Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi*

Ahmet Serhat Şirikçi, Nergis Cantürk

Ankara Üniversitesi, Adli Bilimler Enstitüsü, Kriminalistik Anabilim Dalı, Cebeci, Ankara
ahmetserhatsirikci@gmail.com, nergiscanturk@yahoo.com
(Geliş/Received: 17.07.2012; Kabul/Accepted: 12.10.2012)

Özet- Adli bilişim alanında yapılan incelemelerde tüm inceleme ve analiz faaliyetleri olaya ait delillerin birebir kopyaları üzerinde yapılmaktadır. Birebir kopya delilin üzerindeki bütün verilerin kopyasının alınması anlamına gelmektedir. Adli bilişim laboratuvarlarında yaygın olarak Windows işletim sistemi üzerinde çalışan kapalı kaynak kodlu yazılımlar kullanılmaktadır. Birebir kopya alınması işlemi için açık kaynak kodlu yazılımların da kapalı kaynak kodlu yazılımlar kadar başarılı olup olmadığını gözlemlemek amacıyla çalışma planlandı. 3,8 GB kapasitesi olan USB bellek kapalı kaynak kodlu bir yazılım olan FTK Imager yazılımı ile açık kaynak kodlu bir yazılım olan Guymager yazılımı birebir kopyalayarak karşılaştırıldı. İşlemci kullanımı, kopyalama süresi ve ortalama kopyalama hızı açısından Guymager yazılımının FTK Imager yazılımına göre başarılı olduğu tespit edildi. Hesaplanan Hash değeri bakımından ise her iki yazılımda da aynı sonuç elde edilmiştir. Araştırmamızda birebir kopyalama işleminde açık kaynak kodlu bir yazılım olan Guymager, kapalı kaynak kodlu bir yazılım olan FTK Imagerdan daha başarılı bulunmuştur. Ancak kesin sonuçlar elde edebilmek için bu konuda daha fazla araştırma yapılmasına ihtiyaç vardır.

Anahtar Kelimeler- Adli bilişim, birebir kopyalama, kapalı kaynak kodlu yazılımlar, açık kaynak kodlu yazılımlar

The Importance of Creating a Byte-to-byte Copy (Imaging) at Computer Forensics Investigations

Abstract- All the analyses and investigations in computer forensics are carried out by byte-to-byte copying of the digital evidence which means copying all the data. Closed source softwares mostly operating on the Windows operating systems are commonly used in computer forensics laboratories. This research has been done to observe whether open source softwares are as successful as the closed ones in byte-to-byte copying process. A byte-to-byte copy of a USB thumb drive with 3.8 GB capacity was created both with FTK Imager and Guymager programme of which the first has a closed and the second an open source. It was observed that Guymager is more successfull than FTK Imager software in CPU usage, copy time and average copy speed. The same hash values results were obtained with both softwares. In the research, it was concluded that Guymager, an open source software, is more successfull than FTK Imager which is a closed source software. However, further researches should be carried out to obtain more solid results.

Keywords- Computer forensics, byte-to-byte copy, closed source softwares, open source softwares

* Bu çalışma 5-8 Temmuz 2012 tarihleri arasında İstanbul'da düzenlenen 22. International Academy of Legal Medicine Kongresi'nde poster bildiri olarak sunulmuştur.

1. GİRİŞ

Adli bilişim, elektromanyetik ve elektrooptik ortamlarda muhafaza edilen veya bu ortamlarca iletilen ses, görüntü, veri, bilgi veya bunların birleşiminden oluşan her türlü bilişim nesnesinin, mahkemede sayısal delil niteliği taşıyacak şekilde tanımlanması, elde edilmesi, saklanması, incelenmesi ve mahkemeye sunulması çalışmaları bütünüdür [1]. Kısaca; bilişim cihazlarından delil elde etme sürecidir. Bu süreç; delil toplama (collection), delillerin incelenmesi (examination), sonuçların değerlendirilmesi (analysis) ile raporlama ve sonuç (reporting) aşamalarından oluşur [2]. Adli bilişim uzmanları incelemelerini farklı yazılım ve donanımlar kullanarak gerçekleştirmektedir. Yazılımlara; Encase Forensics, Forensic Tool Kit, ProDiscover, SMART, The Sleuth Kit/Autopsy, donanımlara ise; Tableau yazma-koruma cihazları, Voom Technology cihazları, Solo-III kopyalama cihazları örnek olarak verilebilir [3,4].

