ACTA INFOLOGICA
dergipark.org.tr/acin

İSTANBUL UNIVERSITY PRESS

DOI: 10.26650/acin.804201

RESEARCH ARTICLE

Adli Bilişim İncelemelerinde Şifre Kırma Yöntem ve Teknikleri

Password Cracking Methods and Techniques in Computer Forensic Investigation

İlker Kara[1]

ÖZ

Bilgi sistemleri ve veri kullanımındaki sonsuz artış, bilgi güvenliğinde tehlikenin doğuşunu tetikledi. Son yayınlanan raporlara göre askeri kuvvetler ve e-ticaret web siteleri dışında sıradan kullanıcılarda sistemleri ve belgelerini korumak için şifreleme teknikleri kullanmaya başlanmışlardır. Alınana tedbirlere rağmen çeşitli gizleme tekniklerini kullanarak hazırlanan akıllı saldırılar mevcut korunma yöntemlerini atlatarak hedef sistemdeki parola ve kullanıcı adlarını ele geçirebilmektedir. Kurumsal firmalar ve sıradan kullanıcılar verilerini gizlemek için yeni nesil şifreleme yöntemlerini yaygın olarak kullanmaktadır. Bu durum özellikle adli olaylara konu olan bilgi sistemleri ve dosyaların incelenmesinde büyük engeller oluşturmaktadır. Eğer şüpheli kişi kullanmış olduğu bilgi sistemi veya dosyalarını şifrelenmiş ise delil elde etmek için önce bu şifrelerin önceden bilinmesi ya da şifrenin kırılması gereklidir. Bu adımda şüpheli kendi rızasıyla parola kolluk kuvvetlerine vermemesi durumunda adli uzmanlar çeşitli yönetmelerle şifreleri kırmaya çalışmakta bu süreç genellikle zor olmakta ve bazı durumlarda şüpheli sistemdeki şifreli verilere ulaşılamamaktadır. Bu çalışma iki katkı sunmaktadır. İlk olarak en çok kullanılan şifre kırma yöntemleri detaylı olarak incelenmiştir. İkincisi, "BitLocker" veri şifreleme yöntemiyle şifrelenmiş örnek bir adli vaka incelenerek şifreli verileri kırılma adımları incelenmiştir. Sonuçlardan şifrelenmiş verilerin erişmek için kullanılan yöntemin etkili olduğunu ve şifrelerin kırıldığı göstermektedir.

Anahtar kelimeler: Şifre Kırma, Veri Şifreleme, Güvenlik Saldırıları, Analiz Yöntemleri

ABSTRACT

The unending increase in information systems and data use has triggered the birth of danger to information security. According to recently published reports, apart from military forces and e-commerce websites, ordinary users have begun to use encryption techniques to protect systems and documents. In spite of precautions, smart attacks prepared using a variety of concealing techniques overcome available protection methods and can obtain the passwords and user names of on the target system. Corporate firms and ordinary users commonly use new-generation encryption methods to hide their data. This situation creates large obstacles forto the investigation of computer systems and files which are the subject of forensic events, especially. If a suspect uses a computer system with encrypted files, to obtain evidence, firstly, it is necessary to know these encryptions or to crack them. In this step, if the suspect does not give law enforcement the encryptions willingly, forensic experts attempt to break the encryption with a variety of methods. This process is generally difficult, and in some situations, the encrypted data on the suspect's system cannot be reached. This study provides two contributions. The first is that a detailed investigation of the most commonly used encryption cracking methods are investigated in detail. Secondly, an example forensic case encrypted with the "BitLocker" data encryption method is investigated and the steps to break the encrypted data are investigated. The results show that the methods used to access the encrypted data is effective and that the encryption was cracked.

