Bilişim Suçlarında Delillendirme

Ç. Ülküdemer

Özet— **Bu çalışma, bir adli olaydaki bilişim delillerinin taşıması gereken temel özellikler, kopya çıkarma aşamasında karşılaşılan temel problemler ile dikkat edilmesi gereken konular, kopya çıkarma aşamasında delilin bütünlüğü ve güvenilirliğine yönelik suistimallerin nasıl yapıldığı ile bu suistimallerin tespitinin mümkün olup olmayacağı hususlarını kapsamaktadır.**

Anahtar Kelimeler— **Bilişim suçları, bilişim suçlarına müdahale, elektronik delil, kopya çıkarma, imaj alma, adli kopya, adli bilişim, arama ve el koyma.**

Evidences in IT Crimes

Abstract— **This paper covers the fundamental properties of IT criminal evidences, the problems while getting the digital image of evidences and the important topics related IT criminal. Also includes, abusement of evidence integrity and reliability and if it is possible to understand the integrity problems.**

Index Keywords— **IT crimes, IT crimes incident response, digital evidence, digital image, IT law, criminal investigation on IT crimes.**

I. GİRİŞ

Bilişim teknolojilerinin günlük hayatta kullanımının her geçen gün artarak yaygınlaşması, bilişim sistemlerinin kullanımında suistimallerin artmasına ve bilişim suçlarının oluşmasına neden olmaktadır. Bilişim suçunun konusu bazen araç olarak kullanılan bir bilişim sistemi olabileceği gibi, hedef olarak seçilen bir bilişim sistemi de olabilmektedir. Özellikle internet üzerindeki pek çok platformun hayatımızı kolaylaştıran imkânlar sunması da, suçlular için bu platformları oldukça cazip hale getirmektedir. Bilişim sistemlerinin uzaktan erişim yöntemleri ile kullanılabilmesi, bilişim sistemlerine yapılan kaynağı belirsiz saldırılar, verilere izinsiz erişme, değiştirme ya da silme/bozma gibi durumlarda delillerin toplanması, incelenmesi ve faillerin tespiti adli bilişim uzmanlarının işini her geçen gün zorlaştırmaktadır.

Bilişim sistemlerindeki temel sorunlardan birisi, verinin oluşturulduğu tarih-saat bilgisinin sonradan değiştirilebilmesi ve istenilen tarih-saat bilgisi ile yeniden oluşturulabilmesidir. Bu nedenle delile müdahale aşamasında, adli kopyası (imaj) alınan sistemin tarih-saat bilgisinin güncel tarih-saat bilgisi ile karşılaştırılmasının yapılması ve bu hususun arama el koyma tutanağına yazılması gerekmektedir. Ayrıca, bir sistemde veriler kopyalanırken, kopyalanan verilere ait erişim, değiştirilme, silinme, taşınma, aidiyet, yetki v.b. gibi bilgilerin de kopyasının alınması gerekmektedir. Zira, bilişim sistemlerindeki verilerin çeşitli teknik ve yöntemlerle manipüle edilmesi mümkündür. Bu nedenledir ki, bilişim sistemlerinin adli kopyasının alınması, olaya müdahale (incident response) metotları ile yapılmalı, aksi halde yapılan işlemlerde delilin bütünlüğü ve güvenilirliği şüpheli duruma düşmekte ve delil niteliğini kaybetmektedir.

Bir bilişim sisteminin adli incelemesinde delillerin bulunabileceği alanlar şunlardır:

