

BİLGİLERİMİZİ ARTIK
DİJİTAL ORTAMDA
SAKLAMAYI TERCİH
EDİYORUZ. KİTAP
ÇALIŞMAMIZI,
EN SON
HAZIRLADIĞIMIZ
BESTEYİ,
ÇEKTIĞİMİZ
FOTOĞRAFLARI
KÂĞIT ÜZERİNDE
DEĞİL KİŞİSEL
BİLGİSAYARIMIZDA,
ŞİRKETLERİN
KAYITLARINI KALIN
KLASÖRLERDE
DEĞİL SUNUCU
BİLGİSAYARLARDAKİ
UYGULAMALARDA
TUTUYORUZ.
HATTA BUNUNLA DA
YETİNMIYORUZ,
HER ŞEYİ BULUTA
GÖNDERİYORUZ.
DİJİTALLEŞTİRDİĞİMİZ
BİLGİ ARTIK HER
YERDE VE HER AN
DOLAŞIMDA.
BİR TUŞA BASINCA
KARŞIMIZA GELİYOR,
BİR TUŞLA
ÇOĞALIYOR VE BİR
TUŞLA DA YOK
OLUYOR VEYA BİZ YOK
OLDUĞUNU
ZANNEDİYORUZ!

■ Doç. Dr. Murat Volkan DÜLGER, Akademisyen/Avukat

ADLİ BİLİŞİM & Ülkemizde Uygulaması

Bilgi çağını yaşadığımız 21. yüzyılda teknolojiye bağımlı bir haldeyiz. Yaşamın her alanını dijitalleştiriyoruz. Bankacılıktan ticarete, habercilikten iletişime, iş hayatından sosyal hayata kadar her şeyin önüne “e” harfini koyar olduk. Teknolojinin yardımı ile yaşamımız ne kadar kolaylaşıyor gibi görünse de, maddiyonun öteki yüzünde banka hesaplarımıza girilmesi, e-postlarımızın ele geçirilmesi, kişisel bilgilerimizin çalınması gibi bilişim suçu olarak tabir ettiğimiz istenmeyen ve bize zarar veren olaylara da maruz kalmaya başladık.

Dijital dünya sınırlarımızı zorlarken suçu aydınlatabilecek bilgiyi de yine dijital ortamlardan elde etmek zorundayız. Hal böyle olunca, dijital ortamlardan delil tespit etmek, kıldan DNA tespit etmek gibi uzmanlık gerektiren bir konu oldu. Adli Bilişim (Computer / Cyber Forensic) olarak adlandırdığımız bu uzmanlık alanı artık Adli Bilimler çatısı altında ayrı bir disiplin ve uzmanlık alanı olarak kendini göstermeye başlamış durumda.



Bu makalede adli bilişimin tüm yönlerini teknik detaylara çok fazla girmeden, hukukçuların anlayacağı bir dil ile anlatmaya çalışılacağı. İlk önce dijital delil kavramı ve dijital delilin bütünlüğünü ve sağladığımız veri özet değeri kavramlarını anlattıktan sonra, adli bilişimin temel ilkelerine ve süreçlerine detaylı olarak değineceğim.

DİJİTAL DELİL

Adli bilimler, suçun ispatında kullanılabilecek nitelikteki bilginin, yani delilin bilimsel yollarla ortaya çıkarılmasını edilmesini konu alır. Adli bilişim incelemelerinde ise, sabit disk ve taşınabilir USB bellek gibi elektronik materyallerin içerisindeki gözle görülmeyen, elle tutulmayan ve sanal olarak nitelendirdiğimiz dijital veriler incelenir ve gerçek /fiziksel dünya ile ilişkisi kurulup, suçu ispat edebilecek nitelikteki dijital veriler ortaya çıkarılır.

Elektronik materyallerin içerisinde suçu ispat edebilecek nitelikteki dijital veriler “dijital delil” olarak isimlendirilir.

ELEKTRONİK MATERYALLERİN İÇERİSİNDE SUÇU İSPAT EDEBİLECEK NİTELİKTEKİ DİJİTAL VERİLER “DİJİTAL DELİL” OLARAK İSİMLENDİRİLİR.

