Adlî Bilişim - 3

ADLİ BİLİŞİMDE DELİLLERE ULAŞMA

- **Adli Bilişim Safhaları**
- Elektronik delillerin klasik delillerden farklı özellikler taşıması, delillere ulaşma konusunda da bazı farklılıklar ortaya çıkarmaktadır. Örneğin, bir cinayet vakasında, olay mahallinde bulunan tabanca, kuvvetle muhtemeldir ki suça ilişkin bir delildir. Bu tabanca muhafaza altına alınarak, gerekli incelemelerin yapılması için götürülür. Oysa ki dijital delillerde durum bundan çok farklıdır. Öncelikle, muhafaza altına alınan bir elektronik aygıt içerisinde suça ilişkin delil bulunup-bulunmadığı belli değildir. Örneğin, suç mahallinde bulunan bir bilgisayar. Bu bilgisayarın suçta kullanılıp-kullanılmadığı veyahut suça ilişkin bir delil ihtiva edip-etmediği belli değildir. Şüphesiz ki, tabanca örneğinde de suça ilişkin kesin bir belirginlik yoktur. Ancak ortamda bulunan bilgisayar -yahut bir başka elektronik aygıt- konusunda bu belirsizlik çok daha fazladır.

ADLİ BİLİŞİMDE DELİLLERE ULAŞMA

- **Adli Bilişim Safhaları**
- Muhafaza altına alınarak incelemeye başlanmış bir klasik delil, çeşitli analizlerden sonra çözülür ve nitelendirilir. Ancak elektronik delillerde bu işlem o kadar basit ve kolay olmamaktadır. Adli bilişimde delilin incelenmesi, nitelendirilmesi ve analizi klasik delillere kıyasla daha karmaşık, çok daha teknik ve oldukça pahalı bir işlemdir.

ADLİ BİLİŞİMDE DELİLLERE ULAŞMA

- **Adli Bilişim Safhaları**
- Adli bilişimde elektronik bulgunun, bir hukuki delile dönüştürülme süreci belli prosedürleri takip eder. Uygulanan bu prosedürlerden sonradır ki dijital delil, kendisini bir hukuki delil olarak ortaya koyar. İşte bu prosedüre, *adli bilişim safhaları* diyoruz. Adli bilişim safhaları, bazı yazarlarca dört tane olarak sayılırken; bazı yazarlar ise, bu aşamaları beşe ayırarak incelemektedir. Kimi kaynaklar ise, adli bilişim safhalarına bir de henüz delillere ulaşılmamış olduğu, hazırlık aşamasını da ayrı bir başlık halinde incelemektedir.

ADLİ BİLİŞİMDE DELİLLERE ULAŞMA

- **Adli Bilişim Safhaları**
- Şüphesiz ki, delillerin elde edilip incelemeye başlanmasına kadar olan yapılan hazırlık işlemleri de vardır.
- Toplama (*Collection*)
- İnceleme (*Examination*)
- Çözümleme (*Analysis*)
- Raporlama (*Reporting)*

ADLİ BİLİŞİMDE DELİLLERE ULAŞMA

- **Toplama (Elde Etme) (*Collection*)**
- Toplama, delillerin elde edilmesidir. Öncelikle, delillerin toplanmaya başlanılabilmesi için yasal durumun mevcut olması gerekir. Bu da ancak usulüne uygun olarak verilmiş bir arama kararı veyahut CMK m. 116 gereğince şüphe üzerine arama ile mümkündür. Yasal prosedürün eksiksiz olarak yerine getirilmesi, delillerin hukuka uygunluğu noktasında önem taşımaktadır.
- Toplama aşamasında olay yeri öne çıkmaktadır. İçerisinde delilerin bulunduğu mekân, olay yeridir. Delilerin sağlıklı biçimde toplanabilmesi, olay yerine yapılan ilk müdahalenin ne kadar sağlıklı olduğuna bağlıdır.

