Adli Bilişim
(Computer Forensics – Bilgisayar Kriminalistiği.)

Bilişim sistemlerinin hayatımızın her alanına girdiğini inkâr etmek elbette ki imkânsız. İnsanoğlu büyüğünden küçüğüne gerek sosyal hayatta gerekse iş hayatında bilgisayar kullansın yada kullanmasın, farkında olsun yada olmasın, bir şekilde bilişim sistemlerinin getirdiği nimetlerden yararlanmaktadır. Bununla birlikte; tarihin başlangıcından beridir insanoğlunun var olduğu her sosyal alanda suçun olması doğaldır ve günümüzde bilişim teknolojileri de insanoğlunun suç işlemek için veya suç işlerken kullandığı araçlardandır.

Bir suçlunun arkasında işlediği suçla ilgili delil, iz ve emare bırakmaması doğanın bir kanunu olarak insanoğlunun elinde olmadığından, bilişim sistemleri ile işlenen suçlarda suç ile ilgili deliller farklı şekil ve formatlarda suç sonrasında dijital delil olarak bulunabilmektedir.

Adli Bilişim (Computer Forensics – Bilgisayar Kriminalistiği) bilimi; suçun aydınlatılabilmesi için bilimsel metotlar kullanılarak, çeşitli varyasyonlardaki dijital medyalar üzerinde bulunan, suçla ilgili dijital delillerin bozulmadan ve zarar görmeden anlaşılabilir bir şekilde adalet önüne sunulmaya hazır hale getirilmesini sağlayan ve başlı başına bilimsel teknik prensiplerin uygulandığı bir delil inceleme sürecinin bütünüdür.

İngilizcede, Computer Forensics olarak geçen ve Türkçemizde tam olarak çevrildiği takdirde Bilgisayar Kriminalistiği anlamını olan, ancak dilimizde genel kabul görmüş şekliyle Adli Bilişim diye adlandırılan bilim dalı; aslında delil inceleme bilimi olan Kriminalistik biliminden pek fazla farklı değildir. Kriminalistik bilimindeki gibi amaç işlenmiş bir suçta delillerin ortaya konmasıdır. Aynı zamanda Adli Bilişim biliminde de Kriminalistik biliminde olduğu gibi; suç mahallindeki olay yeri güvenliği ve ilk olay yeri müdahalesi ile incelemesi, delillerin olay yerinden toplanırken zarar verilmeden ve gözden kaçırılmadan toplanması, incelenmek için tam teşekküllü laboratuvarlara götürülürken muhafazalı bir şekilde nakil prosedürleri, inceleme aşamasında delilin bütünlüğünün zarar görmeden incelenmesi ve daha sonrasında da tarafsız olarak bilimsel verilere dayandırılıp elde edilmiş delillerin adli makamlara anlaşılır bir şekilde sunulması için raporlama aşaması gibi delil inceleme süreci mevcuttur. Kriminlistik biliminde delil inceleme aşamasında genellikle elle tutulur gözle görülür deliller varken Adli bilişim bilimi elektronik ortamdaki dijital delillerle ilgilenir. Bilişim sistemlerindeki delil olarak kullanılması muhtemel bulguların tespit edilmesi ve delil olarak ortaya konması, verilerin saklandıkları manyetik dijital ortamlardan anlaşılır bir şekilde çıkartılarak yazılı metin haline dönüştürülmesi suretiyle mümkündür. Bazı durumlarda ise bulgular; yazılı metine dönüştürülse bile, bilişim sistemleri teknolojileri hakkında teknik bilgi ve birikimi olması beklenmeyen adli merciler tarafından anlaşılır formatta olmadığından açıklanmaları ve izah edilmeleri gerekmektedir. Sonuçta adli bilişim bilimi çoğunlukla dijital deliller üzerine yoğunlaşmaktadır. Adli Bilişim biliminin delil inceleme üzerinde ilgilendiği Dijital Delil ne demektir peki? Dijital Delil için aşağıdaki tanımı yapmak sanırım yanlış olmaz.

Dijital Delil: Bilişim sistemlerinin veya bilgileri otomatik olarak işleme tabi tutma yetisine sahip elektronik cihazların veri depolama medyaları üzerinde bulunan yahut bu medyalar üzerinden geçen, suç ile ilgili delil niteliği taşıyabilecek ve suçun aydınlatılmasını sağlayacak verilerdir.

Üzerinde veri depolama yetisi bulunan veya dijital veriyi üzerinden geçiren he türlü elektronik cihaz bilgisayar olsun ya da olmasın dijital delil ihtiva etme potansiyeline sahiptir. Günümüzde elektronik veri depolama ve işleme birimleri öylesine yaygınlaşmıştır ki; Adli Bilişim biliminin inceleme alanında olan dijital deliller, sadece bilgisayar sistemlerinin veri depolama birimlerinde yer almamaktadır. Buda Adli Bilişim biliminin sadece bilişim suçlarında ya da bilişim yoluyla (bilgisayarın araç olduğu yani normal suçla ilgili delil ihtiva etmesi muhtemel durum) işlenmiş suçlarda delil elde etmek için kullanıldığı bir bilim olmaktan çıkması sonucunu doğurmaktadır. Örneğin adli bilişim bir Hacking olayında hacker şahsın bilgisayarındaki verileri delil niteliğinde inceleyebileceği gibi, belge üzerinde sahtecilik suçunun veya bir cinayetin aydınlatılabilmesi için şüphelinin bilgisayar sistemindeki verileri de dijital delil olarak inceleyebilmektedir. Bunun yanında gerek normal suç olsun gerek bilişim vasıtalı veya bilişim suçu olsun Adli Bilişim Bilimi suçu aydınlatabilmek için şüphelinin cep telefonundaki, dijital fotoğraf makinesindeki, elektronik kişisel yönetim sistemlerindeki (PDA), tablet bilgisayar vs gibi veri taşıması muhtemel elektronik cihazlarında da inceleme yapar. Peki, akla gelebildiğince dijital deliller nerelerde bulunur?

Dijital Delil Nerelerde Bulunur?
Hard diskler, CD, DVD ve Disketlerde

USB Hardisk ve USB Flash Disklerde
ZIP, DAT, DLT gibi teyp veri yedekleme birimlerinde
Hafıza Karlarında (SD, MMS, CF, MemoryStick vs)
Dijital Kameralar ve Fotoğraf Makinelerinde, , MP3 Çalarlarda
El bilgisayarlarında (PDA, PALM, PocketPC, Tablet PC vs)
Cep Telefonlarında ve Akıllı Telefonlarda
Oyun Konsollarında
Akıllı Televizyonlarda
Bazı Yazıcı ve Faks Cihazlarında
Network Cihazlarında (Hafızaları varsa)
İnternet ve Network Ortamlarında (Canlı Akışkan Delil)
Ve daha bir çok…

Bu sayılan listenin haricinde de elbette teknolojinin gelişmesiyle birlikte üzerinde veri taşıyabilecek yeni cihazlar ortaya çıkabilecektir. Yukarıda da belirttiğimiz gibi, üzerinde veri depolama yetisine sahip her türlü cihaz dijital delil ihtiva etme potansiyeline sahiptir. Dijital Delil'in ne olduğunu ve nerelerde bulunduğunu izah ettikten sonra ne tür dijital delillerin (dijital delil verisi) bulunabileceğine değinmek gerekmektedir. Aslında dijital delillerin yani delil niteliği taşıyacak verilerin neler olduğu saymakla bitecek bir şey değildir. Bilişim sistemlerinin ve bilgileri otomatik olarak işleme tabi tutan elektronik cihazların veri depolama birimlerinde suçla ilgili çeşitli varyasyonlarda dijital delil türlerine rastlanılabilir. Saymakla bitmeyecek kadar çok olan dijital delil türlerinden az da olsa bahsetmek gerekirse;