Bir adli bilişim uzmanı incelemeler esnasında daha önce hiç görmediği bir cihaz ve bu cihazda kendine özgü bir dil ve konfigürasyona sahip bir yazılım ile karşılaşabilir. Bu nedenle bilişim uzmanları farklı işletim sistemi mimarilerinden ve bileşenlerinden haberdar olmalı, farklı yazılım ve donanımlar ile işletim sistemlerini kullanabilmelidir. Kullanılan yazılımların sınırları ve becerileri çok iyi bilinmeli ayrıca sadece tek bir yazılım veya donanıma bağlı kalınmamalıdır. Farklı yazılımlar kullanılarak farklı sonuçlara ulaşılabileceğinden hangi durumda hangi yazılımın kullanılması gerektiği bilgisi de çok önemlidir[5].

Adli bilişim alanında yapılan tüm inceleme ve analizler orijinalinde herhangi bir değişiklik meydana gelmemesi için delillerin birebir kopyaları üzerinde yapılır. Birebir kopya alma aşamasında özel yazılım ve donanımlara ihtiyaç duyulmaktadır. Birebir kopya delilin üzerindeki bütün verilerin kopyasının alınması anlamına gelmektedir. Alınan birebir kopya; mevcut verileri, silinmiş verileri, gizli bölümlerini, veri depolama biriminde bulunan diğer verileri de kapsar [2]. Kullanılan "birebir aynısı" terimi, orijinal medyanın her sektör ve byte'ının kopyalanması anlamındadır. Birebir kopyada orijinal medyada bulunmayan en ufak bir bilgi olmamalıdır. İdeal bir kopyalama işlemi orijinal medya üzerinde herhangi bir değişiklik meydana getirmemelidir [6]. Birebir kopyalama çeşitli birebir kopyalama cihazları veya yazılımların kullanılması ile yapılabilmektedir.

Birebir Kopyalama Cihazları Kullanılarak Kopya Alınması: Adli bilişim uzmanları hem olay yerinde hem de laboratuvar ortamında çok çeşitli kopyalama donanımları kullanabilmektedir. Bu donanımlardan bazıları doğrudan analiz bilgisayarına bağlanabilmekte bazıları ise Firewire veya USB kapıları aracılığı ile işlem görmektedirler [7]. Bu yöntemde söz konusu kopyalama cihazının bir tarafına yazma korumalı olarak delil, diğer tarafına yazma koruması kullanılmaksızın kopyanın alınacağı veri depolama birimi yerleştirilir ve ekran veya tuşlar yardımıyla kopyalama işlemi yapılır (Şekil 1).

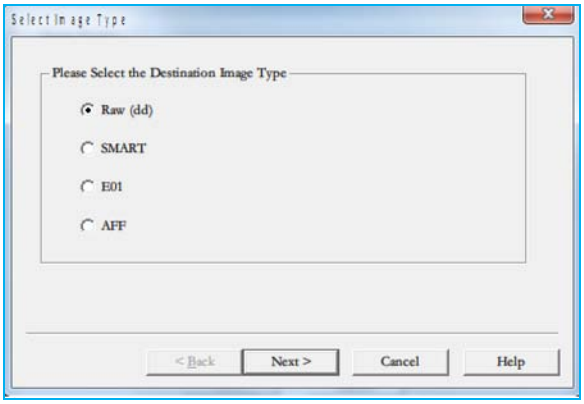
Şekil 1. *SOLO-III birebir kopyalama cihazı*

Yazılımlar Kullanılarak Kopya Alınması: Yazılımsal olarak kopya alınmasında, adli amaçlı olarak kullanılan yazılımlar, işletim sistemini kullanmadan medya ile bağlantı kurmakta ve medyaya istenen işlemleri yaptırmak suretiyle kopyalarının alınmasını sağlamaktadırlar.