ADLİ BİLİŞİMDE DELİLLERE ULAŞMA

- **Toplama (Elde Etme) (*Collection*)**
- Toplama aşaması, klasik suçlarda olduğu gibi kolluğun olay mahalline intikaliyle başlar. Yine klasik suçlarda olduğu gibi olay mahallinin güvenliğinin sağlanması, yetkisiz kişilerin olay yerinden çıkarılması gibi uygulamaların derhal yerine getirilmesi çok önemlidir. Olay yerinde bulunan elektronik aygıtların durumlarının sağlıklı bir biçimde korunabilmesi ancak bu sayede sağlanabilir.
- Olay yerine yetkisiz kişilerin girmemesi temin edildikten sonra, mümkünse bir adli bilişim uzmanının olay yerine getirilerek, delil toplama işinin ona bırakılması gerekir. Esasen elektronik delilerin, klasik delillerden farklı yapısı bunu zorunlu kılmaktadır. Ancak bir adli bilişim uzmanı, delil kaybı yaratmaksızın -ya da mümkün olan minimum kayıpla- dijital delilleri toplayabilecektir.

ADLİ BİLİŞİMDE DELİLLERE ULAŞMA

- **Toplama (Elde Etme) (*Collection*)**
- Ancak olay yerinde dijital delillerden farklı olarak klasik suç delillerinin yer alması da kuvvetle muhtemeldir. Özellikle söz konusu bir bilgisayar olunca, klavye ve fare (mouse) üzerinde bulunabilecek parmak izleri, mahalde bulunan şüpheliye ait giysiler, eşyalar vb. unsurlar da birer delildir. Bu aşamada kriminalistik inceleme de ihmal edilmemelidir. Fakat bu, hassasiyet gerektiren potansiyel dijital delillere zarar vermeden yapılmalıdır. Örneğin bir CD üzerinde yapılacak parmak izi araştırması, kullanılan kimyasallar nedeniyle CD'nin içerisindeki bilgilerin kaybını doğurabilecektir. Bu nedenle kriminal veri toplama ile adli bilişim verileri toplama arasında makul bir denge tutturulmalıdır.

ADLİ BİLİŞİMDE DELİLLERE ULAŞMA

- **Toplama (Elde Etme) (*Collection*)**
- Öncelikle olay yeri fotoğraflanmalı, ortamda bulunan bilgisayar, yazıcı ve diğer donanım aygıtlarının konumları belirtilecek şekilde notlar ve krokiler hazırlanmalıdır. Özetle, bu aşamaya kadar uygulanan yöntemler açısından, kriminalistik ile adli bilişim yöntemlerinin bir arada yürütüldüğünü söylemek mümkündür.

ADLİ BİLİŞİMDE DELİLLERE ULAŞMA

- **Toplama (Elde Etme) (*Collection*)**
- Kriminal inceleme yürütülürken elektronik deliller de toplanmalı, bunun için öncelikle delillerin nerede ve hangi formatta olduğu, nasıl depolandığı tespit edilmelidir.
- Sonrasında, ortamda bulunan elektronik donanımların çalışma biçimleri ve birbirlerine bağlılıkları tespit edilerek buna göre hareket edilir. Örneğin, olay yerinde kapalı konumda bulunan bir bilgisayar varsa kesinlikle açılmamalı; açık bir bilgisayar ise kesinlikle doğrudan kapatılmamalıdır. Bilgisayarın açılması halinde işletim sistemi çalışacak ve bilgisayar verileri işlemeye başlayacaktır. Bunun sonucu ise, verilerin üzerine yeniden veri yazılması ve potansiyel delillerin kaybı olabilecektir. Bilgisayar açık ise kesinlikle hiçbir program çalıştırılmamalı, hatta bilgisayar kapatılmamalıdır. Herhangi bir programın çalışması, bir potansiyel delilin kaybı anlamına gelebilir. Bilgisayar çalışıyor konumda fakat ekranı siyah ise, ekranın açık olup olmadığı kontrol edilmeli, sonrasında fare (mouse) oynatılarak görüntünün gelmesi sağlanmalıdır.
- Çalışmakta olan bir bilgisayar içindeki delillere ulaşma, verileri kurtarma gibi işlemlerin yapılabilmesi, doğal olarak o anda ve olay yerinde mümkün olamayacaktır. Bunun için bilgisayarın muhafaza altına alınması ve götürülmesi gereklidir. Ancak kapatılması dahi veri kaybına yol açabilecek bir donanımın götürülmesi nasıl olacaktır? Bu durumda öncelikle bilgisayar üzerinde bulunan ve çalışma konumundan çıkınca yok olabilecek tüm bulgular tespit edilerek belirlenmeli, kesinlikle ekran görüntüsü fotoğraflanmalı, çalışan programlar varsa not edilmeli ve bilgisayar kapatılmayarak, arkadaki güç kablosu çekilmelidir.
- Bunun yapılması belki birtakım verilerin kaybına yol açabilecekse de, delillerin bütünlüğünün bozulmasının önüne geçecektir. Delillerin tümünün kaybındansa, az miktar verinin kaybı daha tercih edilir bir durumdur. Kaldı ki bilgisayardaki tüm delillere adli bilişim uzmanlarınca ve laboratuar ortamında çeşitli analizler yapılmaksızın ulaşılması çok olası bir durum değildir.

