International Journal of Human Sciences
ISSN:1303-5134

Volume: 13 Issue: 1 Year: 2016

The keyword search method and its importance in computer forensics

Adli bilişimde anahtar kelime araması metodu ve önemi

Hüseyin Çakır[1]
Mehmet Serkan Kılıç[2]

Abstract

In this study "keyword search method" used in the filed of digital forensics sciences is investigated. Similar to using search engines on internet investigations, using keyword search method of computer forensics investigations has too much benefits. In the study, keyword search method loop of preparing of electronic data, indexing, query with keywords, matching on database and showing results to the users are explained. Also information of keyword search method on different data type such as forensic image data, live forensics data, static data and cloud computing data are discussed.

The importance of using keyword search method on computer forensics is examined in 5 different aspect as rapid and effective computer forensics investigations, contribution to privacy, relational analysis of human-event-computing device, creating dictionary for decrypt passwords and recover some deleted data and detect steganography data. In this context, all-round about using keyword searches' contribution to computer forensics investigation are evaluated. Finally, some examples about computer forensics tools are handled.

Keywords: Computer Forensics, Electronic Data, Keyword Search, Electronic Evidence.

(Extended English abstract is at the end of this document)

Özet

Bu çalışmada, adli bilişim biliminde kullanılan "anahtar kelime araması metodu" incelenmiştir. İnternet araştırmalarında yaygın olarak kullanılan arama motorlarına benzer şekilde adli bilişim çalışmalarında da anahtar kelime araması metodu kullanılmasının çok faydası bulunmaktadır. Çalışmada; elektronik verilerin hazırlanması, verilerin indekslenmesi, anahtar kelimeler sorgusu, veri tabanı üzerinde eşleştirme yapılması ve kullanıcıya sonuçlarının gösterilmesi şeklinde oluşan anahtar kelime araması metodu açıklanmış ve adli kopya verileri, canlı sistem verileri, sabit veriler ve bulut bilişim verileri üzerinde anahtar kelime araması hakkında bilgi verilmiştir.

Adli bilişim çalışmaları sürecinde anahtar kelime araması metodunun kullanımının önemi; hızlı ve etkili bir adli bilişim çalışması yapılması, özel hayatın gizliliğine katkı sağlaması, şahıs-olay-bilgisayar medyası arasında ilişki analizi kurulması, sözlük oluşturulması ve şifre tespiti ile silinmiş ve gizlenmiş verilerin tespiti olmak üzere 5 farklı açıdan irdelenmiştir. Bu bağlamda anahtar kelime araması metodunun elektronik delil elde etme çalışmalarına sağlayacağı katkı çok yönlü olarak ele alınmış ayrıca adli bilişim yazılımları özelinde örnekler verilmeye çalışılmıştır.

Anahtar Kelimeler: Adli Bilişim, Elektronik Veri, Anahtar Kelime Araması, Elektronik Delil.

[1] Yrd. Doç. Dr., Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim ABD, hcakir@gazi.edu.tr
[2] Dr., Gazi Üniversitesi, Bilişim Enstitüsü, Bilişim Sistemleri ABD, mserkanklc@hotmail.com

Çakır, H., & Kılıç, M. S. (2016). Adli bilişimde anahtar kelime araması metodu ve önemi. *International Journal of Human Sciences*, *13*(1), 2368-2384. doi:10.14687/ijhs.v13i1.3401

1. Giriş

Gelişen teknoloji ile beraber hayatın her alanına giren bilgisayar medyaları, suç işleme aracı veya amacı olarak kullanılabilmektedir. İnternet sitesi saldırısı, online dolandırıcılık gibi doğrudan bilişim sistemleri ile ilgili suçların yanı sıra hırsızlık, cinayet, tehdit vb. bir çok geleneksel suçta da bilgisayar medyaları kullanılmaktadır. Bir cinayet olayında maktülün kişisel bilgisayarı ve cep telefonunun incelenmesi; şüphelinin tespiti ve olayın meydana geliş sebebinin anlaşılmasına yardımcı olacak ve maddi gerçeğin ortaya çıkarılmasına katkı sağlayacaktır.

Bu noktada, adli bilişim bilimi devreye girmekte, olası delil kabül edilen doneye herhangi bir zarar getirmeksizin, onu ceza yargılaması mekanizmalarına sunma fonksiyonunu üstlenmektedir (Özbek, 2009:2). Bu bağlamda adli bilişim, maddi gerçeğin ortaya çıkarılabilmesi amacıyla laboratuvar ortamında bilgisayar medyaları üzerinde incelenme yapılması, mevcut elektronik veriler ile suç arasında illiyet bağı bulunup bulunmadığının tespit edilerek raporlanması işlemidir. Teknolojik gelişmelere bağlı olarak artan bilgisayar kapasitesi, çeşitlenen elektronik veriler (internet kalıntıları, farklı Office yazılımları, IM uygulamaları…) ve makul sürede adli bilişim çalışmalarının tamamlanması isteği; adli bilişim uzmanlarının farklı yöntemler kullanmasını zorunlu kılmaktadır.

TDK sözlüğüne göre; "bir yazıda konuyu en açık bir biçimde yansıtan kelime veya kelime grubu" olarak tanımlanan anahtar kelime kavramı; adli bilişim disiplini açısından tüm dokümanlar üzerinde arama yapılarak ilgili verilerin belli bir mantık sırası ile adli bilişim uzmanına sunulmasında kullanılan kelimelerdir. Anahtar kelime araması ile doğrudan araştırma konusu ile ilgili sonuçlara ulaşılabilmesi için belirlenecek anahtar kelimelerin özel ve nitelikli olması gerektiği açıktır.

Kelime arama işlemi ile tek tek veya liste halinde verilen kelimeler, diskin bütününde (slackspace, swap space, unallocated space, volume slack, vb.) aranmakta ve sonuçlar liste halinde elde edilmektedir. Bu işlem ile diskin şüpheli tarafından suç ile ilgili bir konuda kullanılıp kullanılmadığı tespit ediebillmekte, eğer kullanılmışsa diskin hangi bölümünde hangi tür verinin bulunduğu öğrenilebilmektedir (Şen, 2005:39). Veri tabanlarında ise anahtar kelime ile arama yapılması daha karmaşıktır. İstenilen bir bilginin tek bir tablo yerine bir kaç tabloya dağıtılmış şekilde tutulması veri tabanlarında anahtar kelime aramasını güçleştirmektedir (Demircioğlu, 2012:1). Yine de anahtar kelime aramasının geleneksel inceleme yöntemlerine göre büyük kolaylık ve zaman tasarrufu sağladığı genel kabül görünmektedir.

Bilginin elde edilmesi, sorgu sonucu ile ilgili dokümana ulaşılmasıdır. Arama sonuçlarının listelenmesi ve dokümanların görüntülenmesi ile bilgiye ulaşma ihtiyacı giderilmektedir. Bilinen en yaygın web tabanlı bilgiye ulaşma aracı ise arama motorlarıdır (Welson vd., 2010:13). Gerçekten de, adli bilişim yazılımları tarafından kullanılan anahtar kelime arama metodu büyük ölçüde web tabanlı arama işlemine benzemektedir. Günümüzde arama motorları "arama-sonuç gösterme" nin ötesine geçmiş ve İngilizce "Advertising Words"'un kısaltması olan AdWords yani "Sponsor Edilmiş Bağlantılar" sisteminin hayata geçmesine sebep olmuştur. Buna göre kullanıcılar tarafından yapılan aramalara (kullandıkları anahtar kelimelere) bağlı olarak işletmelere ait ticari web sayfaları kullanıcıya sunulmakta ve bu sayfalara kullanıcılar yönlendirilmektedir. Arama motorlarının temel gelir kaynaklarından birisini oluşturan bu sistem; kullanıcıların hızlı ve etkili bir şekilde bilgiye ulaşma isteğinin ticari zeka ile değerlendirilmesidir. Sonuç olarak anahtar kelime araması, bir ihtiyaç olarak ortaya çıkmış olup kullanım alanı gün geçtikçe yaygınlaşmaktadır.

2. Anahtar Kelime Araması Metodu

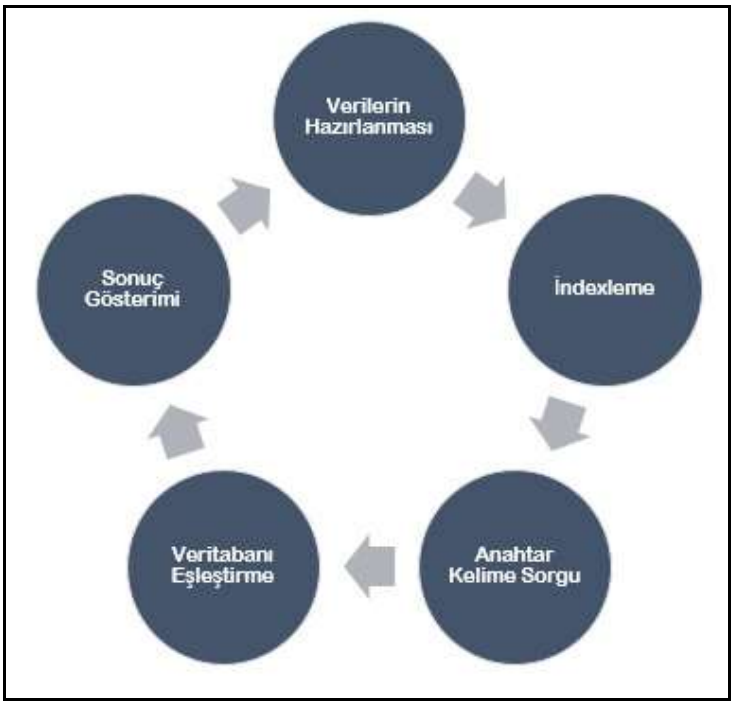
Bilgisayar medyaları üzerinde yapılacak adli bilişim çalışmaları metodundan birisi de anahtar kelime aramasıdır. Bu metot; öncelikle üzerinde arama işlemi yapılacak elektronik verilerin hazırlanması, verilere daha hızlı ulaşılabilmesi için indekslenmesi, daha önce belirlenen anahtar kelimeler ile sorgu yapılması, sistem tarafından indekslenen kelimelerin yer aldığı veri tabanı üzerinde eşleştirme

Çakır, H., & Kılıç, M. S. (2016). Adli bilişimde anahtar kelime araması metodu ve önemi. *International Journal of Human Sciences*, *13*(1), 2368-2384. doi:10.14687/ijhs.v13i1.3401

yapılması ve kullanıcıya sonuçlarının gösterilmesi şeklindedir. Anahtar kelime arama metoduna ait döngü Şekil-1'de gösterilmiştir.