Dijital veriler doğası gereği çok hızlı şekil ve yer değiştirebildiği için, yanlış bir müdahale, dijital delillerin bir daha elde edilemeyecek şekilde yok olmasına sebebiyet verebilir. Bu sebeple dijital delillere müdahale edenlerin bilişim sistemlerinin nasıl çalıştığını, bilgiyi nasıl sakladığını ve nasıl ilettiğini, bununla birlikte siber dünyayı ve bu ortamlardaki dijital delillere nasıl yaklaşılması gerektiğini iyi bilmeleri gerekir. Adli bilişim konusunda tecrübe kazanmış bu insanlar ise “Adli Bilişim Uzmanı” olarak isimlendirilir.

Dijital delillerin incelendiği ortamlar da son derece önemlidir. İncelemeler ister adli kollukta ister özel bilirkişiler tarafından yapılıyor olsun, laboratuvar ortamı sağlanmalıdır. Adli bilişim laboratuvarlarında elektronik materyallere zarar gelmeyecek

şekilde uygun ortam sağlanmalı ve incelemeler adli imaj dosyası üzerinden yürütülmelidir.

VERİ ÖZET DEĞERİ (HASH)

Adli bilişim incelemelerinde en kritik konu delilin değişmeden incelenmesidir. Delilin değişmediğinin ispat edilmesi için veri özet değeri (Hash) olarak tanımlanan bilginin delil ile beraber taşınması gerekir. Veri özet değeri bilimsel olarak kabul edilmiş matematiksel bir algoritmadır.

DELİLİN DEĞİŞMEDİĞİNİN İSPAT EDİLMESİ İÇİN VERİ ÖZET DEĞERİNİN (HASH) DELİL İLE BERABER TAŞINMASI GEREKİR.

Algoritmaya parametre olarak giren veri, işlem sonucunda belirli uzunlukta sayısal bir değer olarak çıkar. Birden fazla veri özet değeri hesaplama algoritması bulunmaktadır. Her algoritmada çıkan verinin özet değerinin sayısal uzunluğu farklıdır. Çıkan değerlerin sayısal uzunluğu, hesaplanan iki verinin özet değerinin aynı olma olasılığını düşürür.

Örneğin, “Adli Bilişim” yazısından oluşan bir verinin özet değerini, MD5 (Message-Digest 5) adlı algoritmayı kullanarak hesaplayacak olursak; “07ffec3f75b3b9b01c4fc3fe85de247” şeklinde bir sayısal değer üretilir. Oluşan veri özet değeri 32 adet 16’lık sayı sisteminin rakamlarını içerir. Bu kadar rakam ile oluşturabileceğimiz değer miktarı 2128, yani kullandığımız sayı sisteminde 36 rakamlı, çok büyük bir sayı olup, iki farklı veriye ait özet değerinin aynı çıkma olasılığının ne kadar düşük olduğunu gösterir.

Eğer “Adli Bilişim” verisinin veri özet değeri, SHA1 (Secure Hash Algorithm 1) algoritması ile hesaplanırsa “b16a22679c9550ad-85cd97621fd9640595ecdb84” sayısal değeri üretilir. Oluşan özet değeri ise bu sefer 40 adet 16’lık sayı sisteminin rakamlardan oluşan başka bir sayıdır.

Ancak burada rakamlar arttığı için olasılık logaritmik olarak düşer. Veri özet değeri hesaplanacak bilgi ister 1 TB boyutunda bir diskin içeriği olsun ister içerisinde sadece “Adli Bilişim” yazan bir metin dosyası olsun oluşan veri özet değerinin uzunluğu hep aynı olacaktır.

Olasılık değerlerinin aşırı düşük olması sebebiyle, oluşan veri özet değerinin veriyi temsil ettiği kabul edilir. Adli bilişim incelemelerinde bir dijital delilin veri özet değeri için hem MD5 hem de SHA1 algoritmaları kullanılır.

ADLİ BİLİŞİM İNCELEMELERİ SÜRECİ

Adli Bilişim incelemelerinin süreci, diğer tüm adli bilimler disiplinlerinde olduğu gibi olay yerinde başlar ve delilleri içeren raporun mahkemeye iletilmesi ile sona erer.