Keywords: Password Cracking, Data Encryption, Security Attacks, Analysis Methods

[1](Dr. Öğr. Üyesi), Çankırı Karatekin Üniversitesi Eldivan Sağlık Hizmetleri Meslek Yüksek Okulu, Çankırı, Türkiye

ORCID: İ.K. 0000-0003-3700-4825

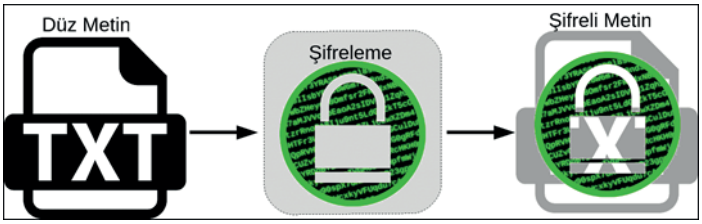
Corresponding author:
İlker KARA
Çankırı Karatekin Üniversitesi Eldivan Sağlık Hizmetleri Meslek Yüksek Okulu, Çankırı, Türkiye
E-mail address: karaikab@gmail.com

Submitted: 02.10.2021
Revision Requested: 19.02.2021
Last Revision Received: 22.02.2021
Accepted: 22.02.2021
Published Online: 31.05.2021

Citation: Kara, İ. (2021). Adli bilişim incelemelerinde şifre kırma yöntem ve teknikleri. *Acta Infologica, 5*(1), 27-38. https://doi.org/10.26650/acin.804201

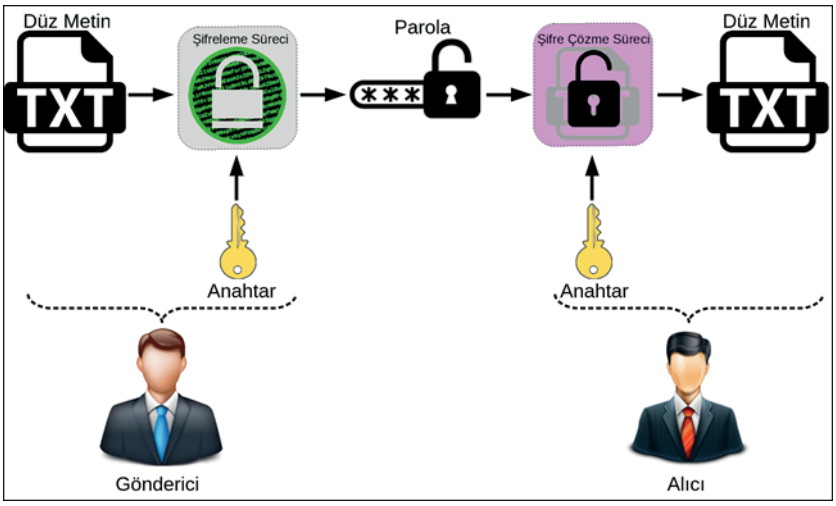
1. GİRİŞ

İlk ortaya çıktığından beri, veri şifreleme yöntemleri bilgi sistemlerini ve verileri en iyi koruma tekniklerinden biri olarak bilinmektedir (Guddeti vd. 2020). Bu güvenlik yaklaşımı, kullanıcının korunan sistemlerin ve verilerin içeriğini erişimi için bir şifre çözme anahtarı kullanılması olarak tanımlanır. Bu şekilde, yalnızca yetkili kişiler (anahtara erişimi olanlar) korunan sisteme veya verilere erişebilmektedir (Bhanot vd. 2015). Bir açık metinin bir şifreleme algoritması vasıtasıyla anlaşılamaz bir metin haline getirilmesi işlemine şifreleme (Encryption) denir (Şekil 1) (Dass vd. 2020). Şifre Çözme (Decryption) işlemi ise bir şifreleme algoritması şifrelenmiş veriyi çözerek ilk haline getirme işlemidir (Şekil 2) (Hur vd. 2019).



Şekil 1. Şifreleme adımları.

Veri şifreleme yöntemi, ticari işletmeler, resmi kurumlar, silahlı kuvvetler, kişisel kullanıcılar ve e-ticaret web sitelerinde ödeme ayrıntılarını korumak da dâhil olmak üzere bir dizi farklı alanda kullanılmaktadır (Saračević vd. 2020). Günümüz teknoloji uygulamalarda veri şifrelemenin doğru bir şekilde yapılmasıyla, verilerin hemen hemen her tehdide karşı koruyabilecek güce sahiptir. Bununla birlikte, birçok kurum ve kullanıcı (son derece hassas verilere sahip olanlar bile) henüz bu yöntemi uygulamamaktadır (Kara 2019). Bu verilerin varlığı şüphesiz siber suçlular için ilgi çekici bir hedeftir ve korunmasız olanlarda ilk saldırıya uğrayanlar arasındadır.



Şekil 2. Şifre oluşturma-çözme süreci.