Bilgisayar medyaları üzerinde Office dosyaları, PDF dosyaları, sistem kayıt defteri (registry), internet kalıntıları, resim-video gibi dosyalara ait üstveri bilgileri, sıkıştırılmış dosyalar, link dosyaları gibi farklı uzantı, format ve veri tiplerine sahip elektronik veriler yer almaktadır. Bu veriler üzerinde arama işlemi yapılabilmesi için öncelikle bu verilerin hazırlanması gerekmektedir. Bu veriler, incelenecek bilgisayar medyasının birebir kopyası olan adli kopya (imaj) dosyası içerisinde olabileceği gibi klasör yapısı halinde bulunan sabit dosyalar da olabilmektedir. Benzer şekilde canlı sistem veya bulut bilişim üzerinde de bulunuyor olabilir.

İndexleme işlemi; hazırlanan veriler üzerinde anahtar kelime araması yapılması ve sonuçlara hızlı şekilde ulaşılabilmesi için verilerin belli algoritmalar doğrultusunda kategorize edilmesi ve veri tabanına kaydedilmesidir. Mevcut veriler haricinde oluşan indeks verileri; bir kitabın içindekiler bölümü gibi kelime-doküman adı (yeri) eşleştirmesi içerir.



Şekil 2.1: Anahtar Kelime araması Metodu Döngüsü

Kullanıcı açısından en önemli aşama ise; anahtar kelime sorgusu işlemidir. Doğrudan konu ile ilgili, nitelikli ve eşsiz kelimelerin belirlenerek sorgu işleminin yapılması ile adli bilişim çalışmasına katkı sağlanacaktır. Bu bağlamda kredi kartı dolandırıcılığı konusunda yapılan bir adli bilişim çalışmasında; "banka", "dolandırıcılık", "sahte" gibi kelimelerin belirlenmesi; hem çok fazla sonuç elde edilmesine hem de konu ile ilgisiz dokümanlara gereksiz yere ulaşılmasına neden olacaktır. Bununla beraber e-posta adresi, telefon numarası, araç plakası gibi kelimelerin anahtar kelime olarak belirlenmesi; nitelikli sonuçlara ulaşılmasını sağlayacaktır.

Adli bilişim yazılımlarında bulunan regular expression (belirli ifade araması) özelliği, banka hesap numaraları, kredi kartı numaraları, vatandaşlık numarası, telefon numarası, IP numarası vb. arama tiplerinde aramayı çok kolay bir hale getirmektedir. Adli bilişim uzmanlarınca, en çok kullanılan arama kelimeleri için regular expression değerlerinin belirlenmesi, incelemek üzere yeni olaylar geldiğinde zaman tasarrufu sağlayacaktır (Aydoğan, 2009:52). Anahtar kelimelerin belirlenmesinde yapılan bir eleştiri, kelimelerin kullanıcının kullanabileceği şekilde ele alınmaması, kelimelerin

Çakır, H., & Kılıç, M. S. (2016). Adli bilişimde anahtar kelime araması metodu ve önemi. *International Journal of Human Sciences*, *13*(1), 2368-2384. doi:10.14687/ijhs.v13i1.3401

varyasyonları ve taksonomilerine dikkat edilmemesi konusudur (Wochna, 2015:859). Birçok kullanıcı günlük hayatta ve akademik literatürde kullanılan terimleri farklı şekilde ifade edebilmekte veya tamamen kendine özgü kelimeler kullanabilmektedir. Bu açıdan anahtar kelimeler belirlenirken suça özgü jargonlara hakim olmak gerekmektedir.

Sistem tarafından gerçekleştirilen veri tabanı eşleştirmesi ve ulaşılana sonuçların kullanıcıya gösterilmesi tamamen İndexleme işleminin kabiliyeti/başarısı ile doğru orantılıdır. Anahtar kelime arama (keyword search) olarak adlandırılan bu işlem bilgisayar imajı üzerinde text arama şeklinde olabileceği gibi hexadecimal değer ile de yapılabilmektedir. Örneğin "ali" kelimesinin el konulan bilgisayar imajı ile ilgisinin tespiti için yapılacak arama işlemi, "ali" kelimesinin text olarak aranması veya 616C6978 hexadecimal karşılığının aranması şeklinde olabilmektedir (Çakır ve Kılıç, 2013:32). Her ne kadar UNIX grep gibi standart arama araçları ile ham binary veri üzerinde anahtar kelime araması yapılması basit bir işlem ise de bu şekilde yapılacak bir aramada istenilen sonuçlara ulaşılamaması mümkündür. Bu eksiklikte, verinin sıkıştırılmış veya şifreli olması, farklı encode yapıda (ASCII, UTF-8, UTF-16, UTF-32, Punycode gibi) olması, üstveri ve etiketlerin veri içerisine gömülmüş olması gibi nedenler bulunmaktadır. Diğer taraftan EnCase[3] ve X-Ways Forensics[4] gibi profesyonel adli bilişim yazılımları ile farklı formatta veriler indekslenebilmektedir (Ali, 2010:1).

2.1. Adli Kopya Üzerinde Anahtar Kelime Araması

Adli kopya alma (imaj alma), bilgisayar medyasının bire bir kopyasının alınması olup bu şekilde alınan kopya, asıl medyadaki tüm verileri (mevcut, silinmiş, gizlenmiş, bozuk gibi) içermektedir. Böylece 500GB boyutunda bir sabit diske ait adli kopyanın sıkıştırma işlemi yapılmamış ise 500GB olması beklenmektedir. Elde edilen adli kopyanın içerisinde 500GB veri olabileceği gibi hiç veri olmaması da mümkündür. Adli bilişim yazılımları özel olarak geliştirildikleri için, mevcut verilerin yanı sıra, silinmiş, gizlenmiş veriler ile sistem dosyalarını da analiz ederek anlamlı hale getirmektedir. Bu bağlamda, adli bilişim yazılımlarından verim alınması ancak, canlı sistem veya adli kopya üzerinde kullanımı ile mümkündür.

Standart dosya kopyalama programları, verileri bir noktadan başka bir konuma taşımakta/kopyalamakta olup delil olabilecek bazı verilerin (silinmiş, sistem verisi olması gibi nedenlerle) kopyalanmaması ve sadece kopyalanan veriler üzerinde adli bilişim incelemesinin yapılması, soruşturmanın eksik yapılmamasına neden olmaktadır (Battula vd, 2009:28). Adli kopya üzerinde adli bilişim çalışması yapmanın bir diğer olumlu yanı; Office dokümanlarının erişim tarihi gibi üstveri bilgilerinin değişmesi, zararlı yazılımlarca istem dışı dosya kopyalanması veya antivirüs programlarca istem dışı dosya silmesi gibi elektronik verilerin etkilenme ihtimallerinin ortadan kalkmasıdır. Anahtar kelime arama işlemi öncesi verilerin indekslenmesi süresince tüm verilere uygulama tarafından erişim sağlanması; dosya erişim bilgilerinin değişmesine neden olacağından delil bütünlüğünün bozulmasına neden olacaktır. Bu açıdan gerek adli bilişim çalışmalarının tamamında gerekse de anahtar kelime arama metodu kullanımında adli kopya üzerinde işlem yapılması önemli ve faydalıdır.

Alınan adli kopyanın sanal makine üzerinde ayağa kaldırılması yani işletim sisteminin çalıştırılması mümkündür. Bunun için LiveView[5] ve VFC[6] (Virtual Forensic Computing) gibi yazılımlar geliştirilmiştir (Bashir ve Khan, 2015:383). İşletim sistemi çalıştırılan bir adli kopya dosyası ile birebir çalışan bilgisayara erişilmiş olmakta ve anahtar kelimesi ile tespit edilen dosyalar yerinde incelenebilmektedir.

[3] https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx
[4] https://www.x-ways.net/forensics/index-m.html
[5] http://liveview.sourceforge.net/
[6] http://www.virtualforensiccomputing.com/

Çakır, H., & Kılıç, M. S. (2016). Adli bilişimde anahtar kelime araması metodu ve önemi. *International Journal of Human Sciences*, *13*(1), 2368-2384. doi:10.14687/ijhs.v13i1.3401

2.2. Canlı Sistem Üzerinde Anahtar Kelime Arama

Canlı sistem; halihazırda çalışan sistemdir. Canlı sistem üzerinde uçucu olarak tanımlanan ve elektrik kesildiğinde kaybolan veriler (RAM, pagefile.sys) ile kriptosu çözülmüş (decrypted) haldeki veriler bulunmaktadır. Özellikle kriptolusu çözülmüş haldeki verilere bir daha erişim sağlanamama ihtimali, bu verilerin önemini ortaya koymaktadır.