Uygulamayı dikkate aldığımızda sürecin tamamını üç ana parçaya ayırmak gerekir. İlk aşama olaya müdahale edilip dijital delilleri içeren elektronik materyallerin toplanmasıdır. Bu aşama ne kadar sağlıklı yürürse, bundan sonraki aşamalarda o kadar sağlıklı yürütülecektir. Ardından elde edilen elektronik materyaller incelenerek dijital deliller ortaya çıkarılır.

Bu aşama, laboratuvar ortamında adli bilişim uzmanlarının gerçekleştirilmelidir. En son aşamada, elde edilen delillerin yazılı olarak raporlanması yapılır.

Anglo Amerikan hukuku sistemine tabi ülkelerde ise ayrıca rapor mahkemede bir sunum eşliğinde anlatıldığından son aşama raporlama ve sunum başlığı altında karşımıza çıkmaktadır



ELDE ETME AŞAMASI

Olay yeri delile ilk temasın yapılacağı aşamadır. Delilin toplanması sırasında uygun koşulların sağlanamaması, delilin sağlıklı toplanamamasına ve delil niteliğini kaybetmesine yol açacaktır. Bu yüzden olay mahalline gelmeden önce kolluk kuvvetleri olay yeri ile ilgili bilgi edinmeli ve gerekli alet ve araçları yanlarına almalıdırlar.

Ülkemizde olay yerinden elektronik materyallerin toplanması ile ilgili gerekli hukuki düzenleme; CMK madde 134’de “Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma” başlığı altında yapılmıştır. Yapılan hukuki düzenleme her ne kadar yeterli olmasa da, olaya müdahale eden ve elektronik materyali toplayan kolluk görevlilerini bağlayan zorunluluklar bulunmaktadır.

CMK 134(1):
... ŞÜPHELİNİN
KULLANDIĞI
BİLGİSAYAR VE
BİLGİSAYAR PROG-
RAMLARI İLE
BİLGİSAYAR KÜTÜK-
LERİNDE **ARAMA**
YAPILMASINA,
BİLGİSAYAR KAYIT-
LARINDAN **KOPYA**
ÇIKARILMASINA ...

Maddenin birinci fıkrasında olay yerinde şüpheliye ait elektronik materyallerin içerisindeki verilerin kopyasının çıkarılması, yani adli imaj dosyasının elde edilmesi tarif edilmektedir. Adli imaj dosyası, materyalin içerisindeki verinin tamamını içeren bir bilgisayar dosyasıdır. İster materyalin içerisindeki verinin veri

özet değeri alınsın ister adli imaj dosyasının veri özet değeri alınsın ikisi de aynı olacaktır. Daha sonra yapılacak incelemeler orijinal materyal üzerinde değil imaj dosyasında gerçekleştirilmelidir.

İkinci fıkrada ise; imaj dosyasının alınmasının mümkün olmadığı durumlarda materyallere el konulması gerektiği ve imajları alındıktan sonra materyallerin gecikme olmaksızın iade edilmesi gerektiği belirtilmektedir.

CMK 134 (2):
...ÇÖZÜMÜN
YAPILABİLMESİ VE
GEREKLİ
KOPYALARIN
ALINABİLMESİ İÇİN,
**BU ARAÇ VE
GEREÇLERE
ELKONULABİLİR.
ŞİFRENİN
ÇÖZÜMÜNÜN
YAPILMASI VE GE-
REKLİ KOPYALARIN
ALINMASI HALİNDE,
ELKONULAN
CİHAZLAR GECİK-
ME OLMAKSIZIN
İADE EDİLİR.**

Dördüncü fıkrada ise; elde edilen imaj dosyasının bir kopyasının şüpheli veya vekiline verilmesi gerektiği belirtilmektedir.

