Açık Kaynak en iyisi mi?
Açık Kaynak Araçlar Kullanılarak Adli Bilişim

Dan Manson, Anna Carlin,
Steve Ramos, Alain Gyger, Matthew Kaufman, Jeremy Treichelt

California State Polytechnic University
Computer Information Systems Department
Pomona, California 91768 USA
Email: {dmanson, acarlin, saramos, acgyger, mdkaufman, jdtreichelt}@csupomona.edu

***Çeviren:** Özgür KOCA, (ozgur.koca@linux.org.tr / www.tankado.com),*

Özet

Adli bilişim oldukça zorlu bir alandır. Adli bilişim, adli bilişimin kaideleri açısından olduğu kadar bu sürece yardımcı olan araçlar açısından da önemlidir. Bu makalede adli bilişimde kullanılan açık kaynak kodlu araçlar, iki ticari alternatifi ile avantaj ve dez avantajları yönünden akademik olarak karşılaştırılmıştır. Çalışmanın kapsamı ve gerekliliği iki akademisyen tarafından desteklenen dört kişilik kıdemli öğrencinin oluşturduğu bir ekip tarafından tanımlanarak, açık kaynak yazılımların kullanılması hakkında üç örnek üzerinde durmuş, herbir yazılım aracının (açık kaynak/ticari) performans değerlendirmesi yapılmıştır. Ekip farklı zorluk seviyelerinde aynı sonucların elde edilmesini sağlayan üç ayrı yazılım aracını incelemiştir. Sonuçlar, Açık Kaynak araçların diğer ürünler kullanılarak elde edilen delillerin doğrulanması açısından çok iyi bir başarıma sahip olduğunu göstermiştir.

1. Sunuş

Açık Kaynak Adli Bilişim alanında iyi bilinen uzman bir isim olan Brian Carrier, hali hazırda kullanılan birkaç ticari adli bilişim yazılımının, Açık Kaynak alternatifleri ile bir karşılaştırmasını yayınlamıştır [1]. Carrier'ın Bu yayını SC Magazine'in Eylül 2000 sayısında [2], ve NationalInstitute of Standards and Technology (NIST) 'nin 2001 tarihli Adli Bilişim Araçları Testi (Computer Forensic Tool Testing [CFTT]) adlı çalışmasında yer almıştır [3,4]. NIST tarafından yayınlanan en son çalışma, güncellenmiş bir sınama testi ile sayısal veri toplama araçları için bir uygunluk kriteri metodolojisinin oluşturulması için katkı sağlamıştır [5]. Diğer taraftan, NIST'in daha önce analiz araçlarını sınamak için geliştirdiği bir metodoloji yer almamaktadır. Proje ekibi Sleuth Kit ve Atuopsy gibi açık kaynak alternatifler ile hali hazırda kullanılan EnCase ve FTK gibi ticari ürünlerin incelemesini gerçekleştirmiştir. Proje ekibi bu üç aracı kullanım kolaylığı, sağlamlığı, güvenilirliği ve doğrulanabilirliği açılarından incelemiştir. Ekip üç aracın göreceli başarımını ölçmek için aynı disk görüntüsünün kullanıldığı üç örnek çalışma yapmıştır. FTK Imager ile elde edilen disk görüntüsü ve sonuçlar üç araç arasında da karşılaştırılmıştır. İşletim sistemi kayıt veritabanı dosyaları (Registry)'nın yanında, disk görüntüsündeki diğer dosyalar da analiz edilmiştir. Parola korumalı çalışma sayfaları (Excel Worksheet) ve çalışma kitapları (Excel Workbook) içeren bir disk görüntüsü oluşturulmuştur. Şüpheli disk görüntüsüne ait ana dizine fotoğraf dosyaları, "Program Files" klasörü ve "Documents and Settings" de klasörü dahil edilmiştir. Çalıştırılabilir dosyalar, analiz sırasında dosya uzantısı uyuşmazlığını tetiklemek için bir metin dosyası uzantısı ile (.txt) değiştirilerek yeniden adlandırılmıştır. Tracks Eraser Pro gibi şüpheli bir program ile içeriği bozulmuş (shredded) bir çok dosya da eklenmiştir. Geri dönüşüm kutusu (Recycle Bin) boşaltıldıktan sonra dosya içerikleri bozulmuştur. Sistemde iki e-posta hesabı oluşturulduktan sonra parolanın hatırlansın

seçeneği aktifleştirilerek oturum açılmış ve parolanın sisteme kaydedilmesi sağlanmıştır. Sonuçların tüm araçların aynı bilgileri tespit etmesi açısından inandırıcılığını yansıtması amaçlanmıştır. Sonuçlar ile araçların elde ettiği aynı bilgilerin çeşitli zorluk derecelerindeki inandırıcılık değerileri ortaya koyulmuştur. Örneğin, Autopsy ile SAM veritabanı ayrıştırılırken RegViewer'a, çerezler (Cookies) ve URL adres bilgilerini görüntülemek için ilgili Registry (işletim sistemi kayıt veritabanı) anahtarları içe aktarılmıştır. Oluşturulan disk görüntüsü üç üründe de incelenmiştir. Sleuth Kit ve EnCase yazılımları disk görüntüsünü kısmen makul bir sürede içe aktarmıştır. Diğer taraftan FTK ile tercih edilen seçeneklere bağlı olarak uzun bir içe aktarma süresi geçmiştir. Her üç ürün de MD5 sağlama değerini (Hash) sunmakla beraber SHA1 sağlama değeri sadece Sleuth Kit ve FTK tarafından sunulmaktadır. Sleuth Kit ve FTK incelemeyi yapan adli bilişim uzmanının tüm işlemlerini kayıt altına alırken, EnCase bunu yapmamaktadır. Proje ekibi tarafından, FTK'nın etkili analizler için sezgisel bir grafik kullanıcı arayüzüne (GUI) sahip olduğu EnCase'in ise inceleyicinin daha fazla zamanını alan bir arayüze sahip olduğu tespit edilmiştir. Sleuth Kit içinde kullanılan Autopsy Gezgini (Browser), sadece Windows'a aşina olan ekip üyeleri tarafından kullanılmıştır. Disk bölümü üzerindeki arama, hızlı ve verimli bir şekilde gerçekleştirilebilmelidir.

