Techniques into Incident Response special Publication 800-86 (s.:3-1)*

NIJ (National Institute Of Justice) (2001). Electronic Crime Scene Investigation: A Guide For First Responders Photodisc Inc. USA.

NOBLETT M G, POLLITT M M, PRESLEY L A (2000). Recovering and Examining ComputerForensic Evidence, Forensic Science Communications, ***Vol. 2,*** *No. 4.)*

ÖZTÜRK B, ERDEM M R (2006). Uygulamalı Ceza Muhakemesi Hukuku. 9. Baskı

PALMER G (2001). DTR-T001-01 Technical Report. A Road Map for Digital Forensic Research, Digital Forensics Workshop (DFRWS), Utica, New York.

Photorec 7.1 Data Recovery Utilities, Christophe GRENIER [http://www.cgsecurity.org] September 2015

POLLITT M M (1995). Computer Forensıcs: An Approach To Evıdence In Cyberspace. Proceeding of the National Information Systems Security Conference (pp. 487-491).

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

REITH M, CARR C, GUNSH G (2002). An Examination of Digital Forensics Models, *International Journal of Digital Evidence, **Vol. 1, No. 3**.*

ROGERS M K, GOLDMAN J, MISLAN R, WEDGE T, DEBROTA S (2006). Computer Forensic Field Triage Process Model, presented at the Conference on Digital Forensics, Security and Law, pp. 27-40

SACHOWSKI J (2016). Implementıng Dıgıtal Forensıc Readıness: From Reactive to Proactive Process 1st edition

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

STEPHENSON P (2003). A Comprehensive Approach to Digital Incident Investigation, Information Security Technical Report, **Vol. 8**, Issue 2, pp 42-52.

SUNDRESAN P (2009). Digital Forensic Model based on Malaysian Investigation Process, *International Journal of Computer Science and Network Security, **Vol. 9,** No. 8.*

Tableu TD2u Forensic Kit Amerika Birleşik Devletlerinde kurulu bulunan Guidance Software firmasının geliştirdiği birebir kopya alma cihazıdır. [www.guidancesoftware.com]

TCK 5237 sayılı Türk Ceza Kanunu

TDK. "Adli Bilişim" Erişim Adresi: [http://www.tdk.gov.tr/index.php?option=com_bilim sanat&arama=kelime &guid=TDK.GTS.5a58cca6486c44.96836850]. Erişim Tarihi: 12/01/2018.

TDK. "Bilişim" Erişim Adresi: [http://www.tdk.gov.tr/index.php?option=com_gts &kelime=BİLİŞİM]. Erişim Tarihi: 12/01/2018.

TDK. "Delil" Erişim Adresi: [http://www.tdk.gov.tr/index.php?option=com_gts &kelime=DELİL].Erişim Tarihi: 12/01/2018.

TDK. "Elektronik Delil" Erişim Adresi: [http://www.tdk.gov.tr/index.php?option =com_bilim sanat&arama=kelime & guid=TDK.GTS.5a5c9efc 771dd3.55188359]. Erişim Tarihi: 12/01/2018.

YURTCAN E (1996). Ceza Yargılaması Hukuku.

ÖZGEÇMİŞ

I- Bireysel Bilgiler

Adı: Ramazan

Soyadı: OĞUZ

Doğum Tarihi ve Yeri: 1980, DİNAR

Uyruğu: T.C.

Medeni Durumu: Evli

Askerlik Durumu: Muaf

İletişim Adresi ve Telefonu: Jandarma Kriminal Daire Başkanlığı, Bilişim Teknolojileri İnceleme Şube Müdürlüğü ÇANKAYA/ANKARA

Tel:0(505) 4532399

II- Eğitimi

2001 – 2007 Anadolu Üniversitesi İktisat Fakültesi Kamu Yönetimi Bölümü (Lisans)