Adli bilişim, sadece olay yerinden alınan bilgisayarların incelenmesi ile yeterli delile ulaşamaz. Bu sebeple adli bilişim uzmanları tarafından, canlı sistem incelemeleri ile yeni veri elde etme yöntemleri geliştirilmektedir (Marthie ve Solms, 2008:3). Bilgisayarın kapatılması ile içerisinde yer alan kriptolu verilere ulaşılamayacağından adli bilişim incelemeleri eksik kalmaktadır. Stefan Bolagh ve Matej Pondelik tarafından kopyası alınan (dump) geçici bellek (RAM) veriş üzerinde kripto anahtarlarının elde edilmesi yönünde teknik[7] geliştirmişlerdir (Bashir ve Khan, 2013:37).

Canlı sistem analizinde kullanılan uygulamalara Nigilant32[8] isimli yazılım örnek olarak verilebilir. CD veya USB'den çalışan ve hedef bilgisayara bazı kurulumlar yapan uygulama, uçucu verilerin kopyasını almakta (dump), daha sonra Window Sysinternals tarafından kullanılan dizinlerin çıkarımını (extract) yaparak text dosyalarına kaydetmekte ve kullanıcı adı ve şifre gibi bilgileri analiz etmektedir. Ayrıca bu dosya üzerinde incelemeci tarafından sorgu (anahtar kelime arama işlemi) yapılabilmektedir (Bashir ve Khan, 2015:383). RAM üzerinde bulunan önemli verilerin elde edilebilmesi için Wetstone's LiveWire[9] isimli yazılım ile canlı sistem üzerinde anahtar kelime araması yapılması mümkündür. Bunun için öncelikle bilgisayara fiziksel olarak veya ağ üzerinden bağlantı sağlanarak RAM'e erişilmesi gerekmektedir (Steele vd., 2011:103). Canlı sistem analizinin en zor tarafı, bilgisayar üzerinde yönetici yetkisine sahip olma gerekliliğidir. Yeterli yetki seviyesi olmadan canlı sistem analizine başlanılması, kullanılan yazılımların hedef bilgisayar üzerinde etkili çalışamamasına neden olacaktır (Marthie ve Solms, 2008:10). Bu konuda yapılan bir diğer eleştiri ise, canlı sistem üzerinde anahtar kelime araması gibi adli bilişim işlemlerinin yapılması; bilgisayarda bulunan elektronik verilerin bütünlüğüne zarar verecek ve dosyalara ait üstveri bilgisi başta olmak üzere bazı değişikliklere sebep olacağıdır.

2.3. Sabit Veriler Üzerinde Anahtar Kelime Araması

Sabit veriler; işletim sistemine sahip olmayan USB bellek; CD/DVD gibi taşınabilir bellekler ile kişisel bilgisayar, sunucu gibi işletim sistemine sahip bilgisayar medyasındaki verilerin başka bir taşınabilir belleğe standart şekilde kopyalanması veya doğrudan harici bellek olarak kullanılması halidir. Adli bilişim çalışmalarında kullanılan bir diğer sabit veri tipi; adli kopyalardaki dosyaların dışa aktarılması (export) ile elde edilmektedir. Çeşitli nedenler ile (adli kopya sayısının fazla olması, ürün lisans problemi, gereksiz verilerin çokluğu gibi) dışa aktarılması gereken veriler üzerinde detaylı inceleme ve analiz işlemi yapılmasında anahtar kelime araması metodunun kullanılması mümkündür.

X-Ways Forensics ve OSForensics[10] başta olmak üzere adli bilişim yazılımlarının tamamına yakını adli kopya veya sabit veriler üzerindeki tüm dosyaları indeksleyebilme ve anahtar kelime araması yapabilme özelliğine sahiptir. Bazı adli bilişim yazılımları ise sadece PDF dosyalarının listelenmesi gibi dosya tipine göre filtreleme yapabilmektedir. OSForensics yazılımı ile Microsoft .pst ve .ost uzantılı dosyalarını okumak ve indekslemek mümkün iken, EnCase yazılımı için 3. parti eklentilerin

[7] Detaylı bilgi için bkz: Stefan Bolagh, Matej Pondelik. "Capturing Encryption Keys for Digital Analysis". In Proceedings 6th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), ss: 759-763, Prag, 15-17 Eylül 2011.
[8] http://www.agilerm.net/publications_4.html
[9] http://wetstonetech.com/livewire_screenshots.html
[10] http://www.osforensics.com/

Çakır, H., & Kılıç, M. S. (2016). Adli bilişimde anahtar kelime araması metodu ve önemi. *International Journal of Human Sciences*, *13*(1), 2368-2384. doi:10.14687/ijhs.v13i1.3401

kullanılması gerekmektedir. Benzer şekilde indekslenen dokümanın elde edilebilmesi (extract) için EnCase, X-Ways Forensics ve ProDiscover[11] yazılımları için scriptler oluşturmak mümkün iken AccessData FTK[12] yazılımında script oluşturma özelliği bulunmamaktadır (Nelson vd., 2015:260).

Sabit veriler, adli kopya dosyası gibi silinmiş verileri içermediği gibi canlı sistemlerde olduğu gibi değişken de değildirler. Sabit, her türlü değişikliğe açık bu veriler üzerinde; adli delil elde etme veya başka amaçla (eğitim, arşiv gibi) anahtar kelime araması işlemi gerçekleştirilebilir. Google firması tarafından Linux, Mac OS X ve Windows işletim sistemleri için geliştirilen Google Desktop[13] ürünü ile veriler indekslenerek dosya tipi, konumu, boyutu gibi çeşitli kriterlerle birlikte anahtar kelime araması işlemi gerçekleştirilmesi mümkündür (Aygün, 2010:34). UltraSearch[14], FileSeek[15], Everything Search Engine[16] vb. ürünler de Google Desktop benzeri anahtar kelime araması işlemi gerçekleştirmek üzere özelleşmiştir.

Veri tabanları üzerinde anahtar kelime araması işlemi ise diğer sabit verilere göre biraz daha zordur. Veri tabanı içerisinde farklı tablolarda birbiri ile ilişkili şekilde verilerin bulunması; yapılacak rutin arama işlemi sonucu anlamlı sonuçlara ulaşılamamasına neden olacaktır. Örneğin, çocuk pornografisine sahip bir sunucunun incelenmesinde veri tabanı içerisinde anahtar kelime olarak "IP Adresi" ile bir arama yapıldığında; sunucuya yapılan bağlantıların kaydedildiği tabloda, söz konusu IP adresine ait kayıtlara ulaşılabilecektir. Diğer taraftan farkı tabloda bulunan "takma isim" ve yüklenen videolara ait bilgilerin kaydedildiği tablodaki kayıtlar elde edilemeyecektir. Bu ve benzeri durumlar için veri tabanlarına özgü arama algoritmaları geliştirilmiştir.

Birçok veri tabanı sorgu uygulaması (DBXplorer, BANKS, BLINKS, DISCOVER vb.), kullanıcının sorgu kelimesi girmesi, sistemin veri tabanında bulunan ilgili tablodan sonuç getirmesi ve derecelendirme yapılarak sonuç üretilmesi gibi benzer girdi-çıktı işlemine sahiptir (Balla ve Chen, 2013:199). Verinin verisi olarak adlandırılan üstveriler üzerinde yapılacak anahtar kelime aramasında da benzer zorluklar mevcuttur. Dosyanın oluşturulma zamanı, yazar bilgisi, yorum bilgisi, lokasyon bilgisi gibi doküman içeriğinin bir parçası olmayan verilere basit kelime araması ile ulaşılamamaktadır (Huynh, 2012:245).

2.4. Bulut Bilişim Verileri Üzerinde Anahtar Kelime Arama

Türkçemize "bulut bilişim" olarak çevrilen cloud computing; kullanıcıların verilerini internet üzerinde paylaşmaları ve erişmeleri hizmetidir. Gelişen teknoloji ile beraber kişisel, ticari veya akademik verilere anlık erişim ihtiyacı ve yüksek kapasitede elektronik verilerin bozulma, kaybolma ihtimali insanları bu hizmeti kullanmaya yönlendirmiştir. Arz-talep dengesinde gelişen bu hizmet, kullanıcılara büyük kolaylık sağlamanın yanı sıra güvenlik birimleri açısından delil elde etme çalışmalarını zorlaştırmaktadır.

Kullanımı hızla yaygınlaşan bulut bilişim kullanımı, araştırmacılar ve güvenlik kuvvetleri için "bulut adli bilişim" (cloud forensic) teriminin ortaya çıkmasına neden olmuştur. Adli bilişim disiplini ve prosedürü içerisinde yaklaşılması gereken bu disipline; Bulut Bilişim Servis Sağlayıcıları (Cloud Service Providers-CSPs), kullanıcılar ve güvenlik güçleri büyük ilgi göstermesine rağmen yeterli teknik, metodoloji, politika ve standartların olmadığı anlaşılmaktadır (Simou vd., 2015:1). Bulut bilişim üzerinde bulunan verilere bilgisayar ağları aracılığıyla ve gerekli doğrulama mekanizmalarının sağlanmasıyla erişilmektedir. Bu açıdan veriler kriptolu olarak saklanmakta ve birçok bulut bilişim

[11] http://www.arcgroupny.com/products/prodiscover-forensic-edition/
[12] http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk
[13] http://googledesktop.blogspot.com.tr/
[14] https://www.jam-software.com/ultrasearch/
[15] https://www.fileseek.ca/
[16] http://www.voidtools.com/

Çakır, H., & Kılıç, M. S. (2016). Adli bilişimde anahtar kelime araması metodu ve önemi. *International Journal of Human Sciences*, *13*(1), 2368-2384. doi:10.14687/ijhs.v13i1.3401

hizmet sağlayıcısı, veri güvenliği açısından uçtan uca kripto hizmeti sunmaktadır. Yine kullanıcılar tarafından yapılan erişim ve sorgular kriptolu şekilde gerçekleşmekte ve kişisel verilerin güvenliğinin sağlanmasına dikkat edilmektedir (Bringer ve Chabarine, 2012:1).