Kurumlar ve kullanıcılar veri şifreleme yönteminin sunabileceği güvenlik avantajlarının farkında olsa da, şifrelenmiş veriler adli incelemelerde birtakım zorluklarla karşılaşılmasına neden olmaktadır. Adli bilişim uzmanı, bilgi sisteminde ki veriye ulaşabilmesi için bu şifreleme mekanizmalarını aşması gereklidir. Çoğu zaman yapılan adli incelemelerdeki şüpheli bilgi sistemlerinin şifrelemeyi aşmaları çok zor hatta imkânsız olabilmektedir. Günümüzde suç işleyenler veya şüpheli durumda olan insanlar kendilerini veya kişisel verilerini gizlemek amacıyla veri şifreleme yöntemlerini kullanarak işlerini kolaylaştırırken adli uzmanların işlerini zorlaştırmaktadır.

Öte yandan gelişen teknolojinin getirdiği avantajlardan faydalanan şifreleme yöntemleri de gün geçtikçe gelişmektedir. Apple iOS 11'de, Firefox arama motorunda, Whatsapp mesajlaşma uygulaması gibi birçok uygulaması güvenlik önlemlerini artırdı ve "end-to-end" olarak bilinen şifreleme kullanılmaya başlamışlardır. Microsoft Windows 8 sürümde standart olarak

sunulan hard disk şifrelemesi kolaylıkla kullanıcılar tarafından uygulanabilmektedir. Sıradan kullanıcılar dahi iletişimlerini ve kişisel verilerini gizlemek için PGP, TrueCrypt, Microsoft BitLocker ve Tor gibi şifreleme uygulamalarını kullanmaktadırlar. Hukuka uygun olarak kişisel verilerin korunması ve gizlilik politikalar kapsamında kişisel veri sahibinin açık rızasının bulunmadan ikinci kişilerin erişmemesi kanunlar ile koruma altına alınmış olmakla birlikte özgürlüklerin ve kamu güvenlik arasındaki bu dengeyi kanunlar ile kullanıcılar arasında kurmak gereklidir.

Bu çalışmada veri şifreleme yöntemleri ve şifre kırma analizlerindeki yeni gelişmeleri anlatılmaktadır. Çalışmanın odak noktası da "BitLocker" veri şifreleme yöntemiyle şifrelenmiş gerçek bir şifreleme vakasının incelenmesi olacaktır. Bu amaçla "BitLocker" veri şifreleme yöntemiyle şifrelenmiş bilgisayardaki verilerin nasıl kurtulabileceğini gösteren uygulanabilir bir yaklaşım önerildi. Önerilen yaklaşımda şifre kırma analizlerinde Windows tabanlı bilgisayarlarda brute force şifre kırıcısı olan "Passware Kit Forensic Version 2019.2.0 (Ücretsiz sürümü)" yazılımı kullanıldı. Bu yaklaşımla benzer yöntemlerle şifrelenmiş bilgi sistemleri ve veriler için uygulanabilir olmasını hedeflenmiştir.

2. ŞİFRE KIRMA (PASSWORD CRACKING) YÖNTEMLERİ

Şifre ve parolalar dijital dünyada siber saldırganların odağında olmakta ve kırılan tek bir şifre ile tüm güvenlik sistemleri atlatılarak tüm sistem veya veriler ele geçirilebilmektedir. Şifreli verilere veya bilgi sistemlerine ulaşmak saldırganlar kadar sıradan insanlarında ilgisini çekmekte bu durum şifre kırmak için her geçen gün yeni yöntemler geliştirmeye çalışılmaktadır. Bu nedenle bu çalışmada şifre kırmak için kullanılan en popüler yöntemlere değinilmiştir. Şifre kırma yöntemlerini "aktif" ve "pasif" yöntemler olarak iki ana gruba ayrılabilir. Bunlar (Kaya vd. 2017):

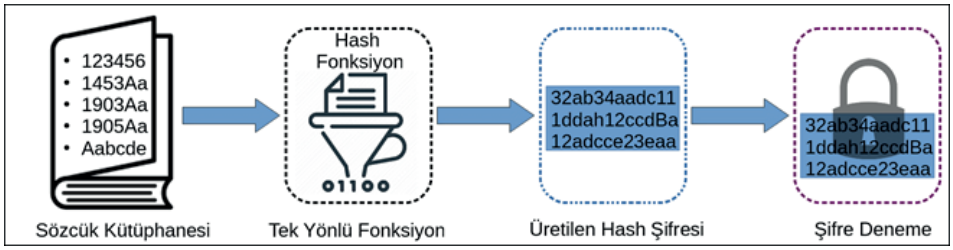
• Aktif şifre kırma yöntemlerinde; hedef bilgi sistemine veya veri dosyalarına çevrimiçi (anlık) olarak şifre kırma saldırıları gerçekleştirilmektedir.