1. Bilgisayar sistemleri veri üniteleri üzerinde bulunması muhtemel dijital delil türleri.

Bilindiği gibi bilgisayar sistemleri günümüzde kişisel kullanımdan sunucu sistemlerine kadar sayılamayacak ölçütte her alana girmiştir. Çeşitli türdeki verileri insanoğlu için işleyen, kayıt altında bulunduran bilgisayar sistemleri ister sunucu hizmeti veren büyük sistemler olsun ister kişisel amaçla kullanılan PC'ler olsun, bir suça ilişkin dijital delil niteliğinde veriler içerebilmektedir. Bu veriler kullanılan sistemin özelliğine ve kullanılan alana göre çeşitli farklılıklar göstermekle birlikte daha önceden de bahsettiğimiz gibi bilgisayar sistemlerinin veri depolama birimleri üzerinde yer almaktadır. Günümüzde her bilgisayarın standart olarak kullandığı olmazsa olmaz veri depolama birimi içerilerinde bulunan hard disklerdir. Bilgisayar sistemleri hard disk veri depolama birimlerinin haricinde CD, DVD, Disket, taşınabilir hard diskler (Usb-FireWire) ve USB flash diskler gibi harici veri depolama birimlerini de artık yoğunlukla kullanmaktadırlar. Genellikle taşınabilir harici veri depolama birimleri; yedekleme veya verilerin nakli amacıyla kullanılırken, özellikle sunucu (hizmet veren büyük ana bilgisayarlar) tipteki bilgisayar sistemleri yedekleme işlemlerini uzun sureli dayanıklılığa ve yüksek kapasitelere sahip yedekleme teyp/kaset/kartuş veri depolama birimleri üzerinde gerçekleştirmektedir. Sunucu sistemlerin yedekleme işlemlerini kısaca ZIP DLT, DAT vs gibi yedekleme üniteleri gerçekleştirmektedir. Aslında bilgisayar sistemlerinin veri depolama birimleri öyle çeşitlidir ki; saymakla bitmeyeceği gibi her gün teknolojiyle birlikte bir başkası çıkmaktadır. Örneğin bir hard disk ünitesinin bile çeşitli ebatlarda, özelliklerde, farklı veri transfer yollarına sahip türleri mevcuttur. Bu çeşitlilik bilgisayar sistemlerinin tüm veri depolama üniteleri için geçerlidir. Bilgisayar sistemlerinin veri depolama birimleri üzerinde ne tür dijital deliller bulunabileceği karşılaşılan suç'a göre değişmektedir. Ancak genel hatlarıyla;

Bilgisayar Hard Diskleri üzerinde:
- Dökümanlar, Kelime işlemci dosyaları, resimler, ses ve video dosyaları
- Veri tabanı dosyaları, veri tabanı erişim kayıtları
- E-Mail veya chat kayıtları, Internet Geçmişi.
- Erişim şifreleri ve kullanıcı adları.
- Silinmiş dosyalar ve silinmiş disk alanları.
- Şifrelenmiş veya Kriptolanmış dosyalar
- Dosya yetkileri ve tarihleri (oluşturma, erişim, silme vs)
- Sistem Kayıt bilgileri (Registery, Event Log vs)
- Sistem tarafından verilen hizmetler
- Virus, Trojan, SpyWare vs gibi zararlı yazılımlar.
- Sistem Üzerinde yüklü yazılımlar
- Sanal Disk alanları ve RAM bilgileri
- Vs…

CD, DVD, Disket ve USB Hard disk ile Fash Disk üzerinde:
- Dökümanlar, Kelime işlemci dosyaları, resimler, ses ve video dosyaları

- Veri tabanı dosyaları, veri tabanı erişim kayıtları
- Şifrelenmiş veya Kriptolanmış dosyalar
- CD ve DVD lerin oluşturulma tarihleri
- USB Hard disk ve Flash disklerde silinmiş dosyalar ile disk alanları.
- Vs.

Bazı bilgisayar işletim sistemleri CD, DVD, Disket ve USB Hardisk veya Flash Diskler üzerinden çalışabilmektedir. Bazı durumlarda özelikle bilişlim suçlarında, şüpheliden elde edilebilecek bu medyalar üzerindeki özel olarak hazırlanmış ve bilişim sistemlerine zarar verme yetisine sahip yazılımlarda delil niteliğini taşıyabilmektedir. CD ve DVD'ler sadece yazılabilir olduklarından bunlar üzerinde çalışan işletim sistemleri tamamen RAM de oluşturulan sanal disk üzerinde çalıştıkları için bilgisayarın kapaması halinde geriye sadece salt okunur CD ve DVD'ler deki bilgiler kalmaktadır. Ancak USB Hard disk ve USB Flash memory üzerinde çalışabilen işletim sistemlerinde medyalar salt okunur olmadıkları için bu medyalar üzerinde bilgisayar hard diskleri üzerinde bulunabilen delil niteliğindeki dijital veriler yer alabilmektedir. Böyle bir durumla karşılaşıldığında, Adli Bilişim uzmanı üzerinde işletim sistemi çalışan USB hard disk veya Flash disklerde de bilgisayar sistemlerinin hard disklerinde uyguladığı inceleme esnasında baktığı verilere de bakmalıdır.

ZIP, DAT, DLT gibi Teyp/Kaset/Kartuş yedekleme üniteleri üzerinde:
- Veri tabanı dosyaları yedekleri
- E-posta sunucu dosyaları yedekleri
- Sistem kayıtlarının yedekleri
- Vs…

Bu tür yedekleme ünitelerinin genellikle sunucu tarzındaki bilgisayar sistemleri tarafından kullanıldığını söylemiştik. Çok büyük veriler tutan ve bu verileri genellikle anabilgisayar şeklinde diğer istemci bilgisayarların hizmetine sunan bilgisayar sistemleri bazı durumlarda yöneticilerinin yedek alma işlemine tabi tutulurlar. Böyle durumlarda verileri uzun süre saklama ve büyük miktarlarda veri saklama kapasitesine sahip bu tarz yedekleme üniteleri kullanılabilir. Genellikle bu üniteler üzerinde sistemler üzerinde bulunan dosyaların veya kayıtların yedekleri bulunmakla birlikte, çoğunlukla yedekler özel yazılımlarla farklı formatlarda sıkıştırılmış halde bulunmaktadırlar.

2. Dijital Kameralar ve Fotoğraf Makineleri, MP3 Çalarlar üzerinde bulunması muhtemel dijital deli türleri.

Günümüzde eski kasetli veya filmli fotoğraf makineleri ile kameraların ve müzik çalarların yerini dijital olanları almış artık bu cihazlarda neredeyse kaset ve film devri ortadan kalkmıştır. Bu yeni dijital cihazlar ya kendi içerilerinde bulunan hafızalarını yada çeşitli ebat ve tipteki ufak taşınabilir hafıza kartlarını fotoğraf, film ve müzik verilerini depolamak için kullanmakta kullanmaktadırlar.

Dijital Kameralar ve Fotoğraf makineleri üzerinde:
- Video, Fotoğraf ve ses kayıtları
- Dijital cihazın tarih ve saatleri
- Hafızalarındaki silinmiş veriler.
- Vs…

Dijital kameralar şayet bilgisayara bağlanabilecek özelliklere sahipse bilgisayar üzerinde buluna veriler bu cihazların hafızalarına gizlenmek üzere atılmış olabilirler. Böyle bir ihtimale karşı yukarıda sayılan verilerden başka verilere bakmak gerekecektir. Yeni teknoloji içeren bazı cihazların içerisinde mini bilgisayar hard diskleri de yer alabilmektedir. Özellikle bu cihazlar çeşitli hafıza kartları kullanabiliyorsa, hafıza kartlarına da bakılmalı ve hatta USB Flash disklerdeki delil olması muhtemel sayılan verilere de bakılmalıdır.