İmaj alma sürelerinin uzun olması, yüksek boyutlardaki disklerin imajlarının almanın mümkün olmaması, imaj almadan inceleme yapılacağı zaman delillerin nasıl toplanacağı gibi durumlar detaylı olarak belirtilmediğinden, kanun

CMK 134 (4):
ÜÇÜNCÜ FIKRAYA
GÖRE ALINAN
YEDEKTEN BİR KOP-
YA ÇIKARILARAK
ŞÜPHELİYE VEYA
VEKİLİNE VERİLİR VE
BU HUSUS TUTA-
NAĞA GEÇİRİLEREK
İMZA ALTINA ALINIR.

maddeleri bu hali ile uygulamada yeterli olmamaktadır.

Kanun maddelerini bir yana koyarsak, sağlıklı ve doğru bir adli bilişim incelemesinin yapılabilmesi için en azından olay yerinde şüpheliye ait elektronik materyallerin imaj dosyasının oluşturulması ve imaj dosyasının veri özet değerinin taraflara verilmesi gerekir. Taraflara veri özet değerinin verilmesi, incelemenin doğru imaj üzerinden yapıldığını ispat etmek içindir. İnceleme sonucunda hazırlanan raporda incelemenin hangi veri özet değerine sahip imaj üzerinden yürütüldüğü belirtilir. Böylece başka bir adli bilişim uzmanı da aynı veri özet değerine sahip imaj dosyasını incelediğinde aynı sonuçlara ulaşacağı ortaya konulmuş olur. Eğer farklı bir veri özet değeri hesaplanırsa imaj dosyasının farklı bir diske ait olduğu veya disk üzerinde değişiklik yapıldığı anlamına gelir. Böyle bir durumda değişikliğin nasıl olduğu ile ilgili geriye doğru bir tespit yapmak da mümkün olmaz.

Elde edilen materyaller toplandıktan sonra imaj dosyası olay yerinde alınmaz ise içerisine sonradan veri eklenip eklenmediği hususunda her zaman bir şüphe söz konusu olur. Bu yüzden delilin niteliği bozulmuş olacak ve yürütülen incelemeler de boşa gidecektir. Bununla birlikte elde edilen imaj dosyalarının veri özet değerleri taraflara verilmelidir. Aksi halde, incelemesi yapılan imaj dosyasının olay yerinde elde edilen

imaj dosyası olup olmadığı ile ilgili şüphe oluşur. Bu şüphelerin önüne geçebilmek için ilke olarak kolluk kuvvetleri olay yerinde imaj dosyasını tarafların huzurunda almalı ve imaj dosyası alınırken oluşan veri özet değeri taraflara verilmelidir (CMK'nın 134/2. maddesi istisnadır ve istisna olarak uygulanmalıdır!).

CMK'nın 134. maddesi bu hali ile uygulandığında en azından olay yerinde dijital delillere müdahale edildiğinde imaj dosyasının alınması ve taraflara veri özet değerinin verilmesi gerektiği konularını içerir. Bu yüzden kanundaki zorunluluklar kolluk kuvvetlerine delilin güvenliği açısından bağlayıcı bir zorunluluk getirmektedir.

ADLİ İMAJ DOSYASI;
OLAY YERİNDEN
ELDE EDİLEN
ELEKTRONİK
MATERYALİN
İÇERİSİNDEKİ
VERİNİN
TAMAMINI İÇEREN
BİR **BİLGİSAYAR
DOSYASIDIR.**

LABORATUVAR İNCELEMESİ

Olay yerinde elde edilen materyaller ve/veya imaj dosyaları henüz bulgu niteliğindedir. Bir sonraki aşama; bulgular incelenip içerisinde suçu ispat edebilecek nitelikte delilin bulunup bulunmadığının tespit edilebilmesidir. Laboratuvar ortamında yapılacak bir incelenmenin ardından materyaller ispata elverişli delil niteliğine kavuşur.

İncelemeler adli imaj dosyası üzerinden yürütülmelidir. Eğer olay yerinden elde edilen materyal laboratuvara gönderildiyse üzerinde

zorunlu kalınmadıkça bir inceleme yapılmamalı ve güvenli bir ortamda saklanmalıdır. Özellikle sabit diskler mekanik aksamlara sahip olduğundan fiziksel güvenliği alınmadığında disk bir daha çalışmayacak bir duruma gelebilir.