• Pasif şifre kırma yöntemlerinde; ise çevrimdışı ortamlarda önceden hazırlanan tahmini şifreler hazırlanarak, incelemeler sonucunda ele geçirilen şifreler denenerek veya olası şifre tahminleriyle yapılan şifre kırma saldırılarıyla gerçekleşmektedir.

Aktif şifre kırma yöntemi kullanılabilmesi için bir şekilde hedef veri tabanı yâda kullanıcı bilgilerinin (olası hesap kullanıcı adı veya parolalar gibi) bilinmesi gereklidir. Bu durum dışında kalan senaryolarda pasif şifre kırma yöntemleri kullanılmaktadır.

2.1. Sözlük Saldırısı (Dictionary Attack)

Sözcük saldırısı "sözlük dosyasında" oluşturulan olası her kelimeyi otomatik şifre kombinasyonları halinde şifrelenmiş sistem veya veri dosyasına karşı deneyerek şifreyi kırma denemelerine denilmektedir (Bhanot vd. 2015). Sözcük dosyası içerisinde kullanıcıların daha önce en sık kullandıkları şifreleri içeren bir dosyadan oluşmaktadır. Sözcük saldırısı üretilen tek yönlü fonksiyon (Hash fonksiyonu) elde edilmiş şifreler hedef sistemdeki parolayı veri tabanında karşılık gelen olasılıkları tahmin etmesiyle şifre kırılmaktadır (Beşkirli vd. 2019) (Şekil 3).

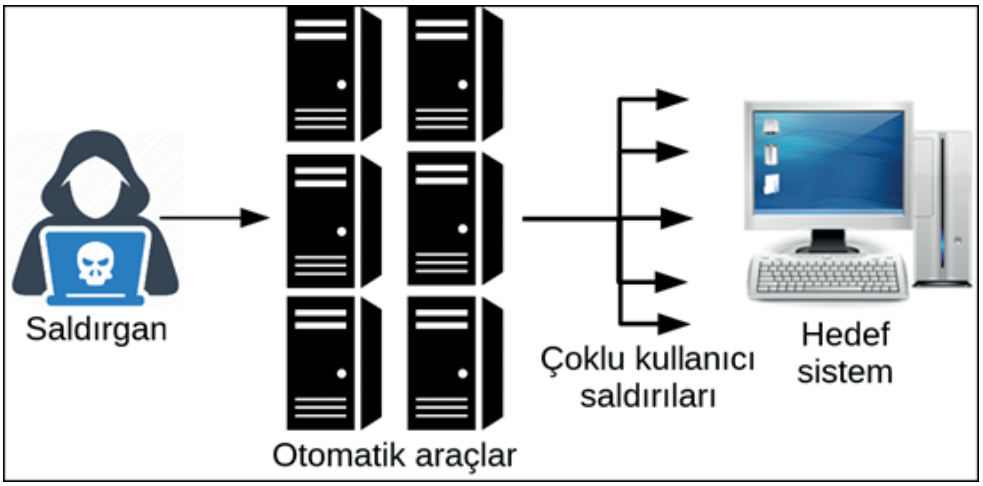


Şekil 3. Sözcük saldırı algoritması.

Sözcük saldırısında üretilen olası hash şifreler ile hedef sistemdeki şifreyi kırmak mevcut parolanın büyüklüğüne ve şifrelenme tekniğine (Gelişmiş şifreleme algoritması-AES, Asimetrik şifreleme algoritması-RSA gibi) göre işlem süresi değişiklik göstermektedir (Beşkirli vd. 2019). Bazen hedef sistemdeki algoritmanın çözülme olasılık süresi yıllar alabilmektedir (Bhanot vd. 2015).