MP3 Çalarlar üzerinde:
- Ses kayıtları
- Olması muhtemel diğer dosyalar
- Silinmiş veriler
- Vs…

Müzik dinlemek için kullanılan MP3 çalarların bir kısmı gerek içerilerinde kendi hafızalarını barındırsın gerekse ek hafıza kartları kullansın birçok mahiyette delil içerebilirler. Şayet bu cihazlar çeşitli hafıza kartları kullanabiliyorlarsa bu hafıza kartları da bilgisayar sistemlerinin Flash disklerinde

olduğu gibi delil içerecek veriler taşıyabilirler. Özellikle MP3 çalarların çoğu flash disk gibi kullanılabildiğinden dolayı inceleme esnasında incelemenin bu doğrultuda geliştirilmesi gerekmektedir.

3. Hafıza Karları (SD, MMS, CF, MemoryStick vs) üzerinde bulunması muhtemel dijital deli türleri.

Aslında bu hafıza kartları bilgisayar sistemleri, dijital kameralar, mp3 çalarlar ve artık cep telefonlarında da kullanıldıklarından dolayı dijital delil elde etmede önemli bir yere sahip veri depolama birimleridir.

SD, MMS, CF, MemoryStick vs üzerinde:
- Ses, Video ve Fotoğraf dosyaları
- Dökümanlar, Kelime işlemci dosyaları
- Küçük veri tabanı dosyaları, veri tabanı erişim kayıtları
- Şifrelenmiş veya Kriptolanmış dosyalar
- USB Hard disk ve Flash disklerde silinmiş dosyalar ile disk alanları.
- Mevcut dosyaların tarihleri
- Vs.

Çok ekstrem durumlarda bazı hafıza kartları da, USB flash disklerde bulunabilen spesifik işletim sistemleri içerebilmektedirler. Böyle durumlarda bilgisayar hard disklerindeki gibi delil elde etmek için ayrıntılı veri araştırılması gerekmektedir. Özellikle Embedded (Gömülü) mini bilgisayar sistemlerinde CF veya SD tarzında veri depolama birimleri kullanılabilmektedir. Buda bu kartların çalıştıkları sistemler üzerinde, hard disk gibi veri depolama ünitesi olarak kullanılması anlamına gelmektedir.

4. El bilgisayarlarının (PDA, PALM, PocketPC vs) ev Cep Telefonlarının üzerinde bulunması muhtemel dijital delil türleri.

El bilgisayarları gün geçtikçe daha da çok yaygınlaşmakta, özellikle iş hayatında yoğun koşuşturmaya sahip insanlar tarafından tercihen kullanılmaktadır. Bu tür cihazlar üzerilerinde ufak ve kendilerine has işletim sistemleri çalıştıran ve veri depolama birimleri olan cihazlardır. Harici ve dahili veri depolama birimlerinde cihazların özelliklerine göre delil niteliği taşıyabilecek çeşitli veriler ihtiva edebilirler.

PDA lar PALM ve POCKETPC lere göre daha az gelişmiş olmakla birlikte POCKETPC cihazlar en yaygın olarak kullanılan Windows işletim sisteminin mobil sürümünü barındıran bir el bilgisayarıdır. PDA lar genellikle data bank seviyesinde fazla gelişmemiş, sadece kısıtlı yazılımlar içeren, üzerlerine yeni yazılımların yüklenmesine izin vermeyen ve mevcut yazılımları ile veri kaydetme yeteneğine sahip cihazlardır. PALM cihazları ise üzerlerinde Windows'un mobil sürümünden farklı olarak geliştirilmiş Palm_Os diye bir işletim sistemi çalıştırmaktadır. PALM ve POCKETPC cihazlar üzerine bilgisayardaki gibi yeni yazılımlar yüklenebilir. Bu cihazların veri depolama birimleri oldukça esnektir ve gelişmeye açık olarak ek hafıza kartları kullanabilirler.

PDA cihazları üzerinde:
- Adres ve telefon bilgileri
- Görev ve Yapılacaklar listesi
- Kişisel notlar, dökümanlar
- E-Posta ve Chat Kayıtları
- Ses kayıtları
- Silinmiş veriler (bazı durumlarda)
- Bilgisayara bağlanabiliyorsa diğer dosyalar
- Vs…

PDA cihazları pek fazla gelişmiş olmadıkları için artık kullanımını yavaş yavaş yitirmekle birlikte, cihazın özelliklerine göre yukarıda sayılan dijital delil niteliğindeki veri listesi Adli Bilişim uzmanının konuya ve cihazı tanımasına göre genişletilebilir.

PALM ve POCKET PC üzerinde:
- Dökümanlar, Kelime işlemci dosyaları, resimler, ses ve video dosyaları
- Küçük veri tabanı dosyaları, veri tabanı erişim kayıtları

- E-Mail veya chat kayıtları, Internet Geçmişi.
- Erişim şifreleri ve kullanıcı adları.
- Silinmiş dosyalar ve silinmiş disk alanları.
- Şifrelenmiş veya Kriptolanmış dosyalar
- Dosya yetkileri ve tarihleri (oluşturma, erişim, silme vs)
- Sistem Kayıt bilgileri (Registery, Temp Log vs)
- Virus, Trojan, SpyWare vs gibi zararlı yazılımlar.
- Sistem Üzerinde yüklü yazılımlar
- Adres ve telefon bilgileri
- Görev ve yapılacaklar listesi
- Cep telefonu mesajları (GSM özelliği varsa)
- SMS kayıtları (Silinmişler dahil)
- GPRS ve GPS erişim logları
- VS…

Özellikle bu cihazlar resmen içerilerinde bir işletim sistemi barındırdıklarından dolayı bilgisayar statüsünde değerlendirilerek Adli Bilişim uzmanı tarafından incelenmelidir. Bu cihazların bazılarının üzerlerinde kablosuz bilgisayar ağlarına erişim modülerlide olduğu için çok rahatlıkla bir bilişim suçu işlemek için kullanılabilirler. Bu doğrultuda bir inceleme gerçekleştirilerek delil niteliğinde dijital verinin aranması sağlıklı olacaktır.

Cep Telefonlarının üzerinde:
- Adres ve Telefon bilgileri
- Kişisel bilgiler, Notlar Ajanda kayıtları
- Mesaj bilgileri, Silinmiş Mesajlar
- Son arama listesi (Cevapsız, arayan, aranan)
- Mobil Internet geçmişi, İnternet Erişim kaydı
- Resim, Video ve Ses kayıtları, Varsa Hafıza kartları
- Vs…

Günümüzde çocukların bile cep telefonu varken cep telefonu olmayan suçlu yoktur diye tahmin edilebilir. Özelikle bilişim suçlarının haricindeki suçlarda cep telefonlarından elde edilebilecek dijital deliller, suç soruşturmalarında suçun bağlantılarının çıkarılması aşamasında oldukça önem arz etmektedir. Cep telefonlarının hafızalarında ve sim kartlarının üzerinde Adli Bilişim bilimi yeni yeni gelişmekle birlikte bilimsel olarak incelemelerin yapılması hali hazırda mümkündür.

4. Oyun Konsolları üzerinde bulunması muhtemel dijital deli türleri.

Bilgisayarlardan önce atari diye bilinen oyun konsollarında oyunlar oynardı 80'li yıllarda gençler. 90 ların ortasında oyun oynama zevki kalitesinden dolayı bilgisayar sistemleri üzerinde yaygınlaştı. Ve sonunda çok kaliteli ses ve neredeyse gerçek zamanlı görüntü hizmeti verebilen oyun konsolları piyasaya çıktı ve oyun meraklıları bilgisayar sistemlerinde oyun oynamaktansa bu oyun konsollarında oyun oynamayı tercih etti. PlaySattion ve XBOX diye tabir edilen bu oyun konsolları o kadar çok gelişti ki içerilerinde bilgisayar sistemlerinde bulunan işlemciler ile veri depolama birimi olan hard diskler yer almaya başladı. Özellikle XBOX gibi cihazlarda bazı modifikasyonlar ile cihazın veri depolama birimi üzerine bilişim camiasında hackerlar tarafından da bir numaralı olarak tercih edilen Linux işletim sistemi yüklenebilmektedir. Böylelikle neredeyse bir PC özelliğini alan oyun konsolları üzerinde neredeyse her türlü suçun dijital delili bulunabilir hale gelmiştir. Adli bilişim uzmanının bilgisi olması dahilinde ilk olay yeri incelemesinde fark edilebilecek oyun konsolları, bilgisiz ve dikkatsiz bir olay yeri incelemesinde gözden kaçabileceği için sağlıklı bir delil elde etme imkanı olmayacaktır.