1994 – 1998 Anadolu Meslek Lisesi (Elektrik Bölümü) -ISPARTA

Yabancı Dili: İngilizce

III Ünvanları

IV- Mesleki Deneyimi

İş Deneyimi Yıl	Firma/Kurum	Görevi
2000 -2005	J.Gn.K.lığı	Çeşitli İlçe Jandarma Komutanlıklarında ve Karakol Komutanlıklarında Karakol/Tim Komutanı
2005 - 2011	J.Gn.K.lığı	Olay Yeri İnceleme Uzmanı
2011 - 2018	Jandarma Kriminal Daire Başkanlığı/ Bilişim Teknolojileri İnceleme Şube Müdürlüğü	Veri ve Donanım İnceleme Uzmanı

V- Üye Olduğu Bilimsel Kuruluşlar

VI- Bilimsel İlgi Alanları

1- Ocak 2012 Jandarma Dergisi, "Polenlerin Şahitliği Kriminalistikte Adli Palinoloji" konulu çalışması.

2- 13. ULUSLARARASI ANADOLU ADLİ BİLİMLER KONGRESİNDE "Ios Mobil İşletim Sistemine Sahip Cep Telefonlarında Periscope Uygulaması Ve Uygulamanın Bıraktığı İzler " konulu sözlü sunum.

3- 13. ULUSLARARASI ANADOLU ADLİ BİLİMLER KONGRESİNDE "Ios Mobil İşletim Sistemine Sahip Cep Telefonlarında Periscope Uygulaması Ve Uygulamanın Bıraktığı İzler " konusu Proceeding Book ta Makale

VII- Bilimsel Etkinlikleri

- 3rd International Symposium on Digital Forensics and Security – ANKARA, 11-12 Mayıs 2015

- 13. Uluslararası Anadolu Adli Bilimler Kongresi – Germencik/AYDIN 05-07 Mayıs 2016

VIII- Diğer Bilgiler (Katıldığım Kurslar)

- Olay Yeri İnceleme Kursu - Ankara, 29.05.2006-07.07.2006
- Olay Yeri İnceleme Tekamül Kursu - Ankara, 05.04.2010-22.05.2010
- Temel Eğitim Katılım Belgesi – Ankara, 12 Eylül 2011-07 Ekim 2011
- Temel Eğitim ve Akreditasyon Konulu Eğitim – Ankara, 13-14.09.2011
- Bilişim Teknolojileri Bilgisayar Kullanım Kursu – Ankara. 3 ay 2011
- Linux, Unix Sistem Yönetimine Giriş – Ankara,12-23 Kasım 2012
- Bilişim Teknolojileri Donanım Kursu – Ankara, 3 ay 2012
- Görsel Programlama-1 [C# Net] Kursu – Ankara, 3 ay 2012
- Veri Tabanı Programlama-1 [Access] Kursu – Ankara, 3 ay 2012
- Veri İnceleme Sistemi Eğitimi – Ankara, 28-30 Ocak 2013
- Access Data Forensic Tool Kit (FTK 5.0) – Ankara, 09-11 Ekim 2013
- Veri Kurtarma Eğitimi – Ankara, 24-28 Aralık 2013
- Veri ve Donanım İnceleme Uzmanlığı Sertifikası – Ankara, 17.12.2013
- Siber Adli Beyaz Şapkalı Hacker kursu – Ankara, 1-5 Eylül 2014

- Kriminal Daire Başkanlığı İç Tetkik Eğitimi – Ankara, 10 Temmuz 2015
- Temel Elektronik ve Sayısal Haberleşme Eğitimi – Ankara, 30.11.2015-25.12.2015
- Avrupa Birliği Eşleştirme Projesi - Olay Yerinden Bilişim Delillerinin Toplanması Kursu – Ankara, 24- 28 04.2017
- Mobil Cihaz İnceleme Eğitimi, Adli Bilişim İnceleme, İnternet Geçmişi ve Sohbet Kayıtları İnceleme ve Analizi Kullanıcı Eğitimi – Ankara, 09 – 13 Ekim 2017
- Veri Kurtarma Eğitimi – Ankara, 30-31 Ekim 2017