Bulut bilişim verileri üzerinde yapılacak adli bilişim çalışmaları; hedef bulut sistemi, erişim sağlanan kaynak bilgisayar ve iletişim sağlayan cihazlar (modem, switch, router) üzerinde yapılacak incelemeleri kapsamaktadır. Hedef bulut bilişim üzerinde yapılacak adli bilişim incelemeleri henüz tam disipline edilmemiş iken kaynak bilgisayar incelemesi ve iletişim cihaz incelemesinde bir takım adli bilişim metot ve araçları mevcuttur.

Bulut bilişim sunucuları üzerinde yapılacak inceleme; sanal makine izleme ve analiz metodu olan Sanal Makine İçgözlem (Virtual Machine Introspection-VMI) incelemesine benzemektedir. Bu metotta, sistem logları, registry kayıtları, sunucu geçici belleği, bağlantı bilgileri gibi donanımsal olaylar ve kullanıcı işlemlerinin kaydedilmesi ve analiz edilmesi amaçlanmaktadır (Baboo ve Megalai, 2015:2). Bu verilerin elde edilmesi için çeşitli yöntemler geliştirilmiştir. Patraşcu ve Patriciu tarafından geliştirilen "Cloud Forensics Logging Framework" de; bulut bilişim sunucularının gerçek zamanlı izlenmesi ve belirlenen işlemlerin kaydedilmesi amacıyla ağ trafiği içerisinde yer alan sunucu üzerinde çalışacak bir uygulama geliştirilmesi hedeflenmiştir (Patraşcu ve Patriciu, 2015:225). James ve Jang ise uluslararası işbirliğindeki zorluklar ve mevzuat yetersizliklerine dikkat çektikten sonra bulut bilişim verilerine; servis sağlayıcıları ile işbirliği ve resen kullanıcı adı-parolanın elde edilmesi olmak üzere iki şekilde erişilebileceğini öne sürmüşlerdir. Buna göre şüphelinin rızası (sözlü onay) ile verdiği kullanıcı adı-parola ile sunucudaki verilere erişilebilecektir. Benzer şekilde şüphelinin bilgisayar veya mobil telefonunda kayıtlı parolalar bulunabileceği göz önüne alınarak bu cihazlar üzerinde yapılacak inceleme ile kullanıcı adı-parola bilgisinin elde edilmesi mümkün olacaktır (James ve Jang, 2014:37). Ko ve Zaw ise dünya geneli 50 milyondan fazla kullanıcısı olan Dropbox bulut bilişim uygulamasına dikkat çekmiştir. 18 sanal makine üzerine Dropbox client uygulaması kurularak Magnet Forensic Tools'a ait Dropbox Decryptor[17] ve SQLite DB Browser[18] yazılımları ile yapılan test çalışmaları sonucu; config.dbx, filecacahe.dbx, sigstore.dbx ve deleted.dbx isimli SQLite veritabanı dosyalarından ve Windows Registry kayıtlarından gerçekleştirilen kullanıcı işlemlerine ait birçok veri elde edildiği görülmüştür (Ko ve Zaw,2015:147).

Bulut adli bilişim çalışmalarında kullanılabilecek bir diğer yöntem; bulut bilişim servis sağlayıcılarına ait API (Application Programming Interface-Uygulama Programlama Arayüzü)'lerin güvenlik kuvvetleri için tanımlanacak özel yetkiler ile kullanılmasıdır. API'lerin kullanılması ile geliştirilecek uygulamaların en büyük dezavantajı ise yapılan her türlü kelime araması ve sorgu işleminin servis sağlayıcısı tarafından bilinmesi ve kaydedilmesi olacaktır.

2.5. Anahtar Kelime Aramasının Önemi

Anahtar kelime araması, arama programları aracılığıyla ilgili karakter, kelime veya cümle yazarak dosya veya başka verilere ulaşma metodu (Nelson vd., 2015:274) olup adli bilişim incelemelerinde uzun süredir kullanılmaktadır. Adli bilişim uzmanı Eoghan Casey, bilgisayara izinsiz erişimin tespitinde; dosya sistemi analizi, dosya yapılandırılması ve başlangıç yerlerinin incelenmesi, sistem loglarının incelenmesi ve uygulama loglarının incelenmesini açıkladıktan sonra anahtar kelime araması metoduna vurgu yapmıştır. Casey'e göre ağ trafiği ve log incelemeleri sonucu ortaya çıkan IP adresi gibi karakteristik verilerin zararlı yazılım içerisinde tespiti, anahtar kelime araması metodu ile mümkündür (Casey, 2011:403).

Anahtar kelime aramasının önemine dikkat çekilmesi amacı ile Microsoft sponsorluğunda ACM SIGMOD (The ACM Special Interest Group on Management of Data) tarafından 2009-2012 yılları

[17] https://www.magnetforensics.com/free-tool-dropbox-decryptor/
[18] http://sqlitebrowser.org/

Çakır, H., & Kılıç, M. S. (2016). Adli bilişimde anahtar kelime araması metodu ve önemi. *International Journal of Human Sciences*, *13*(1), 2368-2384. doi:10.14687/ijhs.v13i1.3401

arasında "Yapılandırılmış Veri Üzerinde Anahtar Kelime Araması Çalıştayı" (Workshop on Keyword Search on Structured Data) düzenlenmiştir. Çalıştayda, akademik araştırmacılar ve endüstriyel uygulamacılar tarafından (yarı-) yapılandırılmış veri, mekânsal veri ve web verisi üzerinde anahtar kelime aramasının fırsatları ve yeni teknikleri konusunda fikir alışverişinde bulunulmuştur.

Adli bilişim açısından anahtar kelime araması metodu; hızlı ve etkili bir adli bilişim çalışması, özel hayatın gizliliği, ilişki analizi, sözlük oluşturulması ve şifre tespiti ile silinmiş ve gizlenmiş verilerin tespiti açısından büyük önem taşımaktadır.

2.6. Hızlı ve Etkili Adli Bilişim Çalışması Açısından

Kullanımı yaygınlaşan teknolojik ürünlerle birlikte elektronik delillerin, maddi gerçeğin ortaya çıkarılmasındaki rolü de artmaktadır. Adli bilişim çalışmalarının amacı, salt suç ile ilgili verilerin tespiti değil, aynı zamanda suç ile ilgisi olmayan tarafların masumiyetinin kanıtlanmasına yardımcı olmaktır. Adli bilişim uzmanı tarafından adil, tarafsız ve taraflar açısından kuşkuya yer vermeyecek şekilde inceleme raporu hazırlanmasında "anahtar kelime araması metodu" önem arz etmektedir. Şöyle ki, hazırlanan inceleme raporunda arama işlemi yapılan kelimelere ve çıkan sonuçlara yer verilmesi; taraflara incelemenin etkili yapılıp yapılmadığı hakkında fikir vereceği gibi yargı mensupları tarafından verilecek kararlara da pozitif katkı sağlayacaktır.

Kullanıcı verilerinin kapasite olarak artması, yargılama aşamasında bu verilerin manuel olarak incelemesini zorlaştırmaktadır (Wochna, 2015:868). Diğer taraftan delile ulaşma aşamasında nereye bakılacağını her zaman bilmek zordur. Örneğin, çocuk istismarı veya cinsel suçlar konusunda; bilgisayar oyunları, resimler, filmler, sohbet kayıtları (chat logs) gibi akla ilk gelen dokümanlar dışında kapsamlı bir inceleme yapılması şarttır (Centel ve Zafer'den akt. Özbek, 2009:16). Bu bağlamda, birçok adli bilişim yazılımında bulunan anahtar kelime ile arama yapılması özelliğinin kullanılması ile adli analiz işlemlerinin hızlanacağı açıktır. Bununla beraber doğru anahtar kelimelerin belirlenememesi, sonuç sayısını arttıracak olup her somut olay için olaya özgü anahtar kelime listesi kullanılması gerektiği sonucu ortaya çıkmaktadır (Nelson vd., 2015:259). Bu durum günlük hayatta herkesin çok basit bir şekilde kullandığı Google arama motoru açısından da geçerlidir. Başta kelime seçimi olmak üzere anahtar kelime araması metodu konusunda "Google Etkili Arama Yöntemleri" (Effective Google Search Method) kavramının ortaya çıkması, konunun önemini ortaya koymaktadır.

EnCase, AccessData FTK, Winhex (X-Ways) ve CnW Recovery[19] adli bilişim yazılımları ile tüm diskin taranarak belirlenen kelime setlerinin aranması ve sonuçlarının csv formatında raporlanması mümkündür (Halboob vd., 2015:374). Bununla beraber bazı durumlarda daha özel şekilde tcpdump dosyasının incelenmesine ihtiyaç duyulabilmektedir. "USER", "PASS" ve "login" gibi anahtar kelimelerin tcpdump dosyasında aratılması ile internet iletişimi hakkında bilgi elde edilebilmektedir. Benzer şekilde IRC bağlantı verilerinin incelenmesinde; takma isim (nickname) ve kanal adı (channel name) araması ile ihtiyaç duyulan bilgiler elde edilmesi mümkündür (Casey, 2011:728).

Adli kopya alma (imaj alma) süresinin kısaltılması için Gier ve Richard tarafından yapılan bir çalışmada, adli kopyası alma sırasında anahtar kelimeler kullanılarak sadece ilgili sektörlerin kopyalanması araştırılmıştır. Çalışmada, anahtar kelimelerin herhangi bir sektörde olabilmesi sebebi ile tüm diskin okunmasına ihtiyaç duyulduğu anlaşılmış ve adli kopya alma sırasında anahtar kelime araması metodunun kullanılabileceği ancak, süre açısından avantaj sağlamayacağı sonucuna ulaşılmıştır (Gier ve Richard, 2015:38).