A) Kapalı Kaynak Kodlu Yazılımlar: Birebir kopya alma işleminde adli bilişim uzmanları EnCase, FTK Imager, Smart, Task, ve Ilook gibi kapalı kaynak kodlu yazılımların analiz ve kopyalama özelliklerinden faydalanmaktadır [7]. Bu yazılımlar genel olarak Windows işletim sisteminde çalışmaktadırlar.

FTK Imager Yazılımı: FTK Imager, AccessData firması tarafından üretilmiş bir yazılımdır. Yazılımın ana amacı veri depolama birimlerinin içeriğini görüntülemek ve birebir kopyasını almaktır. Yazılımın veri kurtarmadaki etkinliği, genellikle verinin silindiği zamana bağlıdır. Diğer bir özelliği de erişilebilen medyaların MD5 veya SHA hash değerlerini üretebilmesidir. Gerçek anlamda, MD5 hash değerinin üretilmesi, orijinal verilerin bütünlüğünün korunduğunun garantisini verebilmek maksadıyla yapılır [8].

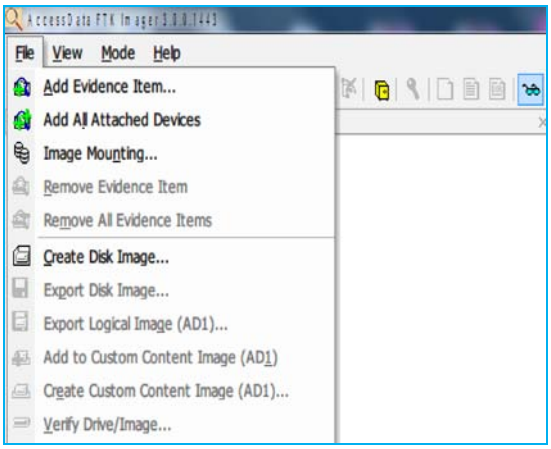
AccesData firması, FTK Imager yazılımının ve güncel versiyonlarının ücretsiz kullanımına izin vermektedir. FTK Imager yazılımı ile ham halde (dd), E01 (Expert Witness, Encase) ve AFF biçimlerinde birebir kopyalar alınabilmektedir (Şekil 2). Ayrıca FTK Imager, FAT, NTFS, ext2, ext3 gibi dosyalama biçimlerini de desteklemektedir [9].



Şekil 2. *FTK Imager yazılımı kopya biçimleri*

FTK Imager yazılımı ile:

- Elektronik medyalar ile bu medyalar içerisinde bulunan dosyaların birebir kopyaları alınabilir, (Şekil 3).



Şekil 3. *FTK Imager yazılımı menü bölümü*

- Medyalar içerisinde bulunan verilerin ön izlemesi yapılabilir,
- Birebir kopyası alınmış olan medyaların kopyalarının ön izlemesi yapılabilir,
- Alınmış olan birebir kopyalar sadece okuma modunda (read-only) görüntülenebilir (mount),
- Kopyalar içerisinden veriler dışarı Windows ortamına aktarılabilir,
- Silinmiş ve çöp kutusuna atılmış olan dosyalar görüntülenebilir,
- MD5 ve SHA-1 algoritmalarını kullanarak hash değeri üretilebilir,
- Birebir kopyalar ile normal dosyalar için hash raporları üretilebilir [10].