2.2. Kaba Kuvvet Saldırısı (Brute Force Attack)

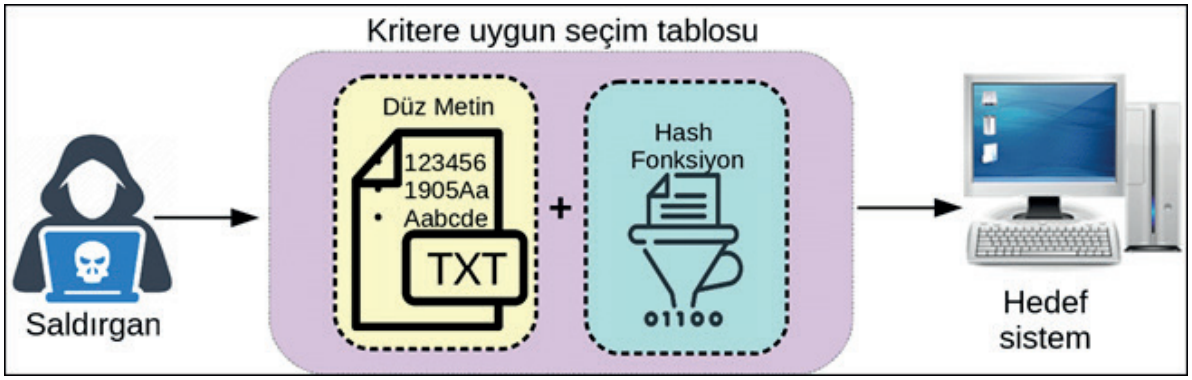
Kaba Kuvvet saldırıları yöntemi hedef sistemdeki parolayı deneme saldırılarıyla kırmak mantığıyla çalışmaktadır. Bu amaçla oluşturulan harfler ve özel karakterler içeren bir liste (Pass List) hazırlanır (Kara 2019). Kaba Kuvvet saldırısının başarı süresi hedef sistemdeki parolanın karmaşıklığına ve saldırıda kullanılan sistemimin donanım gücüne göre değişiklik göstermektedir (Şekil 4).



Şekil 4. Kaba kuvvet saldırı algoritması.

2.3. Gökkuşağı Tablosu Saldırısı (Rainbow Table Attack)

Gökkuşağı tablosu saldırısı yönteminde hedef sistemdeki parolaları kırmak için belirli ölçüte göre seçilen içerisinde düz ve hash fonksiyonlarını içeren bir şifre tablosu hedef sistemdeki parolayı kırmak mantığıyla çalışmaktadır (Bhanot vd. 2015; Beşkirli vd. 2019). Kaba kuvvet saldırılarında olduğu gibi hazırlanan şifre tablosu tek tek hedef sistemdeki parolayı kırmak için kullanılmaktadır. Kaba kuvvet saldırısından ayıran en önemli farkı ise tüm parolaları denemeye dayalı olmasıdır. Dahası denenen parolaları belirli bir düzene dayalı olarak seçmektedir. Bu düzen ise düz karşılığı olan hash edilmiş parolaları bilgisayar sisteminde sürekli olarak denemekten geçmektedir (Beşkirli vd. 2019).



Şekil 5. Gökkuşağı tablosu saldırı algoritması.

Gökkuşağı tablosu saldırısı yönteminde tablo hazırlanırken açık kaynak araması ile kullanıcıların en çok tercih ettiği parola örnekleri ve özel servilerin (rockyou wordlist gibi) hazırladığı listeler kullanılmaktadır (Bhanot vd. 2015).