EnCase'in arama özellikleri diğer iki alternatifi ile karşılaştırıldığında çok daha güçlüdür fakat tüm özelliklerinin kullanılması inceleyicinin daha fazla zamanını almaktadır. EnCase ileri düzey katar (String) ifadeleri, EnCase Scripts (EnCase Betikleri) ve EGREP ile gelişmiş arama özelleştirmeleri yapılmasına izin vermektedir. Bu anlamda proje ekibi bu üç ürünün akademik olarak incelenmesine karar vermiştir

1. Yöntem

Cal Poly Pomona Bilgisayar Sistemleri Bölümü (CIS), çalışmanın değerlendirilmesi için 4 ile 6 öğrenciden oluşan bir danışma kurulu oluşturmuştur. Ekip üyeleri her çeyrekte "yaparak öğrenme" modelli bir eğitimden geçirilmiştir. Bu eğitimlerin içinde programlama, websitesi oluşturma, veritabanı geliştirme, yazılım değerlendirme gibi konular yer alır.

Ulusal bilim vakfı CIS, adli bilişim labaratuvarında kullanılmak üzere Guidance firmasının EnCase Enterprise ve AccessData firmasının Ultimate Kit (UTK) yazılımlarının lisans ücretleri için hibe desteğinde bulunmuştur. UTK, Forensic Toolkit, Registry Viewer, Password Recovery Toolkit, Distributed Network Attack ve FTK Imager yazılım araçlarını kapsamaktadır.

Yukarıda değinilen araçların her ikisi de öğrencilerin indirip kullanabileceği kısıtlı özelliklere sahip tanıtım (demo) sürümlerine sahiptir. Tüm özelliklere sahip sürümleri ise lisans numarasına ve USB kilidine (Dongle) ihtiyaç duyar. Programlar USB koruma kilitleri ve lisans anahtarları nedeniyle labaratuvar ortamında kullanılabilirken, öğrenciler tarafından satın alınamadığı için labaratuvar dışında ve ev ortamında kullanımı çalışmayı sınırlandırmıştır.

Açık kaynak araçlar olan Autopsy ve Sleuth Kit, EnCase ve FTK ile karşılaştırıldığında marjinal maliyetlere sahiptir. Edinme maliyetleri düşünüldüğünde sadece İnternet'ten indirme süreleri ile band genişliği kullanımı ve CD'ye yazma maliyeti ile sınırlı olduğu söylenebilir. Açık kaynak kullanan öğrenciler kendi analizlerini çok düşük maliyetlere gerçekleştirebilirler. Fakat açık kaynak araçlar için kullanıcı yardımı ve desteği düşüktür. Araçlar ile yaşanacak sorunları gidermek için çeşitli topluluklar destek vermekte fakat bu profesyonel bir destek değildir.

Bir öğretim üyesi açısından ticari EnCase ve FTK yazılımları düşünüldüğünde, yardım dökümanları çevrim içi eğitimler ve sık sorulan sorular, teknik dökümanlar ve teknik destek önemli olmaktadır. Öğrenciler sınıf ortamında öğreticinin yönlendirmeleri ile çevrim içi eğitimlere katılabilir, teknik destek ile programların ürettiği herhangi bir çıktı ve sonuç hakkında soru sorabilirler. Eğitici, eğitimlere katılarak yazılımı hızlıca öğrenebilir

ve ortamdaki diğer kullanıcılar ile gelecek için kendi öğrenme ağını oluşturabilir.

Linux hakkında bir deneyime sahip olmadan Açık kaynak araçları öğrenmek pek kolay değildir. Sadece Windows deneyimine sahip bir kullanıcı için bu çok zor bir süreç olabilir. Bu nedenle eğitici kendi öğrenme içeriklerini ve kılavuzlarını hazırlamaya gerek duyabilir. Eğitici, 10 haftalık bu eğitim sürecinde bir teknik destekçi rolünde de yer alır. Öğrenciler tercih ettikleri bir yazılım aracı ile elde ettikleri sonuçları bir diğeri ile doğrulamak için kullanırlar . Buradaki önemli nokta, tüm sonuçların ikinci araç tarafından doğrulanmış olduğundan emin olmaktır.

Bu makelede tartışılan konular ile detaylı CFTT gereksinimleri arasındaki yaklaşım farklılıkları önemli bir noktadır. CFTT gereksinimleri adli bilişim bakış açısıyla eğitim alan deneyimli kişilerin yazma koruması araçlarının kullanmasını ve elde edilen sonuçları yorumlayabilmeyi içerir [5]. Proje ekibi ve müşterilerden elde edilen proje gereksinimleri, proje öncelikleri ve hedefleri, kişisel ihtiyaçlar açısından bir çapraz tablo ile listelenmiştir. Sınırlı girdi ve zaman (4 kısımlı sınıf ve 10 çeyrek hafta) proje ihtiyaç limitlerinin CFTT projesi ile kıyaslanmasını sağlamıştır.

Oluşturulan prosedür ve kategoriler, yazarların projesi ile CFTT'nin hedefleri açısından birçok farklılığını ortaya koymuştur. Projenin hedefi EnCase ve FTK adındaki hali hazırda kullanılan programların, Açık Kaynak eşdeğerlerini değerlendirmektir. Analizde tüm mevcut araçlar aynı disk imajı üzerinde çalıştırılarak, göreceli başarımları değerlendirilmiştir. Aksine, CFTT çalışmasındaki amaç adli bilişim araçlarının sürekliliği, doğru ve tekrarlanabilir test sonuçlarının incelenmesi üzerinedir.

Projenin kısaltılmış olarak 12 ana gereksinimi ile CFTT çalışmasının 26 gereksiniminin karşılaştırması aşağıdaki tabloda verilmiştir.