[19] http://www.cnwrecovery.co.uk

Çakır, H., & Kılıç, M. S. (2016). Adli bilişimde anahtar kelime araması metodu ve önemi. *International Journal of Human Sciences*, *13*(1), 2368-2384. doi:10.14687/ijhs.v13i1.3401

2.7. Özel Hayatın Gizliliğinin Korunması Açısından

Özel hayat, kişilik hakları içerisinde özel bir öneme sahiptir. Demokratik bir hukuk devletinde vazgeçilmez bir özellik olarak görülmektedir. Özel hayat, aynı zamanda kişilik hakkının temel unsurlarından biri olarak da kabul edilmektedir (Pınarbaşı, 2014:14). Özel hayatın gizliliği ve haberleşme hürriyeti Anayasa[20] ve diğer ilgili kanunlarla koruma altına alınan önemli haklardandır. Taraf olduğumuz Avrupa İnsan Hakları Sözleşmesinde de herkesin haberleşme hürriyetine saygı gösterilmesi kurala bağlanmıştır (Yalçın ve Kılıç, 2016).

5271 sayılı Ceza Muhakemesi Kanunu ile "sanıktan delile değil, delilden sanığa ulaşılması" yöntemi benimsenmiş ve soruşturma aşamasında delilleri toplamakla görevli savcılık ve onun emrindeki adli kolluk makamlarına önemli araştırma ve güvenlik tedbire başvurma yetkileri verilmiştir. Bu konuda bilgisayarlarda arama, kopyalama ve el koyma usulleri 134. Maddede düzenlenmiştir (Öztunç, 2010:26). ABD'de de hedef veriler üzerinde yapılacak elektronik inceleme ve araştırmalar Federal İspat Kanunu 702. maddede düzenlenen hükümler çerçevesinde yapılmaktadır (Wochna, 2015:845). Anılan maddeye göre; bilirkişinin (adli bilişim uzmanının) bilimsel, teknik ya da diğer nitelikli bilgisi ile hâkime yardımcı olması, güvenilir prensip ve metotlar ile davanın konusuna uyumlu olarak uygulaması beklenmektedir.

El konulan bilgisayar medyalarının incelenmesinde; hukuk devleti olmanın gereği olarak vatandaşların özel hayatına saygı gösterilmesi devletin görevidir. Bilişim araçları incelemesi ile olayı aydınlatacak önemli deliller elde edilmesinde yüksek masraf çıkması ve zamanın yetersiz olmasının nedenleri arasında verilerin hacmi ve kişilik haklarının ihlali olasılığı bulunmaktadır (Özbek, 2009:17). Örneğin, muhasebe dolandırıcılığı ve kartel sözleşmesi sebebi ile mağdur olan şirketler genellikle uzun süreli bir soruşturma ile karşı karşıya kalmaktadır. İletişim verilerinin önemli delil olarak kabul edilmesi sebebi ile yönetim dokümanları ve e-postalar incelenmektedir. Hassas ve özel bilgiler içeren bu verilerin gizliliğini imkânlar ölçüsünde yasal olarak korumak ise şirketin zorunluluğundadır (Armknecht ve Dewald, 2015:128). Benzer şekilde, bulut bilişim verilerinin klasik adli bilişim incelemeleri ile ele alınması; aynı sunucuda farklı hizmet sağlayıcılarının bulunması veya aynı servis sağlayıcısının çok sayıda sunucuda veri barındırması sebepleri ile zordur. Diğer taraftan sunucunun birebir kopyasının alınması; zaman, maliyet ve veri kapasitesinin yüksek olması sebebi ile imkânsızdır. Bu şekilde kopyalama mümkün olsa dahi çok sayıda gereksiz verinin incelenme ihtiyacı ve kullanıcılara ait kişisel verilerin suiistimali söz konusu olacaktır (Hou vd., 2011:1).

Adli bilişim uzmanı öncelikle verileri suç ile ilgili/ilgisiz olarak sınıflandırmalıdır. İlgili veriler suçun aydınlatılmasına katkı sağlayacak verilerdir. İncelemede sadece bu verilere bakılarak tüm elektronik verilere erişim limiti konulması; özel hayatın gizliliğine katkı sağlayacağı gibi zaman ve personel gücü açısından da tasarruf sağlayacaktır (Halboob vd., 2015:372). Bu bağlamda sadece ilgili dokümanlara ulaşılmasında en etkili ve kolay yöntem "anahtar kelimesi arama metodu" dur. Örneğin, e-posta sunucusunda yapılacak bir incelemede adli bilişim uzmanı tarafından anahtar kelime araması yapılması ile sadece ilgili anahtar kelimelerinin geçtiği e-postalar elde edilecek ve tüm e-postaların incelenmesi engellenmiş olacaktır (Armknecht ve Dewald, 2015:128). Bilgisayar incelemelerinde ise Sleuth Kit - Autopsy[21] adli bilişim yazılımı ile adreslenmemiş alan (unallocated space) dahil bilgisayarın tamamında anahtar kelime araması yapılması mümkündür (Nelson vd., 2015:306). Benzer şekilde web tabanlı bilgisayar incelemelerinde Gmail gibi e-posta iletileri ve ilgili veriler; FTK adli bilişim yazılımında yapılacak anahtar kelimesi araması ile elde edilebilmektedir (Nelson vd., 2015:29).

[20] Özel Hayatın Gizliliği (Md 20), Haberleşme Hürriyeti (Md 22).
[21] http://www.sleuthkit.org/autopsy/

Çakır, H., & Kılıç, M. S. (2016). Adli bilişimde anahtar kelime araması metodu ve önemi. *International Journal of Human Sciences*, *13*(1), 2368-2384. doi:10.14687/ijhs.v13i1.3401

2.7. İlişki Analizi Açısından

Adli bilişim çalışması, fiziksel olarak bilgisayar medyalarının toplanması (olay yeri incelemesi) ile başlamaktadır. Bu aşamada elde edilen sabit disk, PDA, CD gibi fiziksel deliller suç ve suçlu arasında ilişki kurma amaçlıdır. Sabit disk veya cep telefonu içerisindeki veriler gibi elektronik deliller ise; suçun gerçekleşmesini ortaya koymak ve suç ile kurban veya fail arasında ilişki kurmak amaçlıdır (Carrier ve Spafford, 2003:10).

Bilişim suçlarında en önemli delil bulma yöntemi, hiç şüphesiz saldırı yapılan internet sitelerine ait IP adresleri, şahısların yaptıkları internet bağlantı bilgileri ve bu süreçte kullanılan bilişim sistemlerinin incelenmesidir. Diğer taraftan gelişen teknoloji ile beraber açık kaynak üzerinde, gerçekleşen bilişim suçu ve suçun faili olduğu değerlendirilen şahıslar hakkında bilgi toplanabilmektedir. Bununla beraber sadece IP kayıtları, sadece açık kaynak bilgileri veya sadece bilgisayar inceleme kayıtları suç isnat etmek için yeterli olmayabilmektedir. Özellikle bilgisayar korsanları (hacker) tarafından reklam, kendini ispat, siyasi-manevi propaganda vb. saiklerle internet sitesi ana sayfası değiştirilerek (hacklenerek) slogan, takma isim, e-posta adresi gibi bilgileri içeren mesajlar bırakılmaktadır. Salt bir internet sitesine bırakılan mesaj ile bir şahsın ilişkilendirilmesi mümkün değildir. Zira bilişim sistemine erişim sağlayan kişi tarafından kendisine ait bilgilerin (takma isim, memleket, e-posta adresi vb.) paylaşılabileceği gibi bir başka şahsa ait bilgilerin paylaşılması da pekâlâ mümkündür. Bu sebeple hacklenen internet sitelerine bırakılan mesajların, failin tespitine yönelik yardımcı/destekleyici delil olarak değerlendirilmelidir. Bu bağlamda, siber saldırıya uğrayan internet sitesi isimleri ve internet sitelerine bırakılan mesajlar; şüphelilere ait bilgisayarlarda "anahtar kelimesi araması metodu" ile incelenerek suç ve fail arasında ilişki analizi yapılmalıdır.

Kredi kartı dolandırıcılığı olaylarında adli bilişim uzmanı tarafından bilgisayar üzerinde kredi kartı numarasının aranmasının yanı sıra kredi kartı ile işlem yapılan internet sitesine o bilgisayardan erişim yapılıp yapılmadığının da incelenmesi gerekmektedir. İnternet sitesi adı, sunucu IP adresi, indirilen dosyalar gibi bilgilerin anahtar kelime olarak aratılması ile bilgisayar ve suç arasında ilişki kurulabilecektir (Carrier ve Spafford, 2003:15). Bazı durumlarda ise suça karışan bilgisayar medyasının sahibi konusunda tereddütler yaşanmaktadır. Bu gibi durumlarda bilgisayar ve sahibi arasında ilişki kurabilmek için hedef şahsa ait TC kimlik numarası, isim-soyisim, e-posta adresi, takma isim gibi kişisel bilgilerin anahtar kelime olarak aratılması gerekmektedir.

İlişki analizi kurulmasında karşılaşılan problemlerin başında doğru anahtar kelimelerinin tespit edilememesi gelmektedir (Huynh, 2012:251). Bir diğer karşılaşılan problem ise; anahtar kelime arama programlarının mükemmel olmaması ve insan gibi düşünememesidir. Dokümanlarda kelimeler beklenmedik şekilde yanlış telaffuz edilmiş veya yabancı kelime/argo karşılığının kullanılmış şekilde bulunuyor olabileceği gibi dokümanlar fotoğraflar olarak da yer almış olabilir (Goldfoot, 2011:138). İlişki analizi konusunda bahsedilmesi gereken son husus; özellikle bilişim tabanlı suçlarda faili tespit edilemeyen olaylara ait anahtar kelime veritabanı oluşturulması ihtiyacıdır. Her somut olayda yapılacak adli bilişim çalışmaları sırasında, veritabanındaki anahtar kelimelerinin aratılması ile bilişim suçlarının aydınlatılmasına katkı sağlanacağı açıktır.