Modifiye edilmiş Oyun Konsolları Diskleri üzerinde:
- Dökümanlar, Kelime işlemci dosyaları, resimler, ses ve video dosyaları
- Veri tabanı dosyaları, veri tabanı erişim kayıtları
- E-Mail veya chat kayıtları, Internet Geçmişi.
- Erişim şifreleri ve kullanıcı adları.
- Silinmiş dosyalar ve silinmiş disk alanları.
- Şifrelenmiş veya Kriptolanmış dosyalar
- Dosya yetkileri ve tarihleri (oluşturma, erişim, silme vs)
- Sistem Kayıt bilgileri (Registery, Temp Log vs)
- Sistem tarafından verilen hizmetler
- Virus, Trojan, SpyWare vs gibi zararlı yazılımlar.
- Hacking amacıyla kullanılabilecek yazılımlar

- Sistem Üzerinde yüklü yazılımlar
- Sanal Disk alanları ve RAM bilgileri
- Vs…

Modifiye edilmiş bir oyun konsolunda normal bir bilgisayarın içerisinde bulunabilen her türlü dijital delil niteliğindeki verilere rastlamak mümkündür. Yukarıda da bahsedildiği gibi ilk olay yerinde oyun konsollarının fark edilmesi ve sadece oyun için şeklinde düşünüp delil ihtiva edebileceğini düşünmeden göz ardı edilmesi, var olan bir suç soruşturmasında delillerin tam olarak elde edilememesini sağlayacaktır.

5. Yazıcı ve Faks Cihazları üzerinde bulunması muhtemel dijital deli türleri.

Bazı yazıcı ve faks cihazları gelişmiş özelliklere sahiptirler. Üzerlerinde kapasiteleri düşük de olsa veri depolama üniteleri yani hafızaları mevcuttur. Örneğin bazı yazıcılar ve fakslare hafızalarında son işlenen belgelerin kopyalarını, işlenme tarihlerini ve cihazın özelliğine göre daha çok çeşitli bilgileri tutabilirler.

Yazıcılar üzeride:
- Son yazdırılan belgeler
- Yazım tarihi ve adetleri
- Kullanıcı kullanım kayıtları
- Vs…

Faks cihazları üzerinde:
- Son gönderilen belgenin kopyası
- Son alınan belgenin kopyası
- Gönderim ve alım tarihleri saatleri
- Kaç adet gönderim kaç adet alım
- Kayıtlı kullanıcılar
- Vs…

Aslında bu cihazlar pek komplike olmasalar da yinede bazı durumlarda dijital delil elde edilerek suç soruşturmasına yön verebilmektedir.

6. Network cihazları üzerinde bulunması muhtemel dijital delil türleri.

Çoğu network cihazı (router, switch, hardware firewall vs) üzerilerinde network aktivitesi, erişim denetimi ve network konfigürasyonu gibi veriler barındırabilirler. Bu cihazların incelenmesinde Adli Bilişim uzmanı network sistemlerini ileri düzeyde bilmek zorundadır. Aşağıdaki liste genel hatları ile network cihazları üzerlerinde ne tür verilerin bulunabileceğini göstermektedir.

Network cihazları üzerinde:
- Ağın konfigürasyon yapısı
- Erişim ve yönlendirme bilgileri
- Erişim denetim listeleri
- Donanım tabanlı cihaz listeleri (MAC ID)
- Ağ üzerinde oluşmuş bazı arıza bilgileri
- Ağın performans ve kullanım bilgileri
- Ağ üzerindeki yetkisiz erişim bilgileri
- Vs…

Network cihazları üzerinde bulunabilecek veriler yine cihazın özelliklerine göre oldukça farklılık gösterebilmektedir. İncelenmesi yapılacak cihazı tanımak, cihazın fabrika verilerini ve özellikleri bilmek incelemeye başlamadan önce yol haritası çimesi bakımından önemli sayılır.

7. Internet ve Network ortamları üzerinde bulunması muhtemel dijital delil türleri.

İnternet ve Network ortamlarında bilgisayar verileri sürekli olarak akışkanlık sağlamaktadır. Bu ortamlarda da dijital delil elde etmek mümkündür. Ancak bu konu detaylı bir açıklama gerektirdiği için burada şimdilik bahsedilmeyecektir. Kısaca özetlemek gerekirse bilgisayar ortamlarında bulunması muhtemel birçok dijital veri, delil olarak bu ortamlardan elde edilebilir. Bu ortamlardan

elde edilen verilerin delil olarak geçerliliğinin olabilmesi için iyi bir şekilde teknik ten anlaşılabilir seviyeye indirilerek açıklanmaları gerekmektedir.

Buraya kadar anlatılanlarda Adli Bilişim bilimin tanımı ve Adli Bilişim biliminin inceleme hedefi olan Dijital Delil'in tanımı yapılmıştı. Sonrasında dijital delillerin nerelerde bulunabileceğinden bahsedilmiş ve dijital delil verisi ihtiva etmesi muhtemel veri depolama birimlerinin adli bilişim çerçevesinde ne tür veriler içerebileceği hususlarına değinilmeye çalışıldı. Bu çerçevede Adli Bilişim ve Dijital delil kavramlarının anlaşıldığı umut edilerek; Adli Bilişim Biliminin incelemeye yönelik kurallarına ve inceleme uygulanırken inceleme başlangıcından elde edilen delillerin adli makamlara sunulması aşamasına kadar takip edilen adımlarından detayına girmeden bahsedilmeye çalışılacaktır.

Adli Bilişim Biliminin uygulanmasında temel olarak dört önemli adım yer almaktadır. İlk olay yeri müdahalesinden, delillerin var olması muhtemel nesnelerin toplanmasına, karşılaşılan suça göre bir inceleme operasyon planının hazırlanmasından toplanan ve üzerinde delil incelemesi yapılacak veri depolama biriminin bire bir kopyalanmasına kadar olan süreye Elde Etme (Acquisition) adımı adı verilmektedir. Sonraki adım olarak muhtemel suç unsurlarının incelenmesi için yapılan teknik araştırma ve bulunduğu dijital ortamdan çıkarılarak elde edilmesi adımını oluşturan Tanımlama (Identification) yer almaktadır. Teknik incelemenin sonunda Tanımlanan suç unsurlarının delil olarak saptanmasını sağlayan Değerlendirme (Evaluation) aşamasında ise kesin olarak suça konu olan delillerin öz ve mantıklı bir şekilde tespit edilmesi durumu söz konusudur. Son olarak 4.cü adımda, elde edilen delillerin dokümantasyonunun yapılarak adli merciler önüne konulmasını içren Sunum (Presentation) adımı yer almaktadır. Bahsedilen ve aşağıda sıralanan bu adımların sırasıyla düzgün bir şekilde uygulanması Adli Bilişim biliminin vazgeçilmez doğasında yer almaktadır.

Önemli Dört Adım

- **Elde Etme (Acquisition)**
  İlk Olay yeri güvenliği ve müdahalesi, muhtemel delil nesnelerinin toplanması, nakledilmesi, verilerin incelenmek için birebir kopyalanması.
- **Tanımlama (Identification)**
  Araştırma yöntemlerinin belirlenmesi, Teknik araştırmanın yapılarak, muhtemel suç unsurlarının bulundukları dijital ortamdan dışarı çıkarılması.
- **Değerlendirme (Evaluation)**
  Kesin delil niteliği taşıyacak suç unsurlarının tespit edilmesi.
- **Sunum (Presentation)**
  Adli merciler için, saptanan bulguların dokümantasyonun ve sunumunun yapılması.