- Fiziksel alanlar:
  - Manyetik alanlar,
    - Sabit diskler,
    - ZIP kasetler,
    - Floppy disketler.
  - Optik alanlar,
    - CD-R,
    - DVD-R, DVD+R, DVD-RAM,
    - BLUERAY.
  - NAND ve NOR alanlar,
    - USB bellekler,
    - SSD'ler,
    - Diğer bellekler (SD, MMC, MS, xD v.b.)
    - RAM'ler.
- Mantıksal alanlar:
  - Dosya sistemleri,
    - ReFS, NTFS, FAT32, FAT 16,
    - Ext2, Ext3, Ext4,
    - HPFS, HFS+, CDFS.
  - İşletim sistemleri,
    - MS Windows,
    - Linux/Unix/Free BSD,
    - MacOS,
    - Mobil (gömülü) sistemler.
  - Uygulamalar,
    - Veri tabanları,
    - İnternet uygulamaları,
    - Office dosyaları,
    - Diğer dosyalar.
- Ağlar:
  - Yerel Ağlar (LAN),
  - Uzak/Geniş Ağlar (WAN),
  - Özel Sanal Ağlar (VPN).

II. BİLİŞİM SİSTEMLERİNDE ORTAMLAR VE İNCELEMELER

A. *İşletim Sistemleri*

İşletim sistemini çekirdek modunda çalışan bir yazılım olarak tanımlamaktan daha fazla bir şey söylenemez, ki bu her zaman doğru değildir. İşletim sistemi hem programcılara aygıtları yönetebileceği bir komut seti sağlar hem de bu aygıtları kontrol eder [1].

Bu nedenle işletim sistemlerinin çalışma mantığı ve diğer aygıtlarla nasıl bir etkileşim içerisinde olduğu programcıya göre değişen bir kavramdır ve *her sistem kendi bütünü içerisinde incelenmelidir.*

Bir işletim sisteminde verilerin, özellikle değiştirilme, silinme dışında kaybolması ancak;

- Doğal felaketler: Yangın, sel, deprem vb.,
- Donanım ya da yazılım hataları: CPU hataları, disk okuma/yazma hataları, iletişim hataları, yazılım hataları vb.,
- İnsan hataları: Hatalı komut/girdi, hatalı bilişim sistemi etkileşimleri, bilerek/bilmeyerek hatalı program çalıştırma ile mümkündür [2].

Bu nedenle işletim sistemlerindeki komutların özellikleri ve sonuçları adli incelemeyi gerçekleştirecek uzmanlar tarafından tarafsız, önyargısız, varsayımsız olarak incelenmelidir. Bu hususları yerine getirebilmek için bilimsel bir inceleme metot ve yöntemi oluşturulmalı ve oluşturulan bu metot ve yöntem her zaman denetime açık ve kontrol edilebilir olmalıdır.

Günümüzde yaygın olarak kullanılan işletim sistemleri Windows, Linux, Unix, OsX ve BSD'dir. Ancak tüm bu işletim sistemlerinin bir türevinin cep telefonu, tablet vb. araçlarda da kullanıldığını unutmamak gerekir.

İşletim sistemleri belirli ölçülerde özelleştirilebilmekte ve yaygın kullanılan komutlar farklı amaçlar için de kullanılabilmektedir. Bu nedenle inceleme esnasında, kullanılan komutların dosya bütünlük değerleri (hash value), orijinal hali ile karşılaştırıldıktan sonra içerik analizi yapılmalıdır. Linux işletim sistemine özel olarak bu karşılaştırmaları yapan en yaygın araçlardan biri GPL lisans ile açık kaynak kodlu olarak dağıtılan *rootkithunter* projesidir [3].

İşletim sistemlerinin kullanıcılar tarafından özelleştirilmesi, suç işleyenler tarafından da kötüye kullanılabilmekte ve özellikle işletim sisteminin kapatılması esnasında delil niteliği taşıyacak pek çok verinin silinmesi için programlanabilmektedir. Bu nedenle, adli bilişim eğitimlerinde uzman adaylarına olaya ilk müdahalenin nasıl yapılacağı anlatılırken, genellikle sistemleri normal kapatma (shutdown) yerine fişinin çekilmesi (power off) tavsiye edilmektedir [4].

Bu tavsiyenin kabul edilebilir gerekçeleri olsa da, sistemlerin düzgün kapatılmaması yazılımsal ve donanımsal sorunlara yol açıp veri delillerin bozulmasına hatta kaybolmasına sebep olabilir.