Adli bilişim incelemeleri gerekli donanım ve yazılımlarla donatılmış, yetişmiş uzmanları bulunan laboratuvarlarda yürütülmelidir. Laboratuvar ortamında; incelemelerin yapılacağı iş istasyonları, yazma - koruma cihazları, adli inceleme yazılımları, farklı tipteki elektronik materyalleri okuyabilecek dönüştürücüler ve ara kablolar gibi donanım ve yazılımlar bulunmalıdır.

Olay yerinde elde edilen imaj dosyası terabaytlerce veri içeriyor olabilir. Bu kadar çok veri içerisinde suç unsuru verinin bulunması, samanlıkta iğne aramak kadar zor olabilir. Veriler bilinçli olarak değiştirilmiş veya silinmiş olabilir. Her incelemeye başlamadan önce materyalin durumuna göre veri kurtarma işlemleri uygulanmalıdır. Böylece anlamlandırılmış daha fazla bir veri ile çalışma imkânı olacaktır.

Burada en kritik konu incelemeyi yapacak olan uzmanın niteliğidir. Adli bilişim uzmanları bilgisayar sistemlerinin nasıl çalıştığını, bilgiyi nasıl sakladığını ve nasıl ilettiğini, bununla birlikte siber dünyayı ve bu ortamlardaki dijital delillere nasıl yaklaşması gerektiğini iyi bilmelidir. Ülkemizde adli bilişim uzmanlığı ile ilgili bir standart bulunmamaktadır. Ancak bu konuda uluslararası bazı sertifikasyon kurumları sınav ile sertifikasyon sağlamaktadır. Sertifikasyonlar genel şartları sağlıyor olsa da, her inceleme konusu olayda çok farklı durumlarla karşılaşmak mümkün olduğundan, önemli olan adli bilişim uzmanının ne kadar tecrübeye sahip olduğudur.

Bir uzman ne kadar çok dosya üzerinde çalışmış ise o kadar çok tecrübeye sahip olacaktır.



RAPORLAMA AŞAMASI

Adli bilişim incelemeleri sonucunda yapılan çalışmalar ve elde edilen deliller bir rapor eşliğinde ilgili makama sunulmalıdır. Hazırlanan rapor, talep edilen husus doğrultusunda elde edilen bilgileri içermelidir. Raporun içeriği yapılan inceleme doğrultusunda teknik bilgileri içereceği için raporun diline çok dikkat etmek gerekir. Zira kullanılacak gereksiz teknik bilgiler raporun anlaşılabilirliğini azaltacak ve sonucu özetlemeyecektir.

Bir adli bilişim raporu, bir makalede bulunan Giriş-Gelişme-Sonuç bölümlerindeki gibi oluşturulmalıdır. Giriş bölümünde; yapılan inceleme öncesi bilgiler girilmelidir. Bu bilgiler:

- **İncelemede kullanılan donanım ve yazılımların versiyonları ile birlikte bir listesi:** Aynı donanım ve yazılımlar kullanıldığında aynı sonuç elde etmesi gerekir.
- **Talep edilen incelemenin ne olduğu:** Nasıl bir inceleme yapılması istenmiş ise, bu talep rapora dökülmelidir. Yapılan incelemeler de talep doğrultusunda yapılmalıdır. Talep edilen çalışmalardan herhangi biri eksik bırakılmamalı, eğer yapılamıyorsa neden yapılamadığı anlatılmalıdır.
- **Raporu hazırlayan uzman ile ilgili bilgi ve belgeler:** Raporu inceleyen uzmanın yetenekleri ve incelemeyi kapsayıp kapsamadığı ortaya konulmuş olur.
- **Tarih bilgileri:** Talebin ne zaman geldiği, ne zaman incelemeye başlandığı, imajın ne zaman alındığı vs. gibi tarihler raporda belirtilmelidir. Özellikle mahkemelerin en sık sorun yaşadığı konulardan birisi de raporun zamanında hazırlanmasıdır.
- **İncelenen elektronik materyallere ait bilgiler:** İncelenen materyalin cinsi, sabit disk mi yoksa USB bellek mi olduğu, kapasitesi, seri numarası, veri özet değeri, içerisindeki işletim sistemine ait bilgiler vs. belirtilmelidir. Böylece incelenen materyalin detaylı bir künyesi çıkarılmış olur.