Elde Etme (Acuisition)

Bilgisayar kriminalistiğinde normal kriminalistik biliminde olduğu gibi ilk olay yeri müdahalesi oldukça önemlidir. Muhtemel suç delillerinin güvenilir bir şekilde eksiksiz saptanması ve zarar görmeden toplanması ilk olay yeri müdahalesinin düzgün yapılmasıyla mümkündür. Bunun için öncelikle olay yeri güvenliği alınarak, bilgisayar kriminalistiği uzmanlarının haricinde herhangi bir üçüncü şahsın delil içermesi muhtemel bilişim sistemleri ve çevrebirimlerinin bulunduğu ortama girmemesi sağlanmalıdır. İlk olay yerinde yetkisiz üçüncü şahısların bulunması bilişim sistemlerinin ve çevrebirimlerinin içermesi muhtemel suç delillerinin kasıtlı veya kasıt dışı zarar görmesine sebep olabilir. Bunun yanında ilk olay yerindeki sahnenin durumu bile bazı durumlarda suç araştırmacısına muhtemel suç ile ilgili bilgiler verebilecektir. Bilişim sistemlerinin fiziki konumu, cihazların birbirleri ile bağlantıları, ağ cihazlarının bağlantı konumları, bilişim sistemlerinin etrafında bulunabilecek dokümanlar ve notlar suç araştırmacısına azda olsa suç ile ilgili bilgi verebilecektir. Olay yerinin güvenliği alındıktan sonra olay yeri sahnesi detaylarıyla fotoğraflanmalıdır. Fotoğraflama sırasında Bilişim sistemlerinin kablo bağlantılarından, açık monitörlerin ekran görüntüleri ile suç araştırmacısına yardımcı olabilecek her tür bulgunun resmedilmesine özen gösterilmelidir. Fotoğraflama aşaması olay yerinde görülen sahnenin detaylı olarak not edilmesiyle yani raporlanmasıyla birlikte desteklenmelidir. Olay yerine ilk müdahaleyi yapan teknik inceleme ekibi delil ihtiva etmesi muhtemel bilişim sistemleri üzerinde parmak izi taramasını muhakkak yaptırmalıdır. Bu özellikle sistemlerin aidiyetini kanıtlama bakımından ileriki aşamalarda önem taşıyacaktır. Özelikle cd'ler bilgisayar klavyesi ve faresi vs gibi ekipmanların üzerindeki parmak izleri aidiyet bilgisini saptamak için önemli bir delildir. İşlenilen suç tipine göre değişmekle birlikte bazı durumlarda bilgisayar ekipmanları üzeride bulunması muhtemel deri döküntüleri, saç telleri de suçun aydınlatılması için önemlidir. Her ne kadar adli bilişim bilgisayar sistemleri konusunda teknik bilgi ve beceri gerektirse de, konu suç olunca suçun aydınlatılması için bu gibi diğer kriminalistik biliminin inceleme aşamalarını da olay yerinde uygulamak yararlı olacaktır. Şu ana kadar ilk olay yeri sahnesi karşılaşma anı ile ilgili olarak

kriminalistik biliminin olay müdahalesinin ilk aşamasından farksız adımlar izlenmektedir. Bu her ne kadar bilgisayar kriminalistiğinde ki teknik bilgi ve beceriyi ortaya koymasa da çoğu durumda muhtemel suç delillerinin zarar görmemesi, suçla ilgili bazı fikirlerin elde edilmesi bakımından önemlidir.

Karşılaşılan olay yerinde kapalı bir bilgisayar sistemi varsa kesinlikle açılmamalıdır. Bilgisayar sistemlerinin delil ihtiva etmesi muhtemel durumlarda, sistemin açılması mevcut delillerin kesinlikle ve kesinlikle zarar görmesine sebebiyet verebilecektir. Örneğin bilgisayar sistemlerinin işletim sistemleri açılırken bir çok konfigürasyon dosyasına erişim sağlamakta ve ileride suç delili olabilecek verilerin zarar görmesine yol açabilmektedir. Dosyaların erişim tarihleri bile bazı durumlarda delil niteliği taşıyabileceği için bu durum oldukça sakıncalıdır. Aynı zamanda işletim sistemlerinin açılırken oluşturabileceği geçici dosyalar ve geçici hafıza disk alanları daha önceden silinmiş olan veri alanlarının üzerine yazılabileceği için silinmiş verilerin delil niteliğinde kurtarılabilme olasılığını ortadan kaldırmış olacak ve dolayısı ile delilin bütünlüğünü bozmuş olacaktır. Bu yüzden incelemesi yapılacak bilgisayar sistemleri ve bazı ağ cihazları kapalı durumda iseler kesinlikle açılmamalıdır.

Olay yerinde çalışan bir bilgisayar sistemi varsa, genel prensip olarak (bazı durumlarda sunucu sistemler hariç) bilgisayar sistemi asla direkt olarak kullanılıp kapatılmamalı, kullanılmamalı ve üzerinde işlem yapılmamalıdır. Delil niteliğini taşıyabilecek bilgisayar sisteminin kullanılması yukarıda bahsedildiği gibi olası delillerin zarar görmesine sebebiyet vereceği için muhtemel delil bütünlüğünün bozulmasına yol açacaktır. İlk başlarda da bahsedildiği üzere bütünlüğü bozulmuş delil, kanun önünde delil niteliği taşımayacaktır. Ayrıca Bilgisayar Kriminalistiği camiasındaki altın kural olan "Asla Şüpheli Bilgisayarı Kullanma ve Şüpheli Bilgisayara Güvenme" kuralı her zaman akılda tutulmalıdır ve buna göre hareket edilmelidir. Unutulmamalıdır ki bazı bilişim suçlarında şüpheliler tarafından tuzak yazılımlar kullanılmış olabilir ve sistem üzerindeki delil niteliği taşıyan veriler sistemin kullanılması sonucunda ortaya çıkabilecek tetiklenme neticesinde tuzak yazılım sayesinde zarar görebilir. Burada akla elbette; peki çalışan sistem üzerinde de olması muhtemel delilleri bilgisayar sistemlerini kullanmadan nasıl elde edeceğiz sorusu gelebilir. Bilgisayar sistemlerinin geçici hafızaları olan RAM'lerde bulunan veriler, çalışan sistem üzerindeki aktif uygulama işlemleri (Process), sistem üzerindeki aktif ağ bağlantıları yada kapıları (ports), aktif kullanıcılar vs gibi sayılabilecek bir çok veri elbette çoğu zaman delil niteliği taşıyabilecektir. Delil bütünlüğünü bozmadan bu tür verileri elde edebilmek için kullanılabilecek çeşitli donanımsal (hardware) ve yazılımsal (software) çözümler mevcuttur. İleri seviyede teknik bilgi ve beceri isteyen böyle durumlarla karşılaşıldığında elde mevcut çözümler ve kabiliyet yok ise, az da olsa delil kaybetmek delil bütünlüğünün bozulmasından bin kat daha iyidir prensibi bilgisayar kriminalistiğinde kabul görmüş bir fikirdir. Delil bütünlüğünün bozulması elde edilebilecek bütün delillerin geçerliliğini ortadan kaldıracaktır. Bu prensibin uygulanmasından önce düşünülmesi gereken; mevcut olayda kaybedilmesi göze alınan delilin suçun aydınlatılmasında ne kadar önem arz edeceğidir. Bu bağlamda tekrar hatırlatmak gerekirse olay yerinde çalışan bir bilgisayar sistemi varsa, bilgisayar sistemleri asla kullanılmamalı ve üzerinde işlem yapılmamalıdır.