Adli kopyanın çıkarılması ile ilgili diğer temel bir sorun ise; adli kopyası alınacak optik depolama aygıtlarının (CD, DVD, BlueRAY) kopyasının fiziksel ya da mantıksal olarak hangi yazılım ve sürümü ile alındığının ve kopyalama neticesinde oluşan elektronik imzanın arama-el koyma tutanağı ve bilirkişi (expertiz) raporlarına detaylı olarak yazılmamasıdır. Zira, adli bilişim incelemelerinde delilin doğrulanma (verification) aşamasında, adli kopyaların elektronik imzalarının adli bilişim yazılımları ile kontrolü yapılmaktadır. Adli kopyanın alındığı yazılım haricinde başka bir yazılım kullanıldığında, farklı bütünlük değerleri hesaplanabilmektedir. Bu durum, optik disklerin yapısı, verilerin yazılma formatı, adli kopyaların fiziksel ya da mantıksal olmasının adli bilişim yazılımları tarafından farklı işleme tabi tutulması ve bu alandaki standardın tam olarak sağlanamamasından kaynaklanmaktadır [5]. Bu nedenle, doğrulama yapılırken aynı yazılım ve sürümü ile yapılması önerilmektedir.

B. *Dosya Sistemleri*

Bir verinin bir işletim sistemi üzerinde yazılması/okunması için geliştirilmiş algoritmik düzene dosya sistemi denilmektedir [6].

Farklı amaçlar için geliştirilmiş onlarca dosya sistemi mevcuttur. En yaygın kullanılan dosya sistemleri: NTFS, FAT, EXT-3, HFS'tir. Bunlar, yaygın kullanılan işletim sistemlerinin ön tanımlı dosya sistemleridir. Tüm dosya sistemleri disk üzerinde veriyi farklı bir şekilde barındırırlar ve inceleme sırasında bu verilerin nasıl bulunduğunun, kopyalama, değiştirme, taşıma ve silme işlemleri sırasındaki hareketlerinin iyi bilinmesi gerekmektedir.

5271 sayılı Ceza Muhakemesi Kanunu'nun (CMK) 134. maddesi ile Adlî ve Önleme Aramaları Yönetmeliği'nin 17. maddesinde bir bilgisayar sisteminde arama, kopyalama ve el koymanın nasıl yapılacağı belirtilmiştir. Gerekli tedbirlerin alındığı zaruri haller hariç, şüphelinin veri depolama aygıtları üzerinde canlı inceleme yapılmamalıdır. Ayrıca, delil üzerinde değişikliğe yol açacak ve delili şüpheli hale getirecek işlemlerden kaçınmalı, mümkünse delilin adli kopyası iki farklı diske alınmalı ve inceleme bu kopyalardan biri üzerinde yapılmalıdır. Böylece, taşınma ve inceleme esnasında oluşabilecek hata, zarar ve bozulmaların önüne geçilmelidir.

Hemen tüm dosya sistemleri *META DATA* (üst veri) adı verilen bilgiler üzerinde dosyanın oluşturulma, değiştirilme, son erişim, son çıktı alma v.b. bilgiler bulunmaktadır. Tüm bu veriler dosya sisteminin bir parçası olduğundan ve belirli bir sistematikte saklandığından değiştirilmesi mümkündür.

Bu nedenle, *pratikte dosya sistemi üzerindeki veriyi adli kopya (imaj) alma aşamasında bile değiştirmek mümkündür.*

Delilin güvenilirliğini sağlamak için *donanımsal yazma önleme sistemlerinin* (write blocker) adli kopya alma esnasında mutlaka kullanılması gerekmektedir.

Adli kopya alma esnasında *yazılımsal yazma önleme teknikleri* de mevcuttur. Yazılımsal çözümler, BIOS üzerindeki INT13h kodunu engelleyerek bunu gerçekleştirmektedir. Ancak, BIOS kontrollerini etkisiz hale getirmek mümkün olduğundan yazılımsal önleme teknikleri pek tercih edilmemektedir [7].