Raporun gelişme bölümünde ise yukarıda listelenen materyaller üzerinde laboratuvarında bulunan donanım ve

yazılımlar ile nasıl bir inceleme yapıldığı detaylı olarak anlatılmalıdır. Delilin hangi dosya olduğu, dosyanın veri özet değeri, disk üzerinde bulunduğu lokasyon gibi bilgiler belirtilmelidir. Ayrıca tespit edilen delile hangi işlemler sonucunda erişildiği kronolojik olarak anlatılmalıdır.

Bazı adli bilişim raporlarında; sadece delil olarak tespit edilen dosyanın ve/veya veriye ait bilgilerin belirtildiğine rastlanılmaktadır. Ancak bu dosyanın nasıl elde edildiği ve hangi işlemler uygulandığı anlatılmaz ise, aynı süreçler uygulanarak raporda elde edilen sonucun doğrulaması yapılamayacaktır. Bu durum raporların kalitesini gösteren en önemli noktalardan biridir.

Raporun sonuç bölümünde ise; sorulan hususu özetleyecek kısa bir metin yazılmalıdır. Örneğin; eğer sorulan husus, “X dosyası bu bilgisayarda var mı? Varsa ne zaman oluşturulmuştur?” şeklinde ise, raporun sonuç bölümüne “X dosyası incelenen bilgisayarda “C:\Dosyalar” klasörü altında bulunmaktadır. Dosyanın oluşturma tarihi 12.12.2016’dır” gibi kısa ve yalın bir bilgi bulunmalıdır. Bu bilgiye nasıl ulaşıldığı ile ilgili tüm teknik çalışmalar raporun inceleme yani gelişme bölümünde yazılmalıdır. Eğer yapılan inceleme adli bir vaka ise; raporun sonuç bölümü raporu talep eden hakim veya savcıya hitap eder.

Zira hakim ve savcı için önemli olan “sorulan husus tespit edilmiş mi, edilmemiş mi?” olduğudur. Raporun teknik konuları ile ilgilenmeyecektir. Raporda anlatılan teknik kısımlar ise tarafları ikna etmek için yazılır. Avukatlar raporu başka bir adli bilişim uzmanına incelemek isteyebilirler. Bu durumda hazırlanan rapordaki tüm süreç aynı inceleme yapıldığında yine aynı sonucu elde ediyor olmalıdır.

SONUÇ

Adli bilişim uzmanlığı ile ilgili ülkemizde bir standart bulunmuyor olması, çok farklı kalitelere rapor çıkaran özel veya tüzel kişiliklerin bulunmasına sebep olmaktadır. 3.11.2016 tarihli ve 6754 sayılı Bilirkişilik Kanunu dahi bu standartları koymamıştır. Sadece bilirkişilerin denetlenmesini zorunlu hale getirmiştir.

Zorunluluğu denetleyecek ve adli bilişim uzmanlarının kalitesini ortaya koyacak nitelikte bir birimin oluşturulması çok da kolay görünmemektedir.

Sorun ülkemizde adli bilişim konusunda yetişmiş insanların bulunmamasıdır. Mevcut durumda az sayıdaki uzman ise kurmuş oldukları adli bilişim laboratuvarları üzerinden inceleme yapmaktadır ve adli bilişim uzmanlarını denetleyecek daha üst bir makam henüz bulunmamaktadır.

Çok sayıda bilişim suçunun işlendiği günümüzde adli bilişim uzmanlığının önemi yadsınamayacak kadar önemlidir.

BU YÜZDEN
ÜLKEMİZDE ADLİ
BİLİŞİM UZMANI
YETİŞTİRİLMESİNE
BÜYÜK ÇABA SARF
EDİLMESİ GEREKİR.

Doç. Dr. Murat Volkan DÜLGER
Akademisyen / Avukat
volkan.dulger@dulger.av.tr

[1] Ian Walden, Computer Crimes and Digital Investigations, Second Edition, Oxford, Oxford University Press, 2016, s. 371.

[2] Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Altıncı Baskı, Ankara, Seçkin Yayıncılık, 2015, s. 789