Muhtemel delil nesnelerinin toplanması aşamasında akla gelebilecek bir soruda çalışan bilgisayar sistemlerini kullanıp kapatamadıktan sonra nasıl toplayacağız sorusudur. Bura da eğer bilgisayar kriminalistiği uzmanı çeşitli teknik yöntemler kullanarak sistem üzerindeki çalışma anı verilerini delil niteliğinde elde ettiyse ya da, uzman az da olsa delil kaybetmek delil bütünlüğünün bozulmasından bin kat daha iyidir prensibini uygulayarak sistemleri ileriki inceleme aşaması için toplamak istiyorsa, bilgisayar sisteminin işletim sistemine göre değişkenlik gösteren toplama yöntemleri uygulamalıdır. Muhtemel delil nesnelerinin toplanmasından kasıt, delil inceleme için tam teşekküllü bir bilgisayar kriminalistiği laboratuarına götürülmek üzere kanun nezdinde nesnelerin zapt edilmesidir. İncelemesi yapılmak için laboratuar ortamına götürülmesi gereken ve olay yerinde çalışan bir sistemin kapatılması, bilgisayar sisteminin kullandığı işletim sistemine göre değişkenlik göstereceği için aşağıda yer alan prosedürlerin uygulanması genel olarak bilgisayar kriminalistiğinde kabul görmüştür. Genel olarak en az veri kaybına yol açacak şekilde bilimsel olarak belirlenmiş bu prosedürlerde işletim sistemine bağlı olarak ya sistemin elektrik kablosu çekilerek ani kapanması sağlanır ya da normal yollardan kapatılır. Elbette burada bir kesinlik olmamakla birlikte bilgisayar sisteminin verdiği servislere, üzerinde çalışan yazılımlara ve disk yapılarına göre kapatma yönteminde bir kesinlik yoktur. İş yine en az veri kaybının (mümkünse hiç kaybetmemek) yaşanabilmesi ve delil bütünlüğünün bozulmamasını sağlamak bakımından inceleme uzmanının mevcut bilgisayar sistemlerinin donanım özellikleri, yazılım özellikleri, söz konusu işletim sisteminin yapısı vs gibi konularda ileri seviyede bilgi sahibi olmasına bağlıdır. Unutulmamalıdır ki bir bilgisayar kriminalistiği uzmanı her türlü olası sistem ile karşılaşabileceği için, mübalağasız çok fazla teknik bilgi sahibi olmalıdır.

İşletim Sistemi	Kapatma Prosedürü
DOS- Windows 3.1	Ekranı resmini çekin ve çalışan program varsa not edin.Bilgisayarın arkasından elektrik kablosunu çekin.
Windows 95/98/ME	
Windows NT Workstation	
Windows 2000/XP	
Windows NT Server	Ekranı resmini çekin ve çalışan program varsa not edin.Farklı bir durum yoksa normal kapatma yöntemi uygulayın.
Windows 2000 Server	
Windows 2003 Server – Vista	
Unix / Linux / BSD(*Not: Macintosh mimarisindeki bilgisayar sistemlerinde kullanılan MacOS X işletim sistemi de BSD tabanlı bir işletim sistemidir.*)	Ekranı resmini çekin ve çalışan program varsa not edin.Farklı bir durum yoksa normal kapatma yöntemi uygulayın.Eğer sistem üzerinde grafik sunucusu yani X çalışıyorsa konsola geçin ve oradan kapatma işlemine devam edin. Bazı durumlarda sistemi kapatabilmek için sistem yöneticisi root haklarına sahip olmanız gerekir, böyle bir imkan yoksa elektrik kablosu çekilmek zorundadır. Bazı durumlarda ise çalışan servislere göre elektrik kablosu çekilmelidir.

Tabloda listelenmiş genel kapatma prosedürlerine göre bilgisayar sistemlerinin kapatılmasından sonra, muhtemel delil nesnelerinin toplanmasına ve kanun nezdinde inceleme için zapt etme yetkisi alınmış ise toplanan nesnelerin tam teşekkülü bilgisayar kiriminalistiği laboratuarına götürülmesi aşaması yer almaktadır. Ancak bazı durumlarda bilgisayar sistemlerinin zapt edilerek laboratuara inceleme için götürülmesi mümkün olmayabilir. Bu gibi durumlar genellikle mevcut sistemin zapt edilmesi halinde sistemin bulunduğu alanda, sisteme bağlı hizmetlerin aksaması sonucunda ortaya çıkabilecek sorunların mevcut olduğu durumlardır. (Banka sistemleri, büyük bir kuruluşun hizmetinde kullanılan ana sistemler, kamu kuruluşlarındaki bazı hizmet sistemleri vs) İnceleme için laboratuara zapt edilerek götürülecek bilgisayar sistemleri üzerindeki incelemeler, her halükarda delil bütünlüğünü bozmamak için sistemin bire bir alınmış kopyası üzerinde yapılacaktır. İşte bu aşama, şayet sistemin zapt edilerek laboratuara götürülme imkanı bulunmadığı takdir de olay yerinde gerçekleşebilir ve inceleme işlemi için gerekli olan birebir sistemin kopyası bu şekilde alınmış olur. Elbette kanun önünde bu bire bir kopyalama işleminin sistemi zapt etmeden yapıldığına dair geçerli bir tutanak tutularak. Aksi olan her durumda sistemler zapt edilerek inceleme için laboratuara götürülecek, burada incelemede suç ile ilgili delillerin tespit edilmesine yönelik çalışma planı ve yöntemlerin belirlenmesinden sonra alınacak bire bir kopya üzerinde inceleme işlemi başlatılacaktır.

Olay yerinde bulunan dijital delil ihtiva etmesi muhtemel bilgisayar sistemleri ya da veri depolama birimlerinin laboratuara götürülüp inceleme aşamasına başlanması için gerekli olan bire bir kopyalama işlemine geçilmesinden önce; delillerin toparlanması ve laboratuara intikal ettirilirken dikkat edilmesi gereken hususlar mevcuttur. Deliller toplanma, paketlenme ve nakletme sırasında da elbette zarar görme ihtimali içerisindedirler. Özelikle bilgisayar sistemleri ve veri depolama birimleri sarsıntı, statik elektrik, yüksek seviyedeki radyo frekansı, ısı, nem ve bir çok dış etkenden etkilenerek zarar görebilmekte, ya inceleme aşamasına geçilmeden bozulabilmekte ya da inceleme aşamasında çıkabilecek teknik arızalar yüzünden delil elde edilme imkanı ortadan kalkmış olmaktadır. Bu aşamada mevcut olay yerindeki diğer işlemler (güvenliğin alınması, fotoğraflama, normal delil elde etme prosedürleri ve çalışan sistemlerin durdurulması gibi) tamamlandıktan sonra delil ihtiva etmesi muhtemel varlıkların dikkatli bir şekilde toparlanması gerekmektedir. Mümkün mertebe manyetik alanlardan ve statik elektrikten etkilenmeyecek şekilde anti statik paketleme gerçekleştirilmeli, sistemler ile veri depolama birimleri sarsıntıdan korunarak nazikçe inceleme laboratuarına götürülmelidir. Elbette alınan tüm varlıkların birer listesi çıkartılmalı, zapt edilmenin hukuksallık kazandırılmasına dikkat edilmelidir.