Adli kopya (imaj) alma işlemi, dosya sistemi üzerindeki her biti/bloğu sırası ile bir dosya/disk üzerine yazmak için kullanılmaktadır. Adli kopya almak için kullanılan en yaygın yöntemlerden birisi açık kaynak kodlu *dd* yazılımıdır. Pek çok adli kopya alma yazılımının da uyguladığı yöntem bu yazılımdan türemiştir. EnCASE, FTK Autopsy gibi ticari adli inceleme yazılımlarının kendi adli kopya alma sistemleri de mevcuttur.

Disk üzerindeki okuma hataları adli kopya alma sistemi tarafından görmezden gelinerek, okunabilen ilk alandan son alana kadar adli kopyalama işlemi yapılır. Bu hatalar veri alanları arasındaki ilişkileri bozabilir. Örneğin, veri silinmediği halde disk üzerinde gözükmez ve META DATA alanında da silinme tarihi yer almaz. Bu durum, verinin silindiği ve META DATA bilgisinin de bilerek ve isteyerek (delil saklama maksatlı) değiştirildiği şeklinde yorumlanmamalıdır.

Özetle, dosya sistemleri birbirleri ile ilintilendirilmiş çeşitli tablolardaki ilişkisel yapılardan yararlanarak veriye ulaşırlar. Bir nedenle referans tabloları hasar görürse (genellikle disk okuma/yazma hataları sonucu) veri silinmediği halde, dosya sistemi üzerinde ulaşılamaz duruma gelebilir. Bu dosyalar adli inceleme yazılımları ile diskin adli kopyasının incelemesinde görülebilirler, çünkü adli inceleme yazılımları referans tablolarında yer almayan dosyaları da gösterebilmektedir. Bu dosyalar gerçekte silinmediğinden, silinme tarihleri meta data tablosundaki ilgili alanlarda işaretlenmezler ve genellikle 0000.00.00 olarak tespit edilir. Bu durumda *delilin sağlıklı bir şekilde elde edilemediği* unutulmamalıdır.

C. Uygulama ve Veri Tabanları

Uygulamalar, genellikle verilerin oluşturulduğu, veri tabanları ise uygulamalara bağlı olarak bu verilerin saklandığı yerlerdir. Uygulamalar ile oluşturulan verilerin adli incelemesinde genellikle verinin oluşum tarihi ve saati önemlidir. Tarih ve saatin bilgisayarın BIOS'u üzerinden işletim sistemine aktarıldığı, sonrasında ise uygulamaya gönderildiği unutulmamalıdır. Zaman sunucuları (NTP) ya da ara uygulamalar ile işletim sistemi açıldıktan sonra saati değiştirmek mümkün olsa bile bu durum kötüye de kullanılmaktadır.

Uygulamaların oluşturacağı bir verinin ya da sistem kaydının oluşma zamanı, bilerek ve isteyerek sadece bilgisayarın saati değiştirilerek de değiştirilebilir. Bu nedenle inceleme sırasında sistem saatine asla güvenilmemelidir. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da sistem kayıtlarının zaman damgası ile tutulmasının gerekçesi de bundan kaynaklanmaktadır.

Üçüncü bir tarafça sabitlenmeyen hiç bir zaman verisi olay zamanını sabitlemez. Suçlular tarafından bilerek ve isteyerek zaman verilerinin değiştirilmesi özellikle ağ üzerinden yapılan saldırı olaylarının seyrini tamamen değiştirebilecek sonuçlar yaratmaktadır.

Bütün bunlardan hareketle, uygulama incelemelerinde aynı koşullarda uygulamanın algoritmik tepkileri ve oluşturdukları verilerin karakteristik özellikleri, bağlı bulunduğu veri tabanı ve diğer bileşenlerle birlikte değerlendirilmeli, ancak incelemeye konu olan dosyalardaki zamanlara ve verilere güvenilmemelidir.