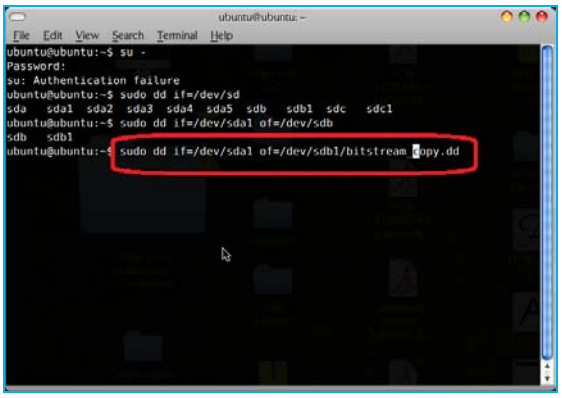
Encase Forensics Yazılımı: Encase Forensics yazılımı, Guidance Software firması tarafından üretilen ve pazarlanan ve tüm dünyada en çok bilinen ve kullanılan adli bilişim yazılımıdır. Yazılım; birebir kopya alma ve saklama fonksiyonlarından anahtar sözcük arama ve basit anlamda veri kurtarma fonksiyonlarına kadar sabit disk içerisinde byte seviyesinde birçok analiz işlemi yerine getirebilmektedir [11]. Encase Yazılımı ücretli bir yazılımdır. CD/DVD İnceleme, Yazma-koruma gibi modülleri de ücret karşılığı elde edilebilmektedir.

Encase yazılımı ile;

- Birebir kopyalama işlemi yapılabilir,
- İncelenecek medya ön izleme modunda incelenebilir,
- Anahtar kelime araması yapılabilir,
- "Gallery" paneli görüntü dosyaları hızlı ve kolay bir şekilde incelenebilir,
- Elektronik medyalar yazma-korumalı olarak inceleme bilgisayarına bağlanabilir,
- Enscript özelliği ile ihtiyaç duyulan işlemler yapılabilir [12].

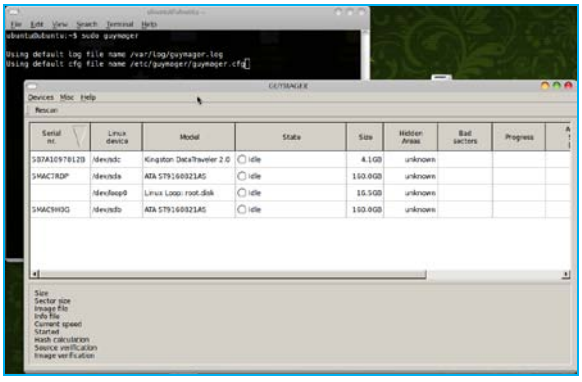
B) Açık Kaynak Kodlu Yazılımlar: Birebir kopyalama işleminde adli bilişim uzmanları genellikle Linux işletim sistemi üzerinde çalışabilen dd, dcfldd, guymager gibi açık kaynak kodlu yazılımlardan da yararlanmaktadırlar (Şekil 4,5). Açık kaynak kodlu yazılımların bazıları Windows işletim sisteminde de çalışabilmektedir.

Bir bilgisayarın sabit diskinin birebir kopyası, Linux işletim sistemine ait dd komutunun grafik ara yüzü olarak kullanılabilen AIR (Automated Image & Restore, Otomatik İmaj & Geri Yükleme) yazılımı ile kolaylıkla alınabilmektedir. AIR yazılımı yanı sıra birebir kopya alma, hash değeri hesaplama ve doğrulama gibi işlemlerde Guymager yazılımı da kullanılabilmektedir [13].



Şekil 4. *dd komutu ile birebir kopyalama işlemi*

Guymager Yazılımı: Guymager yazılımı, adli bilişim uzmanlarınca medyaların ham veya E01 (Expert Witness Format) biçimlerinde kopyalarının alınmasına imkân sağlayan bir yazılımdır [14]. dd üzerine geliştirilmiş bir grafik ara yüze sahiptir. Debian ve Ubuntu türü sistemlerde kullanılmak üzere geliştirilmiştir. Bilgisayara sonradan bağlanan medyalar üst bölümde sıralanır ancak yerel diskler üzerinde işlem yapılamaz. Böylece yanlış diskin kopyasının alınması önlenir. Qt ara yüzünü kullanmaktadır. Ücretsizdir.