Delil ihtiva etmesi muhtemel bilgisayar sistemleri üzerindeki incelemeler, sistemin veri depolama birimlerinin birebir alınmış kopyaları üzerinde gerçekleştirilmelidir. İnceleme için alınan birebir kopyaya bilgisayar kriminalistiği'de İmaj (Forensic Image) adı verilmektedir. Bu birebir kopya yani İmaj alma işlemi, incelemeye tabi hedef sistem üzerindeki verilerin bit bazında düşük seviyede kopyalanması ile gerçekleştirilmelidir. Sistem üzerindeki verilerin sektör sektör birebir yansısının alınması yani düşük seviyede kopyalanması ancak geçerli bir imajın alınması anlamına gelmektedir. Çeşitli kopyalama yazılımları ile yapılan kopyalarda sadece sistem üzerinde var olan dosyalar kopyalama işlemine tabi tutulduğu için geçerli bir imaj alma söz konusu değildir. Düşük seviye bit bazında kopyalamada sistem üzerinde veri depolama biriminin sektör bazında yansısı alındığı için, veri depolama birimi üzerindeki boş veri alanları, silinmiş veri alanları ve disk yapısı olduğu gibi

klonlanmaktadır. Partition Imager ve Norton Ghost gibi sistemin yedeğini almaya yarayan imaj alma çözümleri; sistem üzerindeki veri depolama birimlerini sadece açılış kaydı, bölümleme tablosu, dosya sistemi tablosu ve mevcut dosyalar bazında klonladığı için, sistem üzerinde bulunan ama dosyaların bulunmadığı alanları kopyalamamaktadır. Bu da ister istemez silinmiş verilerin yer alması muhtemel boş disk alanların kaybına yani inceleme aşamasında delil kaybına yol açacaktır. Bu bağlamda dijital delil incelemek için gerekli olan imaj alma işlemini gerçekleştirmek üzere çeşitli özel yöntemler, yazılımsal ve donanımsal çözümler kullanmak gerekecektir. Sistem üzerindeki veri depolama biriminin bit bazında birebir imajının alınmasında dikkat edilmesi gereken bir başka nokta da; imajı alınacak asıl veri depolama biriminin imaj alma sırasında zarar görmesini engellemektir. İmajı alınacak bilgisayar sistemi kesinlikle normal yollardan açılmamalı sistemin üzerindeki işletim sisteminin başlatılmasına izin verilmemeli, sistem üzerindeki veri depolama birimi sökülüp yazma koruması olmayan bir başka sisteme takılarak kopyası alınmamalıdır. Daha öncede bahsedildiği gibi işletim sistemleri açılırken bir çok konfigürasyon dosyasına erişim sağlamakta ve ileride suç delili olabilecek verilerin zarar görmesine yol açabilmektedir. Aynı şekilde delil nesnesi olan bilgisayar sisteminin veri depolama birimi başka bir sisteme takıldığında, o sistem üzerinde takılan veri depolama birimine yazma koruması uygulayan donanımsal veya yazılımsal bir koruma yoksa delil niteliği taşıyan veriler zarar görme ihtimali ile karşı karşıyadır. Örneğin bu şekilde başka bir sisteme takılan veri depolama birimi üzerinde bulunan her hangi bir dosyaya erişilmesi o dosyanın ileride belki delil olabilecek erişim tarihinin değişmesine sebep olabilecektir. Yine özel olarak tasarlanmamış açılış CD'leri veya disketleri ile sistemin açılışı gerçekleştirildiğinde aynı sorun ortaya çıkmaktadır. Bunun için ya donanımsal seviyede delil ihtiva etmesi muhtemel veri depolama birimine yazma koruması önlemini alabilecek bir çözüm kullanılmalı ya da özel olarak veri depolama birimine yazılımsal bağlamda açılış sırasında erişimi engelleyecek bir çözüm kullanılmalıdır.

Hedef sistemin delil bütünlüğünün bozulmaması için gerekli olan bu önlemler alındıktan sonra imaj alma işlemi gerçekleşmelidir. Zaten birebir olarak alınacak İmaj üzerindeki inceleme de, kesinlikle ve kesinlikle gerçek delil nesnesinin inceleme aşamasında zarar görmemesi için gerekli bir işlemdir. Aşağıda çeşitli yazma koruma çözümleri ve imaj alma çözümleri yer almaktadır. Bu çözümlerden yazılımsal olan çözümler çoğunlukla dijital delil inceleme yazılımlarını da içermektedir.

Bazı Yazılımsal Ürünler	
ÜRÜN	**AÇIKLAMA**
EnCase Boot Disk/CD EnCase www.guidancesoftware.com	Yazılımsal yazma koruma, imaj alma ve dijital delil inceleme yazılımı. FBI dahil bir çok polis teşkilat tarafından tercih edilen ve sıklıkla kullanılan bilgisayar kriminalistiği yazlımıdır.
FTK Imager Forensic Toolkit®(FTK™) www.accessdata.com	FTK komple bir bilgisayar kriminalistiği yazılımıdır. Oldukça güçlü özellikleri ile EnCase yazılımını aratmamaktadır. FTK Imager sayesinde yazma koruma tedbiri alınarak Imaj alma işlemi gerçekleştirilebilir.
IXimager ILook Investigator www.ilook-forensics.org	ILook IXimager yazılımı vasıtası ile yazılımsal yazma koruma tedbiri alınarak imaj alma işlemi gerekleştirilebilir. IXImager Linux tabanlı yazılımsal bir çözümdür. ILook Investigator yazılımı ise çok kuvvetli bir bilgisayar kriminalistiği yazılımıdır. ILook bedava bir yazılım olmakla birlikte sadece belirli şartlar ispat edildiği müddetçe kamusal kurum çalışanlarına (polis, asker, adli görevli) dağıtılmaktadır.
Forensic Replicator Paraben Forensic Tools www.paraben-forensics.com	Forensic Replicator Paraben Forensics Software tarafından sunulan yazılımsal bir imaj alma çözümüdür. Paraben firmasının dijital delil incelemeye yönelik yazılımları ve yazma koruma donanımları mevcuttur.
Linux – dd ve diğerleri www.opensourceforensics.org	Linux işletim sistemi (özellikle live dist) üzerindeki dd aracı kullanılarak da bir veri depolama biriminin raw imajı alınabilir. dd aracının aldığı imajı EnCase, ILook ve FTK dahil bir çok dijital delil inceleme yazılımı okuyabilmektedir.

	Linux doğası itibariyle mount (bağlanmayan) edilmeyen hiçbir veri depolama biriminde yazma bağlamında erişmemektedir. Dolayısıyla imaj alma ve işlemi yazma korumalı olarak gerçekleştirilebilir. Hali hazırda Linux işletim sistemi üzerinde bulunan bir çok yazılımla bilgisayar kriminalistiği araştırmaları gerçekleştirilebilir.

Bazı Donanımsal Ürünler	
ÜRÜN	**AÇIKLAMA**
Digital Intelligence Tools ULTRABLOCK FORENSIC CARD READERS ULTRABLOCK USB WRITE BLOCKER ULTRABLOCK IDE, SATA AND SCSI HARDCOPY www.digitalintelligence.com	Digital Intelligence firması bilgisayar kiriminalistiği alanında dijital delil inceleme ve elde etme cihazları üreten en büyük ve en eski firmalardan bir tanesidir. Burada bir çok farklı kullanım amacıyla donanımsal yazma koruma çözümü bulunabileceği gibi, başlı başına bilgisayar kriminalistiği için özel olarak tasarlanmış bilgisayar sistemleri de bunmaktadır. Her türlü veri depolama birimi için özel olarak üretilmiş inceleme ve imaj alma donanımları Digital İntelligence firması bünyesinde mevcuttur.
Image Master Solo Drive Lock Disk Jockey IT www.ics-iq.com	Image Master Solo cihazı o kadar mükemmel bir imaj alma donanımıdır ki üzerinde hiçbir imaj alma donanımını taşımadığı özellikleri taşımaktadır. (Hash alma, bire bir kopyalamanın haricinde çeşitli sıkıştırma algoritmaları kullanma vs.) Firmanın daha bir çok çeşit ürünü mevcut. Drive Lock ise sadece yazma koruması için olan bir ürün olmakla birlikte Disk Jocket IT nin kullanışlılığına sitesinden bakılabilir.
Forensic Computers Write Blockers Imagers Forensic Workstations Forensic Air Lite Series Tableu T335 www.forensic-computers.com	Forensic Computers firması Virginya'da bulunan ve Türk Emniyet teşkilatına ilk olarak bilgisayar kriminalistiği cihazlarının temin edildiği kaliteli bir firmadır. Digital Intelligence firması bu firmadan kopmuş ancak US Hava kuvvetlerinin ve FBI'ın desteğini almasıyla birlikte pazar payında en büyük pastayı kapmıştır. Sitesini ve üretim yaptığı donanımları özenle incelemek yararlı olacaktır.
LCTECHNOLOGY Drag 2000 Drag 1500 Mini Drag P-Drag www.lc-tech.com	Genellikle hazır dijital delil inceleme sistemleri üreten firmanın ürünleri oldukça kullanışlıdır. Dijital Delil inceleme alanında Avrupa birliğinde en çok kullanılan ancak bu alanda ABD'deki sistemleri örnek alan firmanın ürünleri bazı durumlarda yetersiz kalabilmektedir.