Uygulamaların / veri tabanlarının verileri nasıl sildiği, değiştirdiği ya da nereye nasıl bir formatta kaydettiği adli inceleme açısından çok daha önemlidir. Uygulamaların verileri kurtarılamayacak şekilde silmesi ile ilgili durumlara çok nadir rastlanmakla birlikte, çoğunlukla bu sorunun cevabı dosya sistemlerinde aranmalıdır.

D. Bellek ve Takas Alanları

Belleklerin yönetimi işletim sistemlerinin sorumluluğundadır. Bellekler bir uygulamanın çalışması sırasında geçici verilerin yazıldığı ya da değişken bilgilerinin tutulduğu alanlardır. Kullanıcı bellek alanları 3 parçadan oluşmaktadır:

- Code Segment (Kod Kesimi)
- Data Segment (Veri Kesimi)
- Stack Segment (Yığın Kesimi)

Tüm bu veri alanları, kullanıcı kabuk bilgilerini taşıdığı gibi aynı zamanda parolaların ya da kullanıcılar ile ilgili önemli verilerin barındırıldığı yerlerdir. İşletim sistemi üzerinde kullanıcılar arasındaki paylaşımlar da buralarda yapılmaktadır [8].

Takas alanları bir depolama ünitesi üzerinde bellek gibi kullanılan yapılardır. Windows işletim sisteminde bu alana *Sanal Bellek* (virtual memory), Unix/Linux ve türevi işletim sistemlerinde *Swap* adı verilir.

Fiziksel bellekler (RAM) elektrik olmadığı sürece bilgi depolayabilecek bir özelliğe sahip değildirler. Bu nedenle bilgisayar her açıldığında yeniden sıfırlanır.

Bir bilgisayar belleğinin adli incelemesi yapılacak ise sistem kapatılmadan ya canlı olarak yapılması ya da belleğin adli kopyası alındıktan sonra yapılması gerekir. Olaya müdahale esnasında sistemlerin belleğinin adli kopyasının

alınmaması yaygın olarak yapılan hatalardan birisidir.

Takas alanları veri depolama alanları üzerinde durduğu için bu alanlar bilgisayar kapatıldıkran sonra da incelenebilir. Tabi ki bilişim ortamındaki tüm veriler gibi bu alanlardaki verilerin de yeniden üretilmesi, değiştirilmesi ya da silinmesi mümkündür.

E. Ağ İncelemeleri

Ağ incelemeleri, bilgisayar incelemelerinden daha farklı ele alınması gereken bir kavramdır. Ağ üzerinde gelen paketlerin gerçek zamanlı kaydı ile mümkündür. Günümüzde özellikle uzak bağlantıların bir film izler gibi (SSH, RDP, VNC, Telnet, ICA) izlenebildiği ve kayıt edilebildiği sistemler vardır ve adli incelemeler için de bu sistemlerden faydalanılmaktadır [9].

Ağ incelemelerinde, suçu ya da suistimali delillendirmek için gerçek zamanlı ağ trafiği yeterli bir zaman aralığı boyunca kopyalanmalı ve inceleme bu kopya üzerinde adli bilişim imkânları ile yapılmalıdır. Ağ incelemelerinde, gerçek zamanlı yapılmamış kayıtların dışında delil elde etmek mümkün değildir. Ancak ve ancak *gerçek zamanlı olarak kayıt edilen deliller kesin delil niteliği taşır*.

F. Verilerin Kesinliği ve Zaman Damgası

Bilişim sistemlerinde olay anında ayrıca kaydedilmeyen (ki bu ağ bağlantıları için geçerlidir) hiç bir veri kesin delil niteliği taşımaz. ***Bilişim ortamında bütün veriler değiştirilebilir, silinebilir ve yeniden oluşturulabilir.***

Bu nedenle gerçek zamanlı olarak kayıt edilen ağ verileri zaman damgası ile damgalandıktan sonra saklanmalıdır. Zaman damgası ile damgalanan veriler, sadece verinin zaman damgası alındıktan sonra değişmediğinin ispatı için kullanılabilir.