Şekil 5. *Guymager yazılımı ara yüzü*

Guymager yazılımı:

- Farklı dil desteği ve kolay kullanım ara yüzüne sahiptir,

- Sadece belli Linux platformlarda çalışabilir,
- Hızlı ve aynı anda birden çok imaj alabilir,
- Çok işlemcili makinelerde bütün işlemcileri kullanabilir,
- Raw (dd), EWF (E01) ve AFF imaj alabilir,
- Disk klonlama işlemi yapabilir,
- MD5 ve SHA-256 algoritmalarını kullanarak elektronik imza değeri üretebilir,
- Alınan birebir kopyanın doğru olarak alınıp alınmadığının doğrulamasını yapabilir,
- Alınan kopyayı istenilen boyutlarda parçalara bölebilir [15].

Çalışmanın amacı, adli bilişim incelemelerinde, birebir kopyalama aşamasının kapalı kaynak kodlu yazılımlar kadar açık kaynak kodlu yazılımlar ile de yapılabilmesinin mümkün olduğunun ortaya konmasıdır.

2. GEREÇ VE YÖNTEM

Kapalı kaynak kodlu yazılım olarak, imaj alma işlemi açısından en hızlı ve kullanışlı, ayrıca adli bilişim laboratuvarlarında imaj almak için yaygın kullanılan bir yazılım olan FTK Imager yazılımı seçilmiştir. Açık kaynak kodlu yazılım olarak kullanım kolaylığı nedeniyle Guymager yazılımı seçilmiş ve 3,8 GB kapasitesi olan bir USB bellek her iki yazılımla birebir kopyalanarak sonuçlar karşılaştırılmıştır. Kopya biçimi olarak Encase Forensics yazılımı ile uyumlu olan, "Expert Witness Format (E01)" seçilmiştir. Hash fonksiyonu olarak MD5 algoritma türü kullanılmış ancak kopyalama doğrulaması seçeneği seçilmeden kopyalama işlemleri başlatılmıştır. Yazılımların kullanımında işletim sistemlerinin grafik ara yüzleri kullanılmıştır. Söz konusu kopyalama işlemi, her iki yazılım için **Tablo 1**'de belirtilen eşit şartlar oluşturularak gerçekleştirilmiştir. Ancak FTK Imager yazılımının Windows işletim sistemi üzerinde çalışan versiyonu ile Linux işletim sistemi üzerinde çalışabilen Guymager yazılımlarının üzerinde çalıştığı işletim sistemleri tamamen farklı olduklarından, kesin olarak birebir aynı şartların oluşturulması sağlanamaz. FTK Imager (v3.x) yazılımı Windows üzerinde grafik ara yüzü olmadan kullanılamaz [10]. Dolayısıyla testlerde eşit şartların sağlanabilmesi amacıyla, komut satırı aracılığıyla da kullanılabilen Guymager yazılımının grafik ara yüzü kullanılmıştır. Bu işlemde Guymager kullanımında işlemci ve RAM bellek kullanımında doğrudan etkili olmuştur.

3. BULGULAR

Tablo 1'de tanımlanan şartlar altında kapalı kaynak kodlu bir yazılım olan FTK Imager ile kopyalama işlemi 7 dk. 7 sn. sürmüştür. Ortalama kopyalama hızı 9,66 MByte/s. olup, ortalama işlemci kullanımı % 12,87'dir. Bellek kullanımı ise ortalama 17,96 MB'dir. Açık kaynak kodlu bir yazılım olan Guymager ile kopyalama işlemi 6 dk. 9 sn.'de tamamlanmıştır. Ortalama kopyalama hızı 10,67 MByte/s. olup, ortalama işlemci kullanımı %23,81'dir. Bellek kullanımı ise ortalama 14,15 MB'dır (Tablo 2).