ADLİ BİLİŞİMDE DELİLLERE ULAŞMA

- **Toplama (Elde Etme) (*Collection*)**
- Bilgisayarların muhafaza altına alınarak incelenmek üzere laboratuarlara götürülmesi de oldukça dikkat ve özen gerektirmektedir. Donanım araçlarının hassas yapısı gereği, dikkatlice paketlenmesi ve yine aynı dikkatle taşınması şarttır. Sarsıntı, elektrik akımları, elektromanyetik ortamlar, aşırı sıcak ya da sıvı maddelerle teması, bu aygıtların işlevini yitirmesine neden olacaktır ki bu da potansiyel delillerin kaybıdır. Ayrıca paketlemenin, statik elektrikten ve manyetik alanlardan etkilenmeyecek biçimde yapılması da gerekmektedir.
- Delil araştırma amaçlı olarak yapılacak incelemeler, donanımlar üzerinde değil, alınan kopyaları üzerinde yapılacaktır. Bu, donanımlar içerisindeki verilerin kaybını önleyecektir. Bu nedenle aygıtlardaki verilerin sağlıklı kopyalarının alınması çok önemlidir. Adli bilişimde yapılan birebir kopyalama işlemine **imaj** (*forensic image*) denilmektedir. Bu kopyalama, sistemdeki tüm verilerin buna özel yazılımlar kullanmak suretiyle ve düşük seviye bit bazında başka bir ortamda bir örneğinin (imajının / görüntüsünün) oluşturulması suretiyle yapılır. Düşük seviye bit bazında kopyalama yapılmasının önemi, daha sonraki incelemelerde silinmiş, değiştirilmiş, deforme edilmiş verilere de ulaşma olanağını vermesidir.

ADLİ BİLİŞİMDE DELİLLERE ULAŞMA

- **Toplama (Elde Etme) (*Collection*)**
- İmaj alma işleminde dikkat edilmesi gereken önemli bir başka husus da, kopyaların alınacağı sistemin -örneğin bilgisayarın- doğrudan çalıştırılmaması gerektiğidir. Bilgisayarın açılması, işletim sisteminin de çalışmasına bağlı olarak yeni veriler işlerken önceki verilerin kaybı sonucunu doğurabilecektir. Bu nedenle bilgisayarın diskinin sökülüp yazma korumalı bulunmayan bir başka sistem içerisine yerleştirilmeli ve imaj alma işlemi bu biçimde gerçekleştirilmelidir.

- Hangi donanım aygıtı ve hangi modeli için ne tür bir yazılım kullanılacağı, hangi prosedürlerin izleneceği iyi bilinmelidir. Her donanım türü için farklı bir yöntem izlenmesi gerekecektir. Bu nedenle adli bilişim uzmanının, delil kaybını mümkün olan minimum düzeye indirmek için gerekli olan bilgiye sahip olması çok önemlidir.