G. Delil saklama ile ilgili işlemler

Bilişim delilleri bağlı bulunduğu sistemler ile birlikte saklanmalıdır. Hangi kablonun nereye bağlı olduğu, hangi sistemlerin açık olduğu inceleme esnasında çok önemlidir. Özellikle bağlandıkları noktalar ayrıca işaretlenmeli, fotoğraf ve video ile kayıt altına da alınarak yapılan tüm işlemler tutanağa geçirilmelidir.

Bilişim ortamlarında veri saklama ortamlarının çoğu manyetik alan kullanarak veri kaydettiğinden, bu tarz medyaların antistatik bir ortamda saklanması gerekmektedir.

Diskler mutlaka iki farklı diske adli kopya alındıktan sonra alınan kopyalardan biri üzerinden incelenmelidir.

Bilişim sisteminin her açılıp kapanması sırasında verilerin değişebileceği ya da silinebileceği unutulmamalıdır.

III. SONUÇ

Bilişim sistemlerindeki veriler silinebilir, değiştirilebilir ya da yeniden oluşturulabilir. Bu nedenden ötürü gerçek zamanlı olarak kaydedilmemiş hiç bir veri kesin delil olarak değerlendirilmemelidir. Sistemlerin saatlerinin değiştirilmesi dosyalar üzerinde yapılan işlem zamanlarını güvenilmez yapar. Ancak, delile müdahale aşamasında adli bilişim metot ve tekniklerinin usulüne uygun olarak yerine getirilmesi ve yapılan her türlü işlemin kayıt altına alınması elektronik delilin güvenilirliğini sağlayabilir.

Dosya meta dataları bir çok yazılım tarafından değiştirilebildiği için tamamen bu verilere dayanılarak hüküm verilemez, ancak meta data verileri ana delilleri destekleyen yan deliller olarak kullanılabilir.

Veri depolama aygıtlarının adli kopyalarının alınması esnasında donanımsal yazma önleme sistemlerinin kullanılmaması, delilin güvenilirliği ve bütünlüğü konusunda şüpheye neden olur ve alınan kopya delil niteliği taşımaz.

KAYNAKLAR

[1] Andrew S. Tanenbaum, *Modern Operating Systems, 3/E,* Prentice Hall, pp 1-4, 2007.
[2] Andrew S. Tanenbaum, *Modern Operating Systems, 3/E,* Prentice Hall, pp 9-6, 2007.
[3] RootkitHunter, http://www.rootkit.nl/projects/rootkit_hunter.html
[4] Semih Dokurer, Kriminal Polis Laboratuvarı, *Bilişim Suçları ve Adli Bilişim Sunumu* , Wormy, pp 20, 2005.
[5] Christopher Marberry and Philip Craiger, *Factors Affecting One-Way Hashing of CD-R Media*, IFIP Int. Conf. Digital Forensics, pp 1-13 2007.
[6] Daniel Grosshans, *File systems: Design and Implementation*, Prentice Hall, pp1,5, 1986.
[7] Brain Carrier, *File System Analysis*, Addison Wesley Professional, pp 49-50, 2005.
[8] Graham Glass, *UNIX For Programmers and Users* , Prentice Hall, pp 533, 1993.
[9] Shell Control Box, http://www.balabit.com/network-security/scb/features

Ç. Ülküderner 2003 yılında bilgisayar mühendisi olarak mezun oldu. 2007 yılında 'Kablosuz Ağlarda Güvenlik' üzerine yazdığı tezi ile birlikte yüksek mühendis ünvanını aldı. TÜBİTAK'ta uzun yıllar sistem yöneticisi olarak çalıştı sonra, Hacettepe Üniversitesi Bilişim Hukuku yüksek lisans programında ders verdi.

Yurt içi ve yurt dışında bilgi güvenliği ile ilgili pek çok projede yer aldıktan sonra Profelis Bilişim adındaki şirketini kurdu. Halen şirketin yönetcisi olarak meslek hayatına devam etmektedir.