Projenin İzlenebilirlik Gereksinimleri (Kısaltılmış)	**CFTT İzlenebilirlik Gereksinimleri – İlgili Araçlar Gereklidir (Kısaltılmış)**
1. Kullanıcı yazılım yeteneklerinin karşılaştırabilir	1. Sayısal delilleri elde etme
2. Kullanıcı yazılım yeteneklerini bilir	2. Sayısal delilleri klonlama
3. Kullanıcı yazılım inceleme yeteneklerini bilir	3. Çalışma ortamında kullanılan araçlar
4. Kullanıcı parola koruma araçlarını bilir	4. Tüm görünür veri sektörlerini elde etme
5. Kullanıcı kayıt defteri (Registry) görüntüleme araçlarını bilir	5. Tüm gizli veri sektörlerini elde etme
6. Kullanıcı disk imajı görüntüleme yeteneklerini bilir	6. Veri sektörlerini doğru elde etme
7. Kullanıcı raporlama yeteneklerini bilir	7. Çözünlenmemiş hataları teşhis araçları
8. Kullanıcı Açık Kaynak prosedür ve şartlarını sağlar	8. Amaç çıktıların eksiklerini giderebilme
9. Uygulama ve destek maliyetleri karşılanmıştır	9. İstenen biçimde disk görüntüsünü oluşturma
10. Kullanıcı ticari ve yasal kullanım şartlarını bilir	10. Disk görüntüsü hatalarını tanımlama
11. Kullanıcı gereksinimlerini bilir	11. Yetersiz disk alanı sorunlarını tanımlama
12. Güvenilirlik ve işlevsellik tanımlanmıştır	12. Çoklu disk görüntüsü oluşturma becerilerini tanımlama
	13. Disk görüntüsü bütünlüğünü kontrol etme

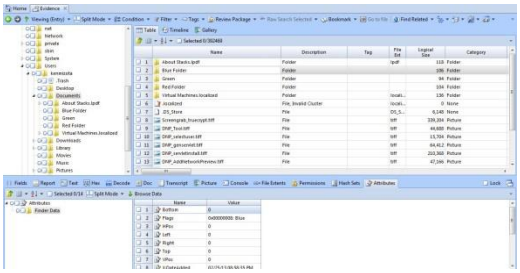
	14. Disk görüntüsü dönüşüm araçlarını kullanma
	15. Hedef aygıtlar arası geçiş araçlarını kullanma
	16. Adli İnceleme sırasında disk klonlama araçlarını kullanma
	17. Disk görüntü dosyasından kopya oluşturma araçlarını kullanma
	18. Disk görüntüsünde kısmı kopya oluşturma araçlarını kullanma
	19. Belirsiz disk bölümlerini kopyalama araçlarını kullanma
	20. Disk silindir referanslı kopyalama araçlarını kullanma
	21. Disk görüntüsünde kullanılmayan veri alanlarını kontrol eden araçları kullanma
	22. Disk görüntüsü oluşturma sırasında kullanılmayan disk alanlarını belirleyebilme
	23. Adreslenmiş disk alanlarındaki yazma hataları
	24. Disk veri bloklarının sağlama değerlerini elde edebilme
	25. Günlük dosyası oluşturmanın detaylarını bilme
	26. Korumasız disk bölümlerinin değişmezliğini saptayabilme

Tablo 1. Projenin ve CFTT adlı çalışmanın gereksinin karşılaştırması [5]

1. Adli İnceleme Yazılım Araçları

1.1. EnCase 1997'de kurulduğudan beri, Guidance Software adli bilişim yazılım ve hizmetleri alanında dünya çapında 20.000'den fazla müşteriye 285 çalışanı ile hizmet veren lider bir şirket oldu [6].

Guidance Software EnCase® paketi altında şirketlere, devletlere ve adli incelemeler yapan kanun güçlerine hizmet veren bir şirkettir [6].



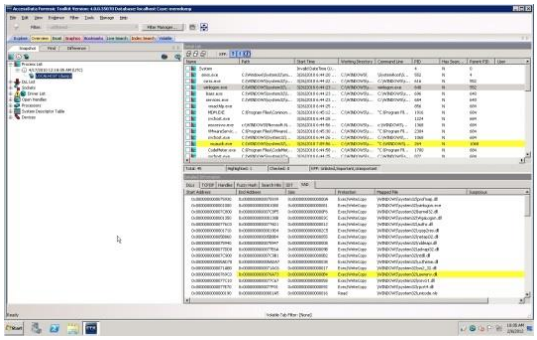
Şekil 1 EnCase Ekran Görüntüsü

Çalışmanın EnCase ön analizinde ürününün şu özellikleri dikkate çekmiştir:

1. FAT, NTFS, ext2, ext3, ReiserFS, UFS ve JFS gibi dosya sistemi formatlarını okuyabilme.
2. Raw (dd), VMWare, EnCase (.E01) ve Safeback gibi disk görüntü dosyalarını okuyabilme.

3. Ağa bağlı EnCase istemcisi yüklü bilgisayarlardan disk görüntüsü elde edebilme.
4. Dahili anahtar kelime arama.
5. EnScript ile detaylı şekilde tüm işlevlerin otomatize edilebilmesi.
6. Diske gözatma, arama ve EnScript olayı analiz etmek için birinci yoldur.
7. Dahili dosya gezgini fotoğraflar gibi birçok popüler dosya formatını görüntülemeye izin verir.
8. Sıkışmış dosya ve dizinleri analiz için indeksleyebilir.
9. Adli inceleme sırasında herhangi bir dosyanın sağlama değerini oluşturabilir.
10. Dahili Registry görüntüleyici.

1.2 FTK AccessData 1987'de kurulduğundan beri sağladığı adli bilişim araçları ile adli bilişim uzmanlarına adli olayların incelenmesi, klonlanması, şifresinin çözülmesi, analiz edilmesi ve raporlanması konularında hizmet vermektedir. Access Data Forensic Toolkit (FTK) kanun güçlerine ve güvenlik uzmanlarına adli bilişim incelemeleri için tam bir paket hizmet sunar [7].