2.8. Sözlük Oluşturulması ve Şifre Tespiti Açısından

Adli bilişim çalışmalarında karşılaşılan en önemli problemlerden birisi şifre korumalı (kriptolu) dokümanlar ile karşılaşılmasıdır. İşletim sisteminde yer alan varsayılan programlar veya ilave programlar aracılığı ile şifrelenen dokümanların çözülmesinin (şifrelerinin kırılmasının); maddi gerçeğin ortaya çıkarılmasına katkı sağlaması beklenmektedir. Bu işlem ise ayrı bir disiplin olup kendi içerisinde zorluklar barındırmaktadır. Bu zorlukların başında güçlü şifreleme algoritmaları ve

Çakır, H., & Kılıç, M. S. (2016). Adli bilişimde anahtar kelime araması metodu ve önemi. *International Journal of Human Sciences*, *13*(1), 2368-2384. doi:10.14687/ijhs.v13i1.3401

uzun-karışık karakterli parola kullanımı gelmektedir. Bilinen en etkili şifre kırma metodu ise sözlükte (kelime listesinde) bulunan kelimelerin taranması şeklinde olan sözlük saldırısı (distionary attack) dır.

Garcia tarafından 2015 yılında yapılan bir çalışmada; Odroid-XU işlemci ile kaba kuvvet (brute-force) ve sözlük saldırısı (dictionary attack) yapabilen şifre kırma yazılımı test edilmiştir. Test sonucunda kullanılan sözlüğün kelime sayısına bağlı olarak sözlük saldırısının başarılı olduğu görülmüştür (Garcia, 2015:36). Bu bağlamda saldırılarda kullanılacak sözlüğün niteliği öne çıkmaktadır. Kullanılacak sözlükler hazır olarak temin edilebileceği gibi olaya özgü özel olarak da oluşturulması mümkündür. Örneğin, şifreli dokümanın elde edildiği bilgisayar içerisinde bu dokümana ait parolanın bulunma ihtimali göz önüne alınarak bilgisayar içerisindeki veriler sözlük haline getirilebilir. Bu işlem; anahtar kelime aramasına sahip adli bilişim yazılımları ile tüm verilerin indekslenip veritabanına kaydedilmesi ve bu kayıtların kelime listesi haline getirilmesi ile gerçekleşebilir.

AccessData FTK adli bilişim yazılımı, bilgisayarın indekslemesi sonrasında kelime listesinin kopyalanmasına izin vermekte, hatta bu listeyi doğrudan AccessData PRTK[22] şifre kırma yazılımının sözlük klasörüne (\AccessData\Dictionaries) kaydedebilmektedir. PRTK ise, kelime listesindeki her bir satırda yer alan kelimeyi sözlük saldırısında kullanmaktadır (AccessData, 2007:207). Sleuth Kit - Autopsy adli bilişim yazılımı da benzer şekilde yapılandırılabilmektedir. Özellikle gizlenmiş verilerin (steganograhpy) tespitinde oluşturulan sözlüğe manuel olarak "steg*", "mandelsteg" kelimelerinin eklenmesi mümkündür. Belirlenen kelimeler indekslenen bilgisayar içerisinde aratılabileceği gibi kelime listesi şeklinde dışa aktarılması (export) da mümkündür (Furuseth, 2005:91).

Adli bilişim çalışması sırasında anahtar kelime arama metodu ile oluşturulan sözlüklerin bir diğer faydası ise benzer kelimelerin tespit edilebilmesidir. Örneğin bilgisayarın indekslenmesi sonucu oluşan kelime listesinin incelenmesi ile "banka" kelimesinin geçtiği "A Bankası", "Banka B" şeklindeki kelimeler de tespit edilebilecek ve yürütülen soruşturmaya yön verilebilecektir. Açık kaynak üzerinde ücretli yayın yapan *www.keywordtool.io* internet sitesi de kelimelerin Google, Bing, Youtube internet sitelerinde sık kullanılan halleri ile beraber sunmaktadır. Örneğin, bahsedilen internet sitesinde "ankara" kelimesi sorgulandığında; Google arama motorunda sırası ile "ankaranın bağları", "ankara hava durumu", "ankara üniversitesi", "ankara iftar vakti", "ankara ezan", "ankara barosu", "ankara oyun havaları", "ankara meb", "ankara iş ilanları" ve "ankara haritası" kelimeleri ile birlikte arandığı anlaşılmaktadır. Bu şekilde anahtar kelimelerin, birlikte sık kullanıldığı kelimelerin tespit edilmesi adli bilişim çalışmalarına katkı sağlayacaktır.

2.9. Silinmiş ve Gizlenmiş Verilerin Tespiti Açısından

Bir dosyanın bilgisayardan silinmesi ve "Geri Dönüşüm Kutusuna" gönderilmesi; gerçek dosya verisinin bilgisayar içerisinde yer almakla beraber silinmiş olarak işaretlenmesinden ibarettir. Bu sebeple veri kolaylıkla geri dönüşüm kutusundan kurtarılarak tekrar elde edilebilmektedir. Eğer dosya geri dönüşüm kutusundan da silinmiş ise dosya verisi üzerine yeni veri yazılana kadar dosya bilgisayarda durmakta ancak adres bilgisi silinmektedir (Huynh, 2012:246). Veri kurtarma işlemi ise, dosya yapısına bakmaksızın medya üzerinde yer alan verilerin ortaya çıkarılmasıdır. Bu açıdan "silinmiş verileri geri getirme" tabiri, bilgisayar medyası üzerinde var olan ancak, mevcut işletim sisteminin görmediği verilerin tekrar elde edilmesi anlamına gelmektedir. Gizlenmiş veri ise; steganografi yazılımları ile veri içerisine veri saklanması sonucu oluşan veridir. Şifreli veya şifresiz şekilde saklanan bu verilerin standart veri inceleme yöntemleri ile fark edilememesi mümkündür.

PTK[23] adli bilişim yazılımına ait arama özelliği, anahtar kelime aramasından daha karmaşıktır. PTK, mevcut veriler ile birlikte diskin tamamında (unallocated space, slackspace, fragmented sectors,

[22] http://accessdata.com/product-download/digital-forensics/password-recovery-toolkit-prtk-version-7.6.0
[23] PTK adli bilişim yazılımı 3.0 versiyonundan sonra üreticisi tarafından geliştirilmemiştir. www.dfresponse.com

Çakır, H., & Kılıç, M. S. (2016). Adli bilişimde anahtar kelime araması metodu ve önemi. *International Journal of Human Sciences*, *13*(1), 2368-2384. doi:10.14687/ijhs.v13i1.3401

resident alternate data stream vb.) arama işlemi yapmakta ve silinmiş, gizlenmiş verilerden sonuç getirmektedir (Zambelli, 2009:1). Diğer taraftan yapılacak anahtar kelime araması ile silinmiş metin (text) verilerinden sonuçlar elde edilmekle beraber resim dosyaları ve sıkıştırılmış dosyaları açısından aynı durum söz konusu değildir (Alherbawi vd., 2013:87). Örneğin silinmiş ve üzerine veri yazılmış fotoğraf dosyaları geri getirilememesine rağmen, "Canon EOS" gibi anahtar kelimeler ile yapılacak aramalar ile üstveri bilgisinde "Canon EOS" bulunan fotoğraf dosyalarının tespiti mümkündür.

Anahtar kelime araması işleminde bilinen steganografi yazılım isimlerinin aratılması ile bilgisayarda steganografi yazılımı kurulu olup olmadığı anlaşılabilmektedir (Furuseth, 2005:83). StegAlyzerAS[24] gibi birçok steganaliz yazılımı; steganografi uygulamalarının Windows Registry üzerinde bıraktığı izleri araştırarak bilgisayarda steganografi yazılımı kurulmuş olup olmadığını analiz etmektedir. Diğer taraftan steganografi yazılımlarının tamamına yakını veri gizledikleri dosya üzerinde kalıntılar bırakmaktadır. Örneğin ücretsiz QuickStego[25] steganografi yazılımı veri gizlediği resim dosyasının başlık bilgisini (header information) .DIB uzantılı resim dosyalarına ait "424D36" değeri ile değiştirmekte ancak, dosya uzantısında değişiklik yapmamaktadır. Bu bağlamda, "424D36" hexadecimal değeri ile yapılacak bir anahtar kelime araması ile elde edilecek sonuçlardan dosya uzantısı .DIB olmayan resim dosyalarının QuickStego steganografi yazılımı ile içerisine veri gizlenmiş olduğu anlaşılabilecektir.

3. Sonuç ve Değerlendirme

Gelişen teknoloji ile beraber hayatın her alanına giren bilişim teknolojilerinin bir yansıması olarak muhakeme sürecinde elektronik veriler ile karşılaşılmaktadır. Bu bağlamda ortaya çıkan adli bilişim bilimi; elektronik verileri barındıran bilgisayar medyalarının incelenmesi, suç konusu olayı aydınlatacak verilerin raporlanması ve delil haline getirilmesini içermektedir (Kılıç, 2015:41). Henüz gelişimini tamamlamamış olan adli bilişim disiplini ise artan sabit disk kapasitesi ve çeşitlenen bilgisayar uygulamaları sebebi ile farklı metot ve çözüm yolları arayışı içerisindedir. Adli bilişim çalışmalarının etkili ve hızlı bir şekilde yapılması ve özel hayatın gizliliğinin korunması başta olmak üzere çeşitli sebeplerle "anahtar kelime araması metodu" öne çıkmaktadır.

Anahtar kelime araması metodu; öncelikle üzerinde arama işlemi yapılacak elektronik verilerin hazırlanması, verilere daha hızlı ulaşılabilmesi için indekslenmesi, daha önce belirlenen anahtar kelimeler ile sorgu yapılması, sistem tarafından indekslenen kelimelerin yer aldığı veri tabanı üzerinde eşleştirme yapılması ve kullanıcıya sonuçlarının gösterilmesi şeklindedir. Bu işlemler adli kopya verileri, canlı sistem verisi, sabit veriler ve bulut bilişim verileri üzerinde farklılık arz etmekte ve avantaj/ dezavantajlara sahip olmaktadır.