4. SONUÇ

Gelişmekte olan ülkemiz Türkiye, çağın gerektirdiği bilgi teknolojileri alanındaki gelişimini sağlamak ve elindeki genç ve dinamik nüfusu doğru yönlendirerek bu alanda önde gelen ülkeler arasında yer alabilmek için gereken stratejileri hazırlamak ve uygulamaktadır. Uygulamada kullanılmış bazı başarısız kapalı kaynak koda dayalı denemeden sonra kendi ulusal işletim sistemini oluşturmanın ve sistemlerde kullanılacak yerli özgür yazılımları üretmenin önemi anlaşılarak bu doğrultuda gerekli çalışmalar başlamıştır [16].

Adli Bilişim alanında da kullanılan açık ve kapalı kaynak kodlu yazılımlar ile ilgili olarak, Encase ve FTK gibi kapalı kaynak kodlu ve ücretli yazılımlara alternatif olarak Autopsy gezginini kullanan ve açık kaynak kodlu SleuthKit yazılımı, bir proje grubu tarafından değerlendirilmiştir. Proje grubu, her üç yazılımı da kullanım kolaylığı, fonksiyonelliği, güvenirliği ve sonuçlarının doğrulanabilir olup olmadığını test etmişlerdir. Sonuç olarak her bir yazılımın belirli alanlarda diğerlerine göre başarılı olduğu belirlenmiştir [17].

Tablo 1. *Yazılımlar için sağlanan eşit koşullar*

	FTK Imager V3.0.0.1443	**Guymager V0.5.7beta1-1**
İşletim Sistemi	Wındows 7 Ultımate (32 Bıt)	Wındows 7 Ultımate (32 Bıt)
Bilgisayar İşlemcisi	Intel Core 2 Duo T9300 2,50 Ghz	Intel Core 2 Duo T9300 2,50 Ghz
Ram (Bellek)	3,00 Gb	3,00 Gb
Kopya Biçimi	Expert Wıtness Format (E01)	Expert Wıtness Format (E01)
Hash Hesaplama	Md5	Md5
Hash Doğrulama	Yok	Yok

Yazılım Kullanımı	Arayüz	Arayüz
Kopyalama Esnasında Çalışan İşlemler	System Monıtor	System Monıtor
Kopyalanan Medya	3,8 Gb Usb 2.0 Bellek	3,8 Gb Usb 2.0 Bellek
Kopyalanan Medya Veri Oranı	688.4 Mb Dolu	688.4 Mb Dolu

Kapalı kaynak kodlu adli bilişim yazılımlarının daha yaygın ve tercih edilen yazılımlar olmalarının nedenlerine örnek olarak; kullanım kolaylıkları, üretici firmalar tarafından eğitimlerinin ve güncellemelerinin sağlanıyor olması, kullanıcıların kurumlarında ücretsiz yazılım kullanmalarının yönetim tarafından cazip bulunması olarak verilebilir.

Her iki yazılım için aynı şartlar oluşturularak yapılan kopyalamada; her iki yazılım da aynı MD5 hash değerini üretmiştir, bu durum her iki yazılımın da doğru olarak birebir kopya aldığını göstermektedir. Hesaplanan hash değeri bakımından her iki yazılımda da aynı sonuç elde edilmiş olması adli açıdan açık kaynak kodlu yazılım olarak kullanılan Guymager yazılımının güvenirliğini ortaya koymaktadır.

İşlemci kullanımı bakımından, Guymager yazılımının FTK Imager yazılımına oranla iki kat daha fazla işlemci kullandığı tespit edilmiş olup bu durumun kopyalama işlemi esnasında başka bir işlem yapılması durumunda bilgisayar performansında azalma yaşanmasına neden olduğu görülmektedir. Ancak bu durumda araştırma açısından hangi yazılımın bilgisayarın kaynaklarını daha iyi kullandığının tespiti önem kazanmaktadır. Söz konusu işlem 3.8 GB'lık bir medya üzerinde yapılmış olduğundan, işlemci performansındaki fark işlemin kısa olması nedeniyle hissedilmeyebilir. Ancak kopyalanacak medyanın daha büyük kapasitelere sahip olması durumunda işlemci performansındaki azalma çok açık bir şekilde tespit edilebilecektir.