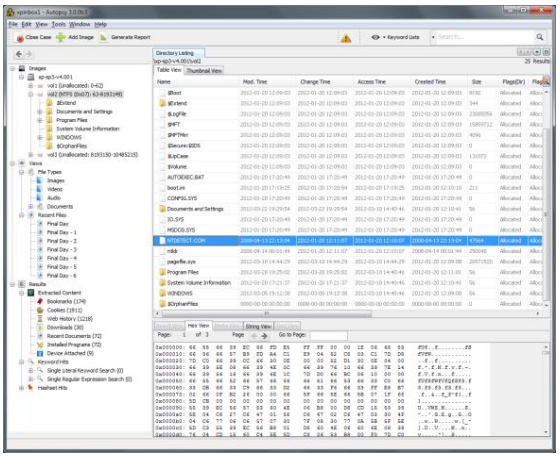


Şekil 2 - FTK Ekran Görüntüsü

Çalışmanın FTK ön analizinde ürününün şu özellikleri dikkat çekmiştir:

1. FAT, ext2, ext3 ve NTFS gibi birçok dosya sistemini okuyabilir.
2. Raw (dd), SMART, EnCase (.E01), Snapback, ve Safeback gibi birçok disk görüntüsü dosya formatlarını okuyabilir.
3. E-posta analizi için çoğu modern e-posta istemci yazılımlarını destekler.
4. Sıkışmış dosya ve dizinleri analiz için indeksleyebilir.
5. Known File Filter (KFF) özelliği inceleyicinin belli dosyalara odaklanabilmesine yardımcı olur.
6. Filitre tabanlı arayüzü, ön programlı filtreleri ile adli olayın incelenmesini sağlar.
7. Dahili dosya görüntüleyicisi inceleyicinin Word, PowerPoint ve Excel dökümanları ve birçok görüntü formatını incelemesinie imkan tanır.
8. Dahili eposta görüntüleyicisi, inceleyicinin istemcisi olmasa bile birçok eposta depolama formatından epostaları görüntüleyebilmesini sağlar.
9. Anahtar kelimeler kullanan arama özelliği.
10. Kayıt defteri görüntüleme ve parola kurtarma gibi

3. Autopsy ve Sleuth Kit Sleuth Kit disk imajlarında ve çalışan/canlı sistemlerde analiz gerçekleştirmek için tasarlanmış ücretsiz bir araçtır. Biri işletim sistemini devre dışı bırakarak dosya sistemlerinde silinen ve gizlenen içerikleri görüntülemek için inceleme gerçekleştirirken, Autopsy Sleuth Kit'e bir grafiksel kullanıcı arayüzü sağlar. Autopsy disk görüntüsü bütünlüğü çıkarma, anahtar kelime araştırma ve işlemleri otomatize etmek için bir adli olay yönetimi özelliği sunar [8].



Şekil 3 - Sleuth Kit Ekran Görüntüsü

Yazılım paketi açık kaynak olduğundan beri, açık kaynak kod yazılımların herkes tarafından incelenmesi ve programcıların yabancı fonksiyonları teşhis edebilmesi gibi avantaj sayılabilecek özelliklere sahip olmuştur.

Proje ekibinin analizleri için bir avantaj da Autopsy'nin bir TCP portu üzerinde çalışmasıdır; böylece birçok öğrenci sunucuya bağlanabilir aynı adli olay üzerinde eş zamanlı olarak çalışabilir. Herbir inceleyici çalışmaya başlamadan önce isimlerini girmeleri gerekir ve tüm günlük kayıtları kendi isimleri ile ayrı bir dosyada tutulur. Böylece herbir inceleyici kendi görev alanları ile ilgili çalışmalarını farklı erişim hesapları üzerinden gerçekleştirebilir [16] .

Yazılım paketinin sadece Sleuth Kit kısmına bakıldığında Dosya Sistemi Katmanı, Dosya Adı Katmanı, Meta Adı Katmanı, Veri Birimi Katmanı, Dosya Sistemi Katmanı, Ortam Yönetimi, Disk Görüntü Dosyası, Disk ve Diğer Araçlar gibi 9 farklı kategori altında 21'den fazla güçlü Linux tabanlı aracı içerdiği görülür [14].

Çalışmanın Autopsy ve Sleuth Kit ön analizinde ürününün şu özellikleri dikkate alınmıştır:

1. Araçlar çalışan bir UNIX sisteminde RootKit'lerce gizlenmiş dosyaların erişim tarihlerini değiştirmeden görüntüleyebilir.
2. NTFS, FAT, ext2fs, ext3fs, UFS, UFS 2 ve ISO 9660 gibi birçok dosya sistemini okuyabilir.
3. Raw (dd), EnCase (.E01), AFF gibi birçok dosya sistemi ve disk görüntü dosyalarını okuyabilir.

4. Karşılaştırma Kategorileri

Sınıflandırma ilgili araçların, adli incelemenin ele geçirme ve analiz aşamalarındaki becerilerini yansıtacak şekilde başarımlarını değerlendirecek kategorilerden seçilmiştir. Bu çalışma sırasında değerlendirmeye alınan kategoriler şunlardır:

- MD5 ve SHA1 sağlama değerlerini hesaplamak
- Herbir dosya için sağlama değeri vermek
- Disk görüntü dosyası bütünlüğünü doğrulamak
- Silinmiş ve şifrelenmiş dosyaları doğru şekilde tanımlamak
- Silinen dosyaları kurtarmak
- Dosya uzantısı uyuşmazlıklarını tanımlamak
- Katar ifadeleri aramak (ASCII ve Unicode olarak)
- HEX kod görüntüleyiciye sahip olmak
- Dosyaları önceden belirlenmiş kategorilere ayırmak
- Fotoğraf galerisi özelliği sunmak
- Dosyaları değiştirme, erişim ve oluşturma zamanlarını göstermek
- Boş/kullanılmayan disk alanlarını tanımlamak
- Kayıt defterinden Çerezleri ve URL geçmişini bulabilmek
- Disk görüntü dosyasını içeri aktarmadaki hızı
- Ön verileri içeri aktarmak