2.4. Otalama (Phishing) Saldırı Yöntem

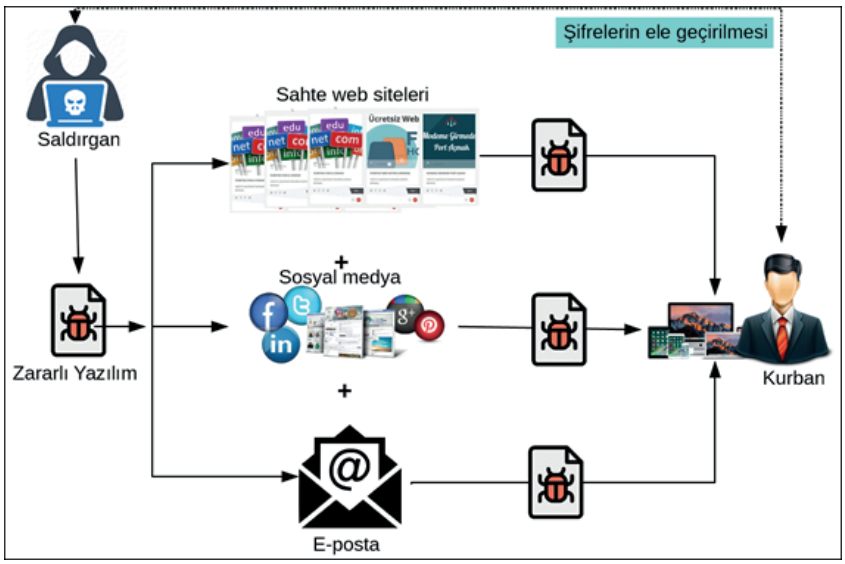
Oltalama saldırıları, kurbana ait şifrelerini ele geçirmek üzere yapılan saldırılardır. Oltalama saldırıları, sahte bir e-posta (İçeriğinde; indirim, bedava ürün ya da hediye çekişi kazandığını belirten) ile kurbana ulaşarak ilk bakışta zararsız gibi

görülen ekinde hedef kişiyi safta web sitelerine yönlendiren saldırgan kurban kişiden kullanıcı adı ve şifresini sisteme girmesi üzerine kurulmuştur (Şekil 6) (Kara 2019).

Şekil 6. Otalama saldırı algoritması.

2.5. Kötücül Yazılım (Malware) Saldırıları

Saldırganlar, şifre kırma yöntemlerinde en çok kötücül yazılım saldırıları tercih etmektedirler. Hedef bilgi sistemindeki parolayı kırmak ya da ele geçirmek için önceden hazırlanmış kötücül yazılımları (Virüs, tuş kaydedici (keylogger), truva atı, fidye yazılım gibi) kullanmaktadır (Kara 2019). Saldırgan bu tür kötücül yazılımları sahte web siteleri, önceden tahrip edilmiş sosyal medya platformları, haber siteleri, ilan siteleri, sahte e-postalar ile hedef sisteme ulaşmaktadır. Hedef sisteme sızan kötücül yazılım sistemde kayıtlı olan tüm kullanıcı adı ve parolayı ele geçirerek saldırgana bir e-posta ile göndermektedir. Böylece saldırgan amacına ulaşmış olup kurbana ait kredi kartı bilgileri, sosyal medya hesaplarını, kimlik verileri, e-posta hesap şifrelerini kolayca ele geçirmektedir.



Şekil 7. Kötücül yazılım algoritması.

3. ŞİFRE KIRMA PROGRAMLARI

Günümüzde farklı stratejilerle çalışan birçok şifre kırma yazılımları vardır. Bunlardan en popüler olanları; Passware Kit Forensic Version, Aircrack-ng, Hydra, Elcomsoft Distributed Password Recovery, Hashcat Password Recovery, John the Ripper, fgdump, Medusa, Cain and Abel ve RainbowCrack'dır. Bu bölümde kısaca bu yazılımlar hakkında bilgi verilecektir.

a) Passware Kit Forensic (PKF): Özellikle bilgisayarlardaki (Windows, Linux ve Amazon EC2(Amazon Web Services)) şifrelerin kırmak için ve adli uzmanlarında adli analizlerde tercih ettikleri etkili bir şifre kırma yazılımıdır. PKF bilgisayardaki tüm alanları veya seçilen özel dosyalar üzerindeki tüm şifre korumalı öğeleri kaba kuvvet saldırı tekniğinle eksiksiz çözebilme yeteneğine sahiptir. Yazılım 280'den fazla dosya türünü tanır ve şifreleri kırmak için toplu modda (aynı anda birkaç şifreli alan veya dosya üzerinde) çalışabilmektedir.

b) Aircrack-ng: Aircrack-ng yazılımı kablosuz iletişim WI-FI sahip olduğu WEP ve WPA-PSK (kablosuz ağları için bir güvenlik algoritmaları) güvenlik algoritmalarını kaba kuvvet saldırı tekniğiyle şifrelerini kıran bu alandaki en popüler yazılım araçlardan biridir.