Tanımlama (Identification)

Elde Etme (Acuisition) aşamasına müteakip birebir kopyası yani imajı alınan bilgisayar sistemi veri depolama birimleri üzerinde incelemeye geçilmeden önce karşılaşılan suça ilişkin araştırma yöntemleri tespit edilmeli bir inceleme planı ortaya çıkarılmalıdır. Burada amaç suça ilişkin ne tür verilerin araştırılacağının saptanmasıdır. Araştırılacak veriler karşılaşılan suça ve suç ile ilgili verilerin bulunduğu veri depolama birimlerine göre değişiklik gösterebilmektedir. Aşağıdaki tabloda örnek olarak bilgisayar vasıtalı bir suç olan çocuk pornografisinin muhtemel delil medyası hafıza kartları üzerindeki özet araştırma yöntemi gösterilmiştir.

SUÇ: Çocuk Pornografisi	**Medya: Hafıza Kartları**
Chat Kayıları,	Yedeklenmiş veya Sıkıştırılmış dosyalar,
E-Postalar, Notlar,	Silinmiş veriler ve dosyalar,
Resim, Animasyon ve Video Dosyaları	Disk Bölümleri veya Formatlanmış alanlar,
İlgili Oyunlar,	Şifreli Disk alanları,
Sık Kullanılan Internet İmgeleri,	Gizlenmiş dosyalar ve alanlar,
Resim İşleme Yazılımları,	Belirlenmemiş Alan ve Slack Space
Vs…	Vs…

Bunun dışında bilgisayar sistemlerinin hedef olduğu bir bilişim suçunda araştırma planın iyi bir şekilde yapılması gerekmektedir. Bilişim Suçları bilgisayar vasıtalı suçlardan daha karmaşık bir yapıya sahip oldugu için elbetteki araştırma yöntemlerinin belirlenmesi daha fazla teknik bilgi birikimi gerektirecektir.

Araştırma yöntemlerinin belirlenmesi ve karşılaşılan suç ile ilgili ne tür bilgilerin hedef dijital delil nesnesi üzerinde araştırılacağının belirlenmesinden sonra teknik araştırma detaylı bir şekilde dijital delil inceleme yazılımlarının desteğiyle yapılmalıdır. Burada bu konuya çok detaylı bir içeriğe sahip olmasından dolayı pek fazla değinilmeyecektir. Ancak ülkemizde kolluk kuvvetleri tarafından sık olarak kullanılan ve beynelminel dijital delil inceleme yazılımları olan EnCase ve FTK yazılımları bu iş için biçilmiş kaftandır. Bunun yanında bilişim sistemlerinin işleyişi hakkıda teknik bilgi birikimi az olan bir kullanıcı bu yazılmlar ile yüzde yüz bir inceleme gerçekleştiremeyecek sadece bu yazılımların menulerinde sunulmuş basit işlemleri gerçekleştirebileceklerdir. Unutulmamalıdır ki; bu yazılımların menülerini çok iyi bilmek asla ve asla iyi bir dijital delil inceleme yapmak ve iyi bir adli bilişim uzamanı olunduğu anlamına gelmemektedir.

Değerlendirme (Evaluation)

Değerlendirme aşamasında bulunan bulguların hangilerinin kesin delil niteliğinde Adli merciler karşısına çıkarılacağının tespiti yapılmaktadır. Burada dikkat edilmesi gereken husus soruşturmaya yön verecek bilgilerin eksiksiz bir şekilde sunum aşaması için tespit edilmesidir. Örneğin delil niteliği taşımayacan normal bilgisayar dökümanları veya dosyaları (işletim sistemi yardım dosyaları yada kişisel eglence amaçlı dosyalar vs vs) elimine edilerek delil şeklinde değerlendirilmemelidir. Dijital delil ihtiva etmesi muhtemel medya üzerinde bulunan tüm verilerin delil niteliğinde düşünülüp sunum aşaması için hazırlanması elbetteki cok aşırı zaman alacak ve tüm verilerin delil katagörisinde değerlendirilmeside mümkün olmayacağı gibi adli mercilerin iş gücünü kırarak kafaları karıştıracaktır. Burada amaç en doğru ve suçu aydınlatacak verilerin delil olarak dışarıya çılarılması ve roparlama aşamasına hazır hale getirilmesidir.

Ayrıca elde edilen delil niteliğindeki verilerin güvenli bir şekilde zarar görmeden ve bire bir değişmemiş halinin inceleme konusu ortamdan çıkarılmış olup olmadığının kontrolü de bu aşamada dikkatlice baştan sona denetlenmelidir. Bu aşama aynı zamanda bir nevi adli bilişim biliminin söz konusu olay ile ilgili kurallarına uygun olarak yapılıp yapılmadığının da kontrolü

yapılmaktadır. **KISACA :** Doğru ve öz veriler, bütünlüğü bozulmadan ve anlaşılabilir ölçüde suçu aydınlatacak şekilde delil olarak ortaya konulmalıdır.

Sunum (Presentation)

Adli Bilişim Biliminin son aşaması olan Sunum kısmında; elde edilen ve değerlendirilmesi tamamlanmış dijital delil niteliğindeki verilerin soruşturmada kullanılmak üzere anlaşılabilir bir dilde raporlanması ve Adli Makamlara ayrıntılı, anlaşılabilir ve teknik bilgileri açıklayıcı bir şekilde sunulması gerekmektedir. Sunum aşamasında hazırlanacak rapor ile ilgili aşağıdaki hususlara dikkat edilmesi gerekmektedir.

- Raporun dili ve İçeriği teknik bilgisi olmayan insanlar tarafından bile anlaşılabilir olmalıdır.
- Teknik terimler ve olgular detayları ile açıklanmalıdır.
- Rapor içerisinde delil niteliğini taşıyacak Kesin ve Somut veriler yer almalıdır.
- Delilere ulaşmak için kullanılan adli bilişim yöntemleri açıklanmalıdır.
- Delil Bütünlüğü bozulmadan delillerin ortaya konduğu ispat edilmelidir.
- İnceleme aşamasındaki yapılan tüm işlemler ek bir rapor hazırlanarak ayrıca rapor edilmelidir.

Şu anada kadar anlatılanlarda bilişim suçlarında ve bilgisayar bağlantılı suçlarda, suça konu olabilecek bilişim sistemleri medyaları üzerinde bulunması muhtemel dijital delillerin tespiti amacıyla uygulanan Adli Bilişim (Computer Forensics - Bilgisayar Kriminalistiği) biliminin ana hatlarıyla temellerinden bahsedilmiştir. Bu konuda ilerleyen zamanlarda elimden geldiğince bölümlere ayırarak daha detaylı bilgi vermeye çalışacağım. Internet üzerinde bu konuda yapılacak aramalar neticesinde oldukça faydalı başka bilgilerde bulunabilecektir. Unutulmamalıdır ki adli bilişim bilimsel temellere dayanan, prensipleri olan ve uygulayıcının bilgi seviyesiyle orantılı olarak verimli bir şekilde kullanılabilecek bilgisayar kriminalistiği bilimidir.

Ahmet Hakan EKİZER

Kaynaklar

http://en.wikipedia.org/wiki/Computer_forensics
http://www.forensicfocus.com/
Computer Forensics: Principles and Practices (Prentice Hall Security Series) by Linda Volonino, Reynaldo Anzaldua, Jana Godwin
Computer Evidence: Collection & Preservation (Networking Series) by Christopher LT Brown
Real Digital Forensics: Computer Security and Incident Response by Keith J. Jones, Richard Bejtlich, Curtis W. Rose
Electronic Crime Scene Investigation: A Guide for First Responders, by National Institute of Justice