5. Prototipler

Bu çalışmanın birinci amacı hali hazırda kullanılan ticari yazılımların Açık Kaynak alternatiflerini değerlendirmektir. Proje ekibi tarafından gerçekleştirilen üç prototipin sonuçları hibe sağlayaıcısı ile paylaşılmıştır. Aynı disk görüntüsü herbir aracın göreceli başarımını ölçmek için kullanılmıştır. Bu yapılırken aşağıdaki adli bilişim inceleme aşamaları gerçekleştirilmiştir:

- FTK Imager kullanılarak hedef sistemin disk görüntü dosyası oluşturulmuştur
- Sonuçlar herbir aracın ki ile karşılaştırılmıştır
- Açık kaynak araçların kullanılması hakkındaki tavsiyeler akademik dile dönüştürülmüştür

5.1. Birinci Prototip Treo 650 telefonun SD kartından elde edilen disk görüntü dosyasından oluşturulmuştur. Tüm yazılım araçlarında kullanılan Disk görüntü dosyası FTK Imager kullanılarak Raw dd (birebir kopya) biçiminde oluşturulmuştur. Raw disk kopyası orijinal diskin birebir kopyasıdır. Windows'un silme fonksiyonu ve Tracks Eraser adındaki dosya içerik bozucu program dosyaları silmek için kullanılmıştır. Dosya ve dosya uzantıları yeniden anlandırılmış ve dökümanlar parola ile korunmuştur.

Aşağıdakiler başarı ile gerçekleştirilmiştir:

- FTK Imager 2.1a tüm paket yazılımlarda adli disk görüntü dosyasının oluşturulması için kullanılmıştır.
- Karşılaştırma kategorileri tanımlanmış ve detaylandırılmıştır.
- Analizler, yazılım tanımlayabilse de tanımlayamasa da bu kategoriler altında gerçekleştirilmiştir.
- Araçlar için bir sınama yöntemi oluşturulmuştur.

Değişiklikler sonraki prototip de değerlendirilmek üzere tanımlanarak, İnternet çerezleri ve kayıt defteri girdileri gibi işletim sistemi dosyalarını analiz etmek için daha büyük kapasiteli bir disk kullanılacaktır. Karşılaştırmalı inceleme için ek kategoriler tanımlanacaktır.

5.2 İkinci Prototip olarak Windows XP Service Pack 2'ye ek olarak çeşitli dosyalar yüklenmiş 15GB'lık bir disk kullanılmıştır. Disk görüntüsü FTK Image kullanılarak alınmıştır. Autopsy ve Sleuth Kit VMWare sanallaştırma ortamı kullanılarak sınanmıştır. VMWare bir fiziksel bilgisayarda aynı anda birçok işletim sistemi çalıştırmaya izin verir.

Disk görüntü dosyası VMware ortamına aktarılması nedeniyle bozulmuştur. Disk görüntü dosyasının bütünlüğünün teyidi için kullanılan sağlama değerleri doğrulanmıştır fakat disk görüntü dosyasının yeniden oluşturulması gerekmiştir. Sayısız yeniden başlatma ile disk görüntüsü oluşturma adımları disk bölümünün boyutunun büyük olması nedeniyle kısıtlı olarak sınanabilmiştir.

Sanallaştırma ortamı adlı bilişim inceleme yazılımları için ayarlamalara gerek duyar. Fiziksel sürücüler sanal sürücülere ek olarak sanallaştırma ortamına mutlaka bağlı olmalıdır. Ayrıca Linux ortamlarında boşluk karakterlerinin dosya patikalarında yol açtıkları sorunlar ve root kullanıcısı erişim izinlerine sahip bu ortamlarda çalışmak zorluklar getirir.

Son prototipte, esas delil diski bir işletim sistemi yüklenebilecek boyuta indirgenmiştir. Windows XP sadece 2GB'lık disk alanı kaplar. Boyutu sınırlandırmak disk görüntüsü oluşturmak için harcanan süreyi de kısaltacaktır. Sanallaştırma sınama ortamında, adli bilişim incelemesi için yapılması gereken değişikliler araştırılmıştır.

5.3 Üçüncü Prototip Tüm paket programlarda kullanılmak üzere, FTK Imager ile 4 GB'lık Raw dd biçimli bir disk görüntü dosyası oluşturulmuştur. Paket programlar FTK 1.61a, EnCase 5.05C, Autopsy 2.06, Sleuth Kit 2.03 ve VMWare EXP build 23869 'dan oluşmaktadır. Autopsy ve Sleuth Kit VMWare sanallaştırma ortamı kullanılarak sınanmıştır.

Sabit disk Windows XP SP2'ye ek olarak üzerine çeşitli dosyalar da yüklemiştir. FTK, EnCase ve Autopsy arasında yapılan karşılaştırmalı inceleme için analiz dosyalarını eklerken ve disk görüntü dosyasını oluştururken şu adımlar takip edilmiştir:

1. İçerisinde resim ve metin olan Workbook1.xls oluşturulmuştur
2. Çalışma sayfası 1dFa466Cis parolası ile korunmuştur
3. Çalışma kitabı 123qwe456RTY parolası ile korunmuştur
4. Workbook1.xls sabit diske eklenmiştir
5. _41463750_gal_map.jpg ve 20051130-0361_RPH_large.jpg diske Program Files klasörüne eklenmiştir
6. dawn7a.jpg, georg-profile.png ve IMG_3492.jpg diskin kök klasörüne yüklenmiştir
7. lake.louise.1.gif, newyork.jpg ve vwboard.jpg Documents and Settings klasörüne yüklenmiştir
8. fileshred.exe diskin kök klasörüne yüklenmiştir
9. fileshred.exe, fileshred.txt olarak yeniden adlandırılmıştır
10. newyork.jpg ve dawn7a.jpg diskten silinmiştir
11. Tracks Eraser Pro 5.7 kurulmuştur
12. georg-profile.png, Tracks Eraser Pro 5.7 ile iki tur bozulmuştur
13. _41463750_gal_map.jpg Tracks Eraser Pro 5.7 ile iki tur bozulmuştur
14. Geri dönüşüm kutusu boşaltılmıştır
15. MS Internet Explorer 6.0.2900.xpsp_sp2_rtm.040803-2158 ile internete girilmiştir
16. thinkgeek.com sitesinde kullanıcı adı: swingtime_45@hotmail.com, parolası: forensics olan bir hesap oluşturulmuştur.
17. slashdot.org sitesinde kullanıcı adı: forensics, parolası: forensics olan bir hesap oluşturulmuştur.
18. Her iki hesaba da MS Internet Explorer ile oturum açılmış parolalar tarayıcıya kaydedilmiştir.