Bir ihtiyaç olarak ortaya çıkan ve kullanım alanı gün geçtikçe yaygınlaşan "anahtar kelime araması metodu" nun adli bilişim çalışmalarında kullanılması ile sağlanacak faydalar şu şekildedir:

- Maddi gerçeğin ortaya çıkarılmasına katkı sağlanacak, suç ile ilgisi olmayan taraflar hızlı bir şekilde ortaya çıkarılacaktır.
- Adli bilişim uzmanının tarafsız bir şekilde hareket ettiği anlaşılacaktır.
- Adli bilişim çalışmaları makul sürede tamamlanacaktır.
- Olay ile ilgisi olmayan verilerin incelenmesine gerek kalmaması sebebi ile zaman ve personel tasarrufu sağlanacaktır.
- Kişilerin özel hayatının korunması sağlanacak, suç ile ilişkili olmayan kişisel veriler incelemeye konu olmayacaktır.

[24] https://www.backbonesecurity.com/EnhancedSteganographyDetection.aspx
[25] http://www.quickcrypto.com/free-steganography-software.html

Çakır, H., & Kılıç, M. S. (2016). Adli bilişimde anahtar kelime araması metodu ve önemi. *International Journal of Human Sciences*, *13*(1), 2368-2384. doi:10.14687/ijhs.v13i1.3401

- Olaya özgü önem arz eden kelimelerin sorgulanması ile el konulan bilgisayar medyasının suç ile ilgili olup olmadığı anlaşılacaktır.
- Özellikle toplu kullanılan bilgisayarlarda bilgisayar medyasının sahibinin tespit edilememesi durumunda; bilgisayar medyası ile gerçek kişi arasında ilişki tespit edilebilecektir.
- Özellikle bilişim tabanlı suçlarda faili tespit edilemeyen her bir olaya ait anahtar kelimelerin tespit edilerek veritabanı oluşturulması ile gerçekleşen her somut olayda el konulan bilgisayar medyaları üzerinde veritabanında yer alan anahtar kelimelerinin sorgulanması ile bilişim suçları aydınlatılacaktır.
- Anahtar kelime araması için indekslenen kelimeler, şifre kırma çalışmalarında sözlük olarak kullanılacaktır.
- Adli bilişim incelemesi yapılan bilgisayar üzerinde stegonografi uygulamaları kalıntıları anahtar kelime sorguları ile tespit edilebilecektir.
- Bazı silinmiş veriler ile üst veri bilgileri yapılacak anahtar kelime araması sonucu elde edilebilecektir.

Çalışmada, anahtar kelime araması metodunun kullanımının adli bilişim çalışmalarında; "hızlı ve etkili adli bilişim çalışması yapılması", "özel hayatın gizliliğine katkı sağlaması", "şahıs-olay-bilgisayar medyası arasında ilişki analizi kurulması", "sözlük oluşturulması ve şifre tespiti" ile "silinmiş ve gizlenmiş verilerin tespiti" olmak üzere beş farklı açıdan fayda sağladığı görülmüştür. Literatür taraması ve doküman analizi türünde yapılan çalışmada her bir fayda sağlanılacak konuda somut yazılım isimlerine ve detaylı bilgi elde edilebilecek internet adreslerine yer verilmiştir.

4. Kaynakça

AccessData (2007), *Forensic Toolkit User Guide*, http://myweb.cwpost.liu.edu/cmalinow/ftk/ftkusersguide.pdf, Erişim Tarihi:22.08.2015.

Alherbawi, Nadeem; Shukur, Zarina ve Sulaiman Rossilawati (2013), Systematic Literature Review on Data Carving in Digital Forensic, *Procedia Technology Journal*, Cilt:11, ss:86 – 92. Doi: 10.1016/j.protcy.2013.12.165

View Article: DOI: http://dx.doi.org/10.1016/j.protcy.2013.12.165

Ali, Reem Al (2010), *Extensible Keyword Search Utility for Digital Forensics*, UCD School of Computer Science and Informatics Final Year Project, Ireland.

Armknecht, Frederik ve Dewald, Andreas (2015), Privacy-Preserving Email Forensics, *The International Journal of Digital Forensics & Incident Response*, Sayı:14, ss:127-136. Doi: 10.1016/j.diin.2015.05.003, **View Article: DOI: http://dx.doi.org/10.1016/j.diin.2015.05.003**

Aygün, İbrahim (2010), *Searching Documents With Semantically Related Keyphrases*, Ortadoğu Teknik Üniversitesi Fen Bilimleri Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Ankara.

Baboo, S Santhosh ve Megalai, S. Mani (2015), Cyber Forensic Investigation and Exploration on Cloud Computing Environment, *Global Journal of Computer Science and Technology*, Cilt:15, Sayı:1, ss:1-4. Doi: 10.1016/j.diin.2012.05.015

View Article: DOI: http://dx.doi.org/10.1016/j.diin.2012.05.015

Balla, Binaya ve Chen Zhengxin (2013), Expanding Database Keyword Search For Database Exploration, Procedia Technology Journal, Cilt:17, ss:198 – 205. Doi: 10.1016/j.procs.2013.05.027

View Article: DOI: http://dx.doi.org/10.1016/j.procs.2013.05.027

Çakır, H., & Kılıç, M. S. (2016). Adli bilişimde anahtar kelime araması metodu ve önemi. *International Journal of Human Sciences*, *13*(1), 2368-2384. doi:10.14687/ijhs.v13i1.3401

Bashir, Muhammad Shamraiz ve Khan, M. N. A. (2013), Triage in Live Digital Forensic Analysis, *The International Journal of Forensic Computer Science*, Cilt:1, Sayı:1, ss:35-44. Doi: 10.5769/J201301005

View Article: DOI: http://dx.doi.org/10.5769/J201301005

Bashir, Muhammad Shamraiz ve Khan, M. N. A. (2015), Review of Live Forensic Analysis Techniques, *International Journal of Hybrid Information Technology*, Cilt:8, Sayı:2, ss: 379-388. Doi: 10.14257/ijhit.2015.8.2.35, **View Article: DOI: http://dx.doi.org/10.14257/ijhit.2015.8.2.35**

Battula, Bhanu Prakash; Rani, Kezia; Prasad, Satya ve Sudha T. (2009), Techniques in Computer Forensics: A Recovery Perspective, *International Journal of Security*, Cilt:3, Sayı:2, ss:27-35.

Bringer, Julien ve Chabanne, Herve (2012), Embedding Edit Distance To Enable Private Keyword Search, *Human-Centric Computing and Information Sciences*, Cilt:2-2. Doi: 10.1016/S0031-3203(02)00030-4, **View Article: DOI: http://dx.doi.org/10.1016/S0031-3203(02)00030-4**

Carrier, Brian ve Spafford, Eugene H. (2003), Getting Physical with the Digital Investigation Process, *International Journal of Digital Evidence*, Cilt:2, Sayı:2, ss:1-20.

Casey, Eoghan (2011), *Digital Evidence And Computer Crime*, Elsevier Academic Press, ABD.

Cruz, Flavio; Moser, Andreas ve Cohen, Michael (2015), A Scalablefile Based Data Store For Forensic Analysis, *The International Journal of Digital Forensics & Incident Response*, Sayı:12, ss: 90-101. Doi: 10.1016/j.diin.2015.01.016,

View Article: DOI: http://dx.doi.org/10.1016/j.diin.2015.01.016

Çakır, Hüseyin ve Kılıç, Mehmet Serkan (2013), Bilişim Suçlarına İlişkin Elektronik Delil Elde Etme Yöntemlerine Genel Bir Bakış, *Polis Bilimleri Dergisi*, Sayı:15(3), ss 23-44.

Demircioğlu, Serap (2012), *İlişkisel Veri Tabanlarında Anahtar Kelime Arama*, Gazi Üniversitesi Fen Bilimleri Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Ankara.

Furuseth, Andreas Grytting (2005), *Digital Forensics: Methods and Tools For Re-Trieval and Analysis Of Security Credentials and Hidden Data*, Norveç Bilim ve Teknoloji Üniversitesi, Bilgi ve Teknoloji Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Trondheim, Norveç.

Garcia, Ricardo A. (2015), *Computer Forensics: Password Recovery Tool Using Odroid-XU Implementation*, Texas A&M Universitesi, Bilgisayar Bilimleri Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Corpus Christi, Teksas, ABD.

Goldfoott, Josh (2011), The Physical Computer and The Fourth Amendment, *Berkeley Journal of Criminal Law*, Cilt:16, Sayı:1, ss:111-167. Doi: 10.15779/Z38GS5N

View Article: DOI: http://dx.doi.org/doi:10.15779/Z38GS5N

Grier, Jonathan ve Richard, Golden G. (2015), Rapid Forensic Imaging of Large Disks With Sifting Collector, *The International Journal of Digital Forensics & Incident Response*, Cilt:12, ss:34-44.

Halboob, Waleed; Mahmod, Ramlan; Udzir, Nur Izura ve Abdullah, Mohd. Taufik (2015), Privacy Levels for Computer Forensics: Toward a More Efficient Privacy-Preserving Investigation, *Procedia Computer Science Journal*, Cilt:56, ss:37-375. Doi: 10.1016/j.procs.2015.07.222

View Article: DOI: http://dx.doi.org/10.1016/j.procs.2015.07.222

Hou, Shuhui; Uehara, T. ; Yiu, S.M. ; Hui, L.C.K. ve Chow, K.P. (2011), *Privacy Preserving Multiple Keyword Search for Confidential Investigation of Remote Forensics*, 2011 Third International Conference on Multimedia Information Networking and Security (MINES), 4-6 Kasım 2011, Şangay, Çin Halk Cumhuriyeti.