Yazılımlar, bellek kullanımı açısından değerlendirildiğinde; FTK Imager yazılımının Guymager yazılımına oranla yaklaşık olarak 4 MB.lık fazladan RAM bellek kullandığı tespit edilmiştir. Ancak bu durum, işlemlerin 3 GB.lık bir RAM bellek üzerinde yapılmasından dolayı bilgisayar performansında belirgin bir farka neden olmamaktadır.

Tablo 2. *Yazılımların kopyalama işlemi sonucu karşılaştırılması*

Usb Taşınabilir Bellek	**Ftk Imager V3.0.0.1443**	**Guymager V0.5.7beta1-1**
Medyanın Kapasitesi	4127195136 (3.8 Gb)	4127195136 (3.81gb)
Kopya Biçimi	Expert Witness Format, (.E01)	Expert Witness Format, (.E01)
Hash Hesaplaması	Evet	Evet
Hash Değeri	B6fbb1e40f9ae724c5c3c4724887ee0e	B6fbb1e40f9ae724c5c3c4724887ee0e
Hash Doğrulama	Hayır	Hayır
Hash Algoritma Türü	Md5	Md5
Kopya Doğrulama İşlemi	Hayır	Hayır
Kopyalama Süresi	7 Dk. 7 S.	6 Dk. 9 S.
Kopyalama Hızı	9.66 Mbyte/S	10.67 Mbyte/S
Bad Sektör	Tespit Edilmedi	Tespit Edilmedi
İşlemci Kullanımı	% 12.87	%23.81
Bellek Kullanımı	17.96 Mb	14.15 Mb

Adli bilişim incelemelerinde, inceleme süresi çok önemlidir. Guymager yazılımının bu aşamada FTK Imager yazılımına oranla 58 sn. gibi büyük bir farkla işlemi daha hızlı bitirdiği tespit edilmiştir. Bunun en büyük nedeninin Guymager yazılımının bilgisayar kaynaklarını (işlemci ve RAM bellek)

daha fazla kullanabilmesidir. 3.8 GB'lık bir medya incelemesinde 58 saniyelik bir gecikme yaşanması, yüksek kapasiteli medyaların (2 TB gibi) incelemesinde büyük süre kayıplarına neden olacaktır. Sürenin uzaması işlemci ve bellek kullanımının da uzamasına neden olur.

Kopyalama süresi ve ortalama kopyalama hızı bakımından Guymager yazılımının üstün olduğu görülmektedir. Guymager yazılımının 1 saniyede kopyaladığı veri miktarının, FTK Imager yazılımına oranla 1 MB daha fazla olduğu tespit edilmiş olup bu durumun yukarıda belirtilen kopyalama süresine doğrudan etki ettiği açıktır.

Araştırmada, kapalı kaynak kodlu FTK Imager yazılımı ile açık kaynak kodlu Guymager yazılımları kullanılarak yapılan birebir kopyalama işlemleri karşılaştırılmış ve Guymager yazılımının, işlemci kullanımı, kopyalama süresi ve ortalama kopyalama hızı açısından FTK Imager yazılımından daha başarılı olduğu tespit edilmiştir. Hesaplanan hash değeri bakımından ise her iki yazılımla da aynı sonuç elde edilmiştir. Ancak hangi yazılımın adli bilişim incelemelerinde daha etkin olduğunun tespiti için bu konuda daha fazla araştırma yapılmasına ihtiyaç vardır.

KAYNAKLAR

[1] İnternet: ''Vikipedi Özgür Ansiklopedi'', 2012 http://tr.wikipedia.org/wiki/Adli_bili%C5%9Fim/, 10 Ekim 2012.

[2] R. Ceylan, A.S. Şirikçi, ''Bilişim Teknolojileri İncelemeleri- Veri İncelemeleri'', **Adli Bilimler,** Cilt 2, Editör: Cihangiroğlu, B., Jandarma Kriminal Daire Başkanlığı Yayınları, Ankara, 152-174, 2011.