6. Sonuçlar

6.1 Çeviklik Başarımı Üç aracın da işlevselliğine ilişkin şunlar elde edilmiştir:

1. EnCase'in öne çıkan karakteristik özellikleri şöyle tanımlanmıştır:
- İnceleyicinin etkin bir analiz yapabilmesi için daha fazla eğitim süresini gerektirir
- Arama işlevleri kafa karıştırıcı hal alabilir
- İnceleme oturumu içerisinde inceleyicinin yaptığı işlemlerin kaydı tutulmaz
- Katar ifadeleri, EnScript dilinin komutları, GREP ve filtreler ile gelişmiş arama özelleştirmelerine izin verir
- Şifrelenmiş dosyaları koklaylıkla tespi edemez
- Çoğu işlev "Dosya tipine göre sıralama" yı gerekitirir
- Uygun bir analiz için disk görüntüsünü içeri aktarma ve dosyaların sağlama değerlerini oluşturmayı arka planda gerçekleştirebilir

2. FTK'nın öne çıkan karakteristik özellikleri şöyle tanımlanmıştır:
- Programın kullanılması için gerekli eğitimin süresinin az olması
- Daha hızlı analizler için sezgisel bir GUI tasarımına sahip olması
- Uzun içeri aktarma işlemi ile dosya içeriklerinin analizni kısıtlaması

3. Autopsy ve Sleuthkit'in öne çıkan karakteristik özellikleri şöyle tanımlanmıştır:
- Şifreli dosyaları kolayca testpit edememe
- Çoğu işlev "Dosya tipine göre sıralama" yı gerekitirir

- Üzerine tekrar yazılmış dosyalarda kötü tanımlama
- PERL betik dili ile ve Linux ortamının yardımı ile yeteneklerin olağanüstü düzeyde özelleştirilebilmesi
- Diğer Linux araçları ile birlikte çalışabilme

6.2 Güvenilir ve doğrulanabilir sonuçlar

	Kategori	**EnCase**	**FTK**	**Autopsy**
1	MD5 sağlama değerini kullanır	Birkez taradıktan sonra - Evet	Evet	Evet
2	SHA1 sağlama değerini kullanır	Hayır	Evet	Evet
3	Her dosya için sağlama değerini gösterir	Birkez taradıktan sonra - Evet	Evet	Evet
4	Disk görüntü dosyası bütünlüğünü doğrular	Evet	Evet	Evet
5	Silinen dosyaları bulur	Evet	Evet	Evet
6	Silinen dosyaları sorunsuzca tespit eder	Evet	Evet	Evet
7	Silinen dosyaları kurtarır	Üzerine yazılmamışsa - Evet	Üzerine yazılmamışsa - Evet	Üzerine yazılmamışsa - Evet
8	Şifreli dosyaları tespit eder	Evet	Evet	Evet
9	Şifreli dosyaları sorunsuzca tanımlar	Hayır	Evet	Hayır
10	Dosya uzantısı uyuşmazlıkları tespit eder	Uzantısı değiştirilenler seçeneği kullanılırsa - Evet	Evet	Uzantısı değiştirilenler seçeneği kullanılırsa - Evet
11	Katarlar için arama yapabilir (ASCII ve Unicode)	Evet	Evet	Evet
12	Hex görüntüleyici vardır	Evet	Evet	Evet
13	Dosyaları önceden belirlenmiş kategorilerde sınıflandırır	Evet – “Filtreler” / “Koşullar”	Evet	Dosya tipine göre sıralama yapılırsa - Evet
14	Fotoğraf galerisi görüntüler	Evet	Evet	Dosya tipine göre sıralama yapılırsa - Evet
15	Dosyaların değiştirme/erişim/oluşturma zamanlarını gösterir	Evet	Evet	Evet
16	İnceleyicinin analiz aktivitelerinin kaydını tutar	Hayır	Evet	Evet
17	Boş/kullanılmayan alanları analiz ve teşhis eder	Evet	Evet	Evet
18	Üzerine yazılmış dosyaları bulur	Evet	Evet	Evet
19	Üzerine yazılmış dosyaları tanımlar	Evet	Evet	Yalnızca dosya adına göre

6.3 Kullanım kolaylığı Programların kullanılabilirliği kullanıcının bilgisayar bilgisi ile bağıntılıdır. Örneğin Sleuthkit/Autopsy Linux deneyimi olan kullanıcılar için kullanılması kolaydır fakat sadece Windows ile çalışmış olanlar için zor olabilir. FTK’nın kullanımı temel adli bilişim bilgisi olan ve bilgisayarın arka planını bilen birçok insan için kolaydır. EnCase’in kullanımı EnScript, eksik yardım dosyaları ve genel kullanıcı arabirimi açısından çoğu kimse için

zordur. Bu nedenlerle programın kullanılabilirliğini ölçmek kişilerin bilgi ve birikimlerine göre değişkenlik gösterebileceği için bu ölçütü belirlemek zordur.

6.4 Destek Sorunları EnCase ve FTK gibi ticari ürünler için ödenen ücretin içerisinde destek hizmeti de yer alır. Her iki şirket de yeterli zamanda programlarla ilgili sorunları çözmek için teknik destek grubu ve mesaj listeleri/forumlar a sahiptir. Her iki şirkette ürünlerinin özelliklerinin yer aldığı kullanım kılavuzlarını ve yardımcı işlem basamaklarının yer aldığı belgeleri sunarlar.