ADLİ BİLİŞİMDE DELİLLERE ULAŞMA

- **İnceleme (Tanımlama) (*Examination*)**
- Toplama safhasının, imaj alma işlemi ile sona ermesinden sonra inceleme aşaması başlar. İmajın alınmasından sonra artık işin teknik yönü, bu aşamada biraz geride kalmıştır. Bu safhada elimizde birtakım bulgular vardır. Bunların bazıları görünmekte, bazıları henüz görünmemektedir. Görünmeyen bulgulardan kasıt, gizli ve silinmiş dosyalardır. İşte inceleme ile tüm bu bulgular üzerinde çeşitli işlemler yapılarak olası suç unsurları ortaya konacaktır. Yani inceleme safhası özetle, imajı alınmış verilerin gözle görünür biçime getirilme sürecidir.
- İnceleme aşaması sonucunda her türlü veri ortaya konmuş olacaktır. Örneğin; fotoğraflar, grafik dosyaları, videolar, çeşitli yazı dökümanları (word, excell, openoffice vb.), konuşma kayıtları (chat, MSN, GTalk vb.), e-postalar, ziyaret edilmiş ve sık kullanılan web siteleri, sıkıştırılmış dosya ve klasörler, şifreli dizinler, silinmiş dosya ve klasörler, dosyaların oluşturulma, değiştirilme ve erişim tarih kayıtları ilk başta akla gelen ve de en sık rastlanan hususlar olarak sayılabilir.

ADLİ BİLİŞİMDE DELİLLERE ULAŞMA

- **İnceleme (Tanımlama) (*Examination*)**
- Bu aşamada da birtakım yazılımlar kullanılmaktadır. Bu yazılımlara da, ülkemizde de kolluk tarafından kullanılan *EnCase* ve *FTK* örnek olarak verilebilir.

ADLİ BİLİŞİMDE DELİLLERE ULAŞMA

- **Çözümleme (Değerlendirme / Analiz) (*Analysis*)**
- Sistemden imajı alınmış verilerin tümünün gözle görünür hale getirilmesinden sonra analiz aşamasına geçilecektir. Bu aşamada, elde edilen verilerin hangilerinin ve ne ölçüde adli makamlara sunulmak üzere raporlanacağının tespiti yapılmaktadır.
- Bu safhanın bir tür ayıklama aşaması olduğunu söylemek yanlış olmayacaktır. Tüm ilgisiz dosyalar bu değerlendirme aşamasında elenecek, raporlama aşamasına geçilmeyecektir. Ancak işe yarayabileceği düşünülen bulgular, elde ediliş metodlarını da ayrıntılarıyla anlatan tutanaklarla teslim edilecektir.

ADLİ BİLİŞİMDE DELİLLERE ULAŞMA

- **Raporlama (Sunum) (*Reporting*)**
- Dijital deliller toplanmış, inceleme ve analiz aşamalarından geçmiş ve artık adli bilişimin son safhası olan raporlamaya gelinmiştir. Bundan sonra yapılacak olan, hangi bulguların o soruşturma açısından kullanılabilir olduğunun belirlenerek adli makamlara sunulmasıdır.
- Bu yönüyle raporlama safhası, hukuki bir değerlendirmeyi içermektedir. Ancak burada başka bir soru akla gelmektedir: Bu hukuki değerlendirmeyi kim yapacaktır? Bu değerlendirmeyi artık adli bilişim uzmanı değil, kolluk yapacaktır. Adli bilişim uzman(lar)ının inceleme aşamasından geçmiş verilerden hangilerinin delil olabileceği, o suç için kullanılabilir nitelikte olduğu soruşturmada görevli kolluk tarafından değerlendirilecek ve adli makamlara sunulacaktır.

ADLİ BİLİŞİMDE DELİLLERE ULAŞMA

- **Raporlama (Sunum) (*Reporting*)**
- Bu sunum ile birlikte ayrıca ayrıntılı olarak dijital delillerin nasıl elde edildiğine ilişkin teknik boyutu ve adli bilişimin hangi metodlarının kullanıldığı da anlaşılır bir dille belirtilecek, açıklayıcı bir rapor hazırlanacaktır.
- Hazırlanacak bu raporda ayrıca, olayla ilgili bilgiler, araştırmanın yapıldığı zaman dilimi, incelenen elektronik deliller, inceleme esnasında kullanılan yazılım ve donanımlar hakkında bilgiler, inceleme sırasında kullanılan metodlar, araştırma sonunda ele geçen bulgulara ilişkin bilgiler yer almalıdır.