Çakır, H., & Kılıç, M. S. (2016). Adli bilişimde anahtar kelime araması metodu ve önemi. *International Journal of Human Sciences*, *13*(1), 2368-2384. doi:10.14687/ijhs.v13i1.3401

Huynh, Knanh T. (2012), Search Method in E-Discovery: How Rule 26's Silence Poses a Risk of Sanctions to Attorneys and Increases the Cost of Litigation, *The University of Massachusetts Law Review Journal*, Cilt:7, Sayı:1, ss:236-262.

James, Joshua I. ve Jang, Yunsik (2014), Practical and Legal Challenges of Cloud Investigations, *The Journal of The Institute of Internet, Broadcasting and Communication*, Cilt:14, Sayı:6, ss:33-39. Doi: 10.7236/JIIBC.2014.14.6.33,**View Article: DOI: http://dx.doi.org/10.7236/JIIBC.2014.14.6.33**

Kılıç, Mehmet Serkan (2015) Elektronik Delillerin Hukuken Geçerliliği Açısından İlk Müdahalenin Önemine İlişkin Bir İnceleme, *Terazi Hukuk Dergisi*, Cilt:10, Sayı:102, ss:34-41.

Ko, A.C. ve Zaw, W.T. (2015), *Digital Forensic Investigation of Dropbox Cloud Storage Service*, Network Security and Communication Engineering (Ed:Kennis Chan), CRC Press: İngiltere, ss:147-150.

Kules, Bill; Wilson, Max L ve Shneiderman Ben (2008), *From Keyword Search to Exploration:How Result Visualization Aids Discovery on the Web*, http://hcil2.cs.umd.edu/trs/2008-06/2008-06.pdf, Erişim Tarihi: 05.07.2015.

Marthie, Lessing, Marthie ve Solms, Basie (2008), *Live Forensic Acquisition as Alternative to Traditional Forensic Processes*, IT Incident Management & IT Forensics (IMF 2008), Mannheim, Almanya, 23 - 25 Eylül 2008.

Nelson, Bill; Phillips, Amelia ve Steuar Christopher (2015), *Guide to Computer Forensics and Investigations*, Coengage Learning, USA.

Özbek, Onur (2009), *Bilişim Teknolojileri ve Bireysel Güvenlik*, Hukukun Gençleri Sempozyumu: Hukuk Devletinde Kişisel Güvenlik, 20-21 Mart 2009, Ankara.

Öztunç, Özgün (2010), *Ceza Muhakemesinde Hukuka Aykırı Deliller*, Marmara Üniversitesi Sosyal Bilimleri Enstitüsü Yayınlanmamış Doktora Tezi, İstanbul.

Patruşçu, A. ve Patriciu, V.V. (2015), Logging for Cloud Computing Forensic Systems, *International Journal Of Computers Communications & Control*, Cilt:10, Sayı:2, ss: 222-229. Doi: 10.15837/ijccc.2015.2.802, **View Article: DOI: http://dx.doi.org/10.15837/ijccc.2015.2.802**

Pınarbaşı, Murat (2014), *Özel Hayatın Korunması Kapsamında İstihbarat Faaliyetlerinin Hukuksal Sınırları*, Kara Harp Okulu Sosyal Bilimleri Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Ankara.

Rumpf, Christian (2010), Türk Hukuku ile Mukayese Edildiğinde Almanya'da ve Avrupa'da Avukatların Reklam Yapma Hakkı, *Ankara Barosu Dergisi*, Sayı:2010/1, ss:145-166.

Simou, Stavros; Kalloniatis, Christos; Mouratidis, Haralambos ve Gritzalis, Stefanos (2015), *Towards the Development of a Cloud Forensics Methodology: A Conceptual Model*, Advanced Information Systems Engineering Workshops, Lecture Notes in Business Information Processing, Cilt:215, ss:470-481.

Spencer, Shaun B. (2015), The Aggregation Principle and the Future of Fourth Amendment Jurisprudence, *New England Journal on Criminal and Civil Confinement*, Cilt:41, ss:289-301.

Steele, J., O'Shea, K., Brittson, R. & Reyes, A. (2011), *Cyber Crime Investigations*, Elsevier Science, ABD.

Şen, O. N., (2005), "Polisin Adli Bilişimde Kullanabileceği Programların Bir Değerlendirilmesi", *2. Polis Bilişim Sempozyumu Bildirileri*, 14-15 Nisan 2005 Sheraton Hotel, Ankara: Emniyet Genel Müdürlüğü Bilgi İşlem Daire Başkanlığı, ss.35-41.

Wilson, Max L; Kules, Bill; Schraefel, M.C. & Shneiderman Ben (2010), From Keyword Search To Exploration: Designing Future Search Interfaces For The Web, *Foundations and Trends in Web Science Journal*, Cilt:2, Sayı:1, ss:1-97, USA. Doi: 10.1561/1800000003

Çakır, H., & Kılıç, M. S. (2016). Adli bilişimde anahtar kelime araması metodu ve önemi. *International Journal of Human Sciences*, *13*(1), 2368-2384. doi:10.14687/ijhs.v13i1.3401

View Article: DOI: http://dx.doi.org/10.1561/1800000003

Wochna, Donald (2015), Electronic Data, Electronic Searching, Inadvertent Production of Privileged Data: A Perfect Storm, *AkronLaw Review*, Cilt:43, Sayı:3, ss:842-868.

Yalçın, Nursel ve Kılıç, Mehmet Serkan (2016), *Windows Registry ile Bilgisayar Güvenliğinin Sağlanması*, Gazi Üniversitesi Bilişim Enstitüsü.

Zambelli, Michele (2009), PTK Live and Indexed Keyword Search, https://digital-forensics.sans.org/blog/2009/02/02/ptk-live-and-indexed-keyword-search/, Erişim Tarihi: 09.08.2015.

Extended English Abstract

Computer forensics is a branch of digital forensic science which is deal with gather and preserve evidence from computers and digital storage media, investigation and analysis of electronic data and presentation in a court of law in acceptable form. Like "keyword search method", computer forensics investigation has too many methods about analysis of computing device and gather electronic evidence.

Keyword search method loop is formed 5 nodes which are preparing of electronic data, indexing data, queries with keywords from users, matching on database automatically and showing result to the users. The most important node is keyword search query because of human factor. Because of getting relavant result, detecting keywords must be appropriate to every specific events.

Using keyword search method on different data type like forensic image data, live forensics data, static data and cloud computing data has advantages and disadvantages. Forensic image is bit to bit copy of original computing device. So it also contains all deleted and hidden data. Because of scanning all data on the disk, using keyword search gets more result, but not get any information from volatile data. Live forensic investigation captures volatile information like running processes, event logs, network information, registered drivers and services. Because of data is vanished when computer is turned off, keyword search on live data has advantage. On the other hand, interfere on working computer has reveal doubts about electronic data integrity, thus keyword search on live forensics data has disadvantages. Static data means, local stored data on computer or exported data from forensic image. Because static data doesn't consist of any deleted data, computer forensics standarts are not met and the analyses of electronic data is inadequate level. Cloud computing is a solution that users store, access and process their own data in third-party data centers remotely. Cloud computing data (or shortly cloud data) is data where data is stored remotely. Similar to other computer forensics process, keyword search on these data has big problem. Although some solutions are developed for solving the problem of accessing data, it is not adequate.

Similar to using search engine in internet investigations, using keyword search method in computer forensics investigations has too much benefits. In this study, it is examined 5 different aspect as;

1-) Rapid and Effective Computer Forensics Investigations

Because of increasing capacity of harddisks, in trial phase it will be more difficult to analysis all electronic data manually. In this context, using "keyword search method" in computer forensics investigations provides time saving and reaches results earlier. On the other hand, using "keyword search method" provides computer forensics experts' fair and impartial.

2-) Contribution to Privacy

Privacy, is the ability of individuals to hide their privacy. Privacy partially overlaps confidentiality, which can include the concepts of appropriate use, as well as protection of information. Privacy

Çakır, H., & Kılıç, M. S. (2016). Adli bilişimde anahtar kelime araması metodu ve önemi. *International Journal of Human Sciences*, *13*(1), 2368-2384. doi:10.14687/ijhs.v13i1.3401

uses the theory of human rights, and generally responds to new information and communication technologies. New technologies alter the balance between privacy and disclosure, and that privacy rights may limit government surveillance to protect democratic processes.

In computer forensics investigations, first of all, electronic data must be classified as relevant or irrelevant crimes. Relevant data contributes to clarification of the crime. While investigation, accessing only relevant data will help to protect privacy. The easiest method of these is using "keyword search method" in computer forensics investigations.

3-) Relational Analysis

Relational analysis uses a specific concept of information. It defines situations with limited information and find out the relations of objects. Computer forensics investigations, it is important to find out the relational analysis of Person-Event-Computing Device. At this point, keyword search method solves the problem easily.

In cyber crimes investigations, IP addresses and internet connection information are important evidence. While analyses of attackers' computers and target systems, using keyword search method provides a positive contribution to investigations.

4-) Creating Dictionary for Decrypt Passwords

In computer forensics investigations, encrypted files are big problem, because of unknown content. Cryptanalysis is the study of access to the contents of encrypted messages, even if the cryptographic key is unknown. Solving the key in order to decrypt the password of a file, dictionary attack is the populer method.

Most of computer users save passwords in files or use common passwords in different places. In this context, every word in computer is a potentialy important. Because of computer is indexed while using keyword search method, using words list as a dictionary helps to decrypt passwords.

5-) Recover Some Deleted Data and Detect Steganography Data

Data recovery is a process of rescue inaccessible data from corrupted or damaged files. In addition to most of method about data recovery, keyword search method recovers some file with the help of metadata. For example, if "Canon EOS" keyword is searched, some deleted photo files can be recovered. Similarly, some steganography files can be detected if right keywords determine, like artifacts of steganography softwares.