Açık kaynak alternatifler için destek konusu ise daha sınırlıdır. Program için sorun gidermede yardımcı olan bir topluluk vardır ve fakat bu hizmet profesyonel seviyede değildir. Sleuth Kit/Autopsy paketi kendini kanıtlamaya devam ettikçe, popülaritesinin artırmaya ve belgeleme eksikliklerinde mesafe katetmektedir. Belgelemelerdeki eksiklikler, kullanılan araçların hali hazırda Linux kullanıcılarının işletim sisteminden bildiği komutları kullanmasından kaynaklanmaktadır. Diğer taraftan bu özellik grafik arayüze bağımlı Windows kullanıcıları için çok yıldırıcı olabilir. Autopsy'nin istemci kısmı grafikseldir fakat hala ana işlevleri komut satırından kontrol edildiğinden, Windows kadar kullanıcı dostu bir arabirime sahip olmaması bu anlamda bir dönemeç noktasını oluşturur.

7. İleri Düzey Araştırma Tavsiyeleri

Bu çalışmada, bir adli inceleme sırasında araştırmacıya açık kaynak adli bilişim araçlarının kullanılması hakkında daha fazla güven vermek için bir araştırma ve kapalı kaynak kod yazılımlar ile karşılaştırma analizi gerçekleştirilmiştir.

Bu araştırma güvenilir ve yetkili kuruluşlar tarafından gerçekleştirilmiştir. Bu devlet kuruluşları Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) , Savunma Bakanlığı (DoD) [10] ve Adalet bakanlığıdır. Diğer güvenilir organizasyon ve kuruluşlar içerisinde enstitüler, devlet kurumları, yetkili okullar, ticaret birlikleri ve firmalar yer alır.

NIST tarafından gerçekleştirilen Adli Bilişim Araçları Testi adlı araştırma projesinde, incelenen araçlar sınırlı kalmıştır. İlgili calışmada açık kaynak adli bilişim araçlarından sadece, disk görüntüsü oluşturmak için kullanılan dd aracı incelenmiş, iki kez, iki farklı platform üzerinde sınanmıştır [3].

Çeşitli sınama paketleri oluşturmak adli bilişim yazılımlarını derecelendirmek için kullanışlı olabilir. Sleuthkit/Autopsy, FTK ve EnCase programlarının son sürümlerinden oluşan bir sınama paketi ile standardize edilmiş bir disk görüntü dosyası kullanarak her bir yazılımı derecelendirmek için yeterli olacaktır. Bu disk görüntü dosyası özenli şekilde oluşturulmuş ve ilgili yasal standartlara uygun olmalıdır.

Daha ileri düzey bir araştırma, yazılım programlarının kullanılabilirlik ve kararlılıkları gibi teknik açılardan nasıl karşılaştırılabileceği ile ilgili olabilir. Ancak herbir programın kullanılabilirliği kendi yeteneklerinin genişliği açısından çeşitlilikler gösterecektir. Temel teori, bir disk görüntü dosyasının bu araçlardan herhangi biri ile etkin şekilde incelenmesidir.

Temel teori, bu araçları kullanarak disk görüntü dosyasının içindeki disk ve bölümleri, dosya değişiklik süreçlerini, şifrelemiş ve diğer disk alanlarını etkin şekilde inceleyebilmelidir. Temel düzeyde bilgi olmadan sabit diskin incelenmesi, istenmeyen durumların oluşmasına neden olarak başka hiçbir program tarafından incelenememesine de neden olabilir.

Her bir programın kararlılığı donanım, işletim sistemleri, kullanıcı deneyimi, ortam koşulları, disk görüntüsünün kalitesi, disk görüntüsünün temiz olması (örn. virus enfoksiyonları, zararlı yazılımlar, spyware, adware vs) ve diğer faktörlere derinden bağlıdır. Yapılacak incelemede tüm bu faktörlerin izole edilememesi, kararlılığın ölçülmesini zorlaştıracaktır. Windows ve Linux tabanlı işletim sistemleri tüm bu programları çalıştırmak için kullanılamaz. Windows virüsleri bulunduran disk görüntü dosyaları, Windows tabanlı programların tüm ortamın kararlılığını etki edebilecek sorunlara yol açmasına neden olabilir. Linux tabanlı işletim sistemleri, Windows'da olduğu kadar tüm donanım üreticilerinin firmware ve sürücü desteğine sahip değildir.

Bu tarz sınamalar gerçekeltirirlebilir fakat her yapılan sınama kontrol edilemeyen birçok faktör tarafından etkilenecek ve her seferinde değişik sonuçlar verebilecek, bu da sınama ortamının ve prosedürlerinin tutarsız sonuçlar üretmesine neden olacaktır. Bundan dolayı proje ekibi bu tarz sınamalar üzerinde durmamıştır.

Bu raporda, içerisinde yazılımların kalitesini artıran Linux için Air ve DD grafik arayüzü ve/veya DCFLDD [12] ile Windows kayıt defteri için RegViewer[13] gibi ek yazılımlar değerlendirilmiş ve önerilmiştir. Gelecekteki incelemeler Autpsy sunucusunda çoklu inceleyici oturumlarını ve tüm yazılım paketleri hakkında detaylı raporlamaları içerebilir.

8. Sonuç

Bu proje Sleuth Kit ile EnCase ve FTK'yı elde ettikleri deliller açısından karşılaştırmıştır. Proje ekibi Sleuth Kit'i kolay kullanılabilir, güçlü fonksiyonlara sahip, güvenlilir ve doğrulanabilir sonuçlar sunduğuna karar vermiştir. Ayrıca sınıf ortamında açık kaynak araçların kullanımı da değerlendirilmiştir.

Ayrıca, aynı disk görüntüsü herbir yazılım aracının önceden belirlenen değerlendirme kriterlerine göre göreceli başarım ölçümünü yapmak için kullanılmıştır. Ekip tarafından yapılan üç prototipten elde edilen sonuçlar hibe sağlayıcı kuruluşlar ile de paylaşılmıştır.

Araçlar tarafından sunulan sonuçlar değişik seviyelerde farklılıklar içermiştir. Örneğin EnCase ve FTK fotograflar için otomatik olarak bir galeri sunarkern Autopsy bu özelliği dosya türüne göre sıralama yaptırdıktan sonra sunmuştur. Elde edilen disk görüntü dosyası her üç üründe de içe aktarılmıştır. SleuthKit ve EnCase disk görüntü dosyasını makul bir sürede içer aktarmıştır. Diğer taraftan FTK, seçilen içe aktarma seçeneklerine bağlı olarak daha uzun bir sürede içe aktarmıştır. Her üç ürün de MD5 sağlama değerini sunmuş yalnızca Sleuth Kit ve FTK, SHA1 sağlama değerini sunmuştur. Sleuth Kit ve FTK inceleyicinin yaptığı tüm işlemlerin kaydını tutabilirken EnCase bunu yapmamaktadır.