[3] B. Carrier, ''Digital Investigation Foundation'', **File System Forensic Analysis**, Editor: Carrier, B., Addison Wesley Professional, NJ, 12-21, 2005.

[4] İnternet: R. Botchek, ''Benchmarking Hard Disk Duplication Performance in Forensic Applications'', (10):1-12, 2008., http://www.google.com.tr/url?sa=t&rct=j&q=benchmarking%20hard%20disk%20duplication%20performance%20in%20forensic%20applications&source=web&cd=1&ved=0CCAQFjAA&url=http%3A%2F%2Fwww.tableau.com%2Fpdf%2Fen%2FTableau_Forensic_Disk_Perf.pdf&ei=vG21ToOmNYeXhQemn_yeBA&usg=AFQjCNGbtrymQrWQJu_d1NqIM5gxPFFd_A&sig2=g6BqMW7UTwNMyWFuu_wh6Q&cad=rja, 05.11.2011.

[5] K. J. Jones, R. Bejtlicj, C.W. Rose, ''Forensic Analysis Techniques'', **Real Digital Forensics: Computer Security And Incident Response,** Editors: Jones, K.J., Bejtlıcj R., Rose C.W., Addison Wesley Professional, NJ, 205-246, 2006.

[6] C. Altheide, H. Carvey, R. Davidson, ''Appendix A'', **Digital Forensics with Open Source Tools,** Editor: Davıdson, R., Elsevier Inc, MA, 241-255, 2011.

[7] D. Garza, ''Data Acquisition and Duplication'', **Computer Forensics Investigating Data & Image Files,** Editor: Garza, D., EC-Council, NY, 65-94, 2010.

[8] İnternet: K.K. Arthur, H.S. Venter, ''An Investigation Into Computer Forensic Tools'',1-9, http://icsa.cs.up.ac.za/issa/2004/Proceedings/Full/060.pdf, 08 Mayıs 2012.

[9] C. Altheide, H. Carvey, R. Davidson, ''Disk and File System Analysis'', **Digital Forensics with Open Source Tools**, Editor: Davıdson, R., Elsevier Inc, MA, 39-67, 2011.

[10] İnternet: AccesData, ''FTK Imager_User Guide 2010'', http://accessdata.com/downloads/current_releases/imager/FTKImager_UserGuide.pdf, 08.05.2012.

[11] İnternet: "Forensic Tools EnCase Forensic", http://whereismydata.wordpress.com/2008/08/10/forensic-tools-encase-forensic/, 10 Ekim 2012.

[12] D. Pettinari, "EnCase Forensic Evidence Acquision and Analysis", **Investigative and Technical Protocols -- EnCase Forensic Imaging and Evidence Acquisition,** Editor: Pettinari, D., 1-3, 2000.

[13] C.Yang, P.Yen, ''Fast Deployment of Computer Forensics with USBs'', **2010 International Conference on Broadband, Wireless Computing, Communication and Applications**, 415, 2010.

[14] S.D. Bassi, **An Automated Acquisition System For Media Exploitation**, Yüksek lisans Tezi, Naval Postgraduate School, 2008.

[15] İnternet: http://guymager.sourceforge.net/, 26.02. 2011

[16] İ. Güneş, ''Kamu Kurumlarında Açık Kaynak Kodlu Yazılımların Kullanılmasının Ekonomik Faydaları: Yerel Yönetimler İçin Pilot Uygulama Önerisi'', *Selçuk Üniversitesi Karaman İ.İ.B.F. Dergisi Yerel Ekonomiler Özel Sayısı*, 161, 2007.

[17] D. Manson, A. Carlin, S. Ramos, A. Gyger, M. Kaufman, J. Treichelt, ''Is the Open Way a Better Way? Digital Forensics using Open Source Tools'', **Proceedings of the 40th Hawaii International Conference on System Sciences**, 9, 2007.