EnCase ve FTK kullanılırken Grafik Kullanıcı Arabirimi (GUI) ekip öğrencilerinin araştırması sırasında sıcak bir tartışma konusu olmuştur. Proje ekibi, EnCase'in kullanımı için daha fazla eğitime ihtiyaç duyulurken, FTK'nın etkili bir analiz gerçekleştirebilecek sezgizel bir arayüze sahip olduğu doğrulamıştır.

Delil aramak bazen bazen samanlıkta iğne aramaya benzer. Bir disk görüntüsünde eleme yapmak hızlı ve etkin şekilde gerçekleştirilebilmelidir. EnCase'in arama özellikleri diğer iki ürün ile karşılaştırıldığında daha güçlüdür fakat tüm özelliklerinin kullanılması bir eğitimi gerektirir. EnCase karakter katarı kuralları, EnScript komutları ve GREP kullanılarak özelleştirilebilen ileri düzey bir arama sistemine sahiptir.

Proje ekibi her üç ürünün de akademik ortamda kullanılabileceğine karar vermiştir. Her araç da akademik ortamda kullanılabilecek kendi güçlü ve zayıf yönlerine sahiptir.

Proje ekibinin sonuçları bir Ubuntu Linux içeren Linux DVD üstünde WMware ve kullanım prosedürlerini içeren sanallaştırma ortamı kullanılarak elde edilmiştir. İstenildiğinde bu DVD'nin kopyası verilebilir. Ek olarak, yazarlar, gelecekte diğer enstitü üyeleri ile açık kaynak ve ticari yazılım ve donanımlarının inceleme ve karşılaştırmasını yapmaktan mutluluk duyacaktır.

Yazarlar adli araçların güvenilirliğinin yayın, inceleme ve resmi sınamalar sayesinde dahada artacağını kabul ederler [1]. Açık kaynak yazılımlar adli bilişimde en geniş kullanıma sahip araçlar olmaya devam edecektir [15]. Bu çalışmada elde edilen sonuçlar bu yönde atılmış bir adımdır.

SleuthKit/Autopsy gibi araçlar bir delil dosyasından delil elde etme gibi hayati öneme sahip belli görevleri yerine getirirken çok iyi başarımlar sunarken bir diğeri aynı başarımı sağlamayabilir.

Diğer taraftan adli bilişim kendini kanıtlamış teknolojiler arasındaki çekişmeden ziyade bir adli soruşturmada sanığın delillerini güvenilir şekilde elde etmeyi amaçlamalıdır. Bu nedenle açık ve kapalı kaynak kod programlar birlikte çalışıp, birbirlerinin sonuçlarını doğrulayarak adeletin yerinin bulmasının sağlanması önemlidir. Bu şu anlama gelir; kapalı kaynak kullanıcıları mutlaka açık bir zihne sahip olmalı, tercihen açık kaynak gibi diğer araçları da denemeli ve sonuçlarını teyit etmelidir. Bir açık kaynak araç kapalı araç ile aynı sonuçları üretiyorsa, açık kaynak aracın kaynak kodları incelenerek doğru çalıştığından emin olunabilir. Bu nedenle kapalı kaynak kodlu araçların kodlarının da incelemeye gerek olmadan doğru çalıştığından emin olunabilir [16]

9. Kaynaklar

[1] Carrier, Brian, OpenSource Digital Forensic Tools: The Legal Argument, @stake Research Report, October 2002.

[2] James Holley. Computer Forensics Market Survey. SC Magazine September 2000.

Şu adresten edinilebilir: http://www.scmagazine.com/scmagazine/2000_09/survey/survey.html

[3] NIST. Computer Forensics Tool Testing. Şu adresten edinilebilir: http://www.cftt.nist.gov/

[4] NIST CFTT. Disk Imaging Tool Specification, 3.1.6 Edition, Şu adresten edinilebilir: http://www.cftt.nist.gov/DI-spec-3-1-6.doc.

[5] Digital Data Acquisition Tool Test Assertions and Test Plan, November 10, 2005. Şu adresten edinilebilir: http://www.cftt.nist.gov/DA-ATPpc-01.pdf.

[6] Guidance Software, maker of EnCase, provides Incident Response and Computer Forensics Solution, ExpertForensic Services and Computer Forensic Training. Şu adresten edinilebilir: http://www.guidancesoftware.com/.

[7] Welcome to Access Data! Şu adresten edinilebilir: http://www.accessdata.com/.

[8] The Sleuth Kit & Autopsy: Digital Investigation Tools for Linux and other Unixes. Şu adresten edinilebilir: http://www.sleuthkit.org/.

[9] E-mail response from Gregory Carlton, 5/26/2006.

[10] DoD Cyber Crime Center. Şu adresten edinilebilir: http://www.dc3.mil/.

[11] National Institute ofJustice – Electronic Crime Şu adresten edinilebilir: http://www.ojp.gov/nij/topics/ecrime/welcome.html

[12] Air: Automated Image and Restore. Şu adresten edinilebilir: http://air-imager.sourceforge.net/.

[13] SourceForge.net: regviewer. Şu adresten edinilebilir: http://sourceforge.net/projects/regviewer/.

[14] Carrier, Brian. The Sleuth Kit: Tool Details. Sleuthkit.org. 13 Feb. 2006 http://www.sleuthkit.org/sleuthkit/tools.php

[15] Byfield, Bruce. The two-edged sword: Legal computer forensics and open source. 11 April. 2005. News Forge. 13 Feb. 2006 http://software.newsforge.com/software/05/04/05/2052235.shtml

[16] Gyger, Alain. Sleuthkit/Autopsy: An Open Source Forensic Package. February 15, 2006.