c) Hydra: Uzak erişim protokolündeki şifreleri kaba kuvvet saldırı tekniği kullanarak kırmaya yarayan ayrıntılı şifre kırma programlardandır. Hidra programı HTTP, VNC ve TELNET ağ protokollerini desteklemektedir. Linux işletim sisteminde ücretsiz olarak sunulan programın Windows işletim sistemi sürümü de bulunmaktadır.

d) Elcomsoft Distributed Password Recovery: Farklı dosya türlerinin (FAT, NTFS gibi) şifrelerini kırmaya yarayan Elcomsoft şifre kırma programı resmi kurumlarda ve kişisel kullanıcılar tarafından sıklıkla tercih edilmektedir. Windows sişletim sistemlerinde yaygın olarak kullanılmaktadır. Kaba kuvvet saldırı tekniğiyle çalışan bu program TrueCrypt, VeraCrypt, Bitlocker, PGP Disk ve LUKS şifreleme programları üzerinde başarılı sonuçlar vermektedir.

e) Hashcat Password Recovery: Hashcat, kolayca hash algoritma şifrelerini kırmaya yarayan bir şifre kırma programıdır. Çalışma mantığında kaba kuvvet saldırı tekniğini kullanan Hashcat'in Linux, OS X ve Windows işletim sistemleri için sürümler bulunmaktadır.

f) John the Ripper: John the Ripper özellikle hash algoritma şifrelerini kırma programıdır. Linux işletim sisteminde yaygın olarak kullanılan bu programın Windows işletim sistemi versiyonu da bulunmaktadır. Çalışma mantığı Hashcat programına benzeyen John the Ripper, kaba kuvvet saldırı tekniğiyle şifre kırma saldırıları düzenlemektedir.

g) fgdump: fgdump şifre kırma programı lokal veya diğer kullanıcı hesap şifrelerini kırmak için tasarlanmıştır. Programın ilk sürümü olan "pwdump" 2019 yılında güncellenmesiyle programın adı "fgdump" olarak değiştirilmiştir. fgdump şifre kırma programının son sürümümde şifre geçmişlerini görüntüleme özelliğinde eklenmiştir.

h) Medusa: Uzak erişim sistemlerin şifrelerini kırmak üzerine geliştirilmiş bir şifre kırma programıdır. Medusa hedef sistemdeki şifreleri kırmak için kaba kuvvet saldırı tekniklerini kullanmaktadır. Nisan 2018 yılında güncellene son sürümüyle güncellenerek HTTP, SQL, POP3, Telnet ve VNC gibi birçok ağ protokolleri desteklemektedir.

j) Cain and Abel: Microsoft Windows için tasarlanmış bir şifre kırma programıdır. Kaba kuvvet ve kripto analiz teknikleri kullanan Cain and Abel programı, IOS, RDP ve PIX gibi ağ protokollerini desteklemektedir. Ayrıca son sürümünde getirilen güncellemeler ile IP üzerinden ağ parolası dinleme ve kayıt konuşma özelliğide eklenmiştir.

k) RainbowCrack: RainbowCrack şifre kırma programı kaba kuvvet saldırı tekniği yerine gökkuşağı tabloları üretme tekniğiyle hedef sistemdeki şifreleri kırmak üzerine tasarlanmıştır. Gökkuşağı tabloları olarak isimlendirilen bu tablolar önceden planlanmış olarak hazırlanmasıyla geleneksel yöntemlere göre daha kısa sürede şifreleri kırabilmektedir. Ağustos 2020 yılında güncellenen RainbowCrack şifre kırma hızı ve yüksek başarı oranıyla dikkat çekici olmakla birlikte tabloların hazırlanmasındaki güçlükler ve şifreleme algoritmaların karmaşıklığının artması yöntemin uygulanabilirliğini olumsuz yönde etkilemektedir.

4. LİTERATÜR TARAMASI

Şifre kırma saldırılarına bakıldığında kayıtlara geçmiş ilk olayların 90'lı yıllarında kaydedilmiştir. 16 Temmuz 1998 yılında ABD'de, topluluk acil müdahale ekibi (Community Emergency Response Team (CERT)) 186.126 şifrelenmiş verileri ait bir parolaları bulunduğunu bildirmiştir (Madsen 1998). 2009 yılında o güne kadar yaşanmış en büyük şifre kırma saldırısı (SQL Injection) olan "Rockyou.com" web hizmeti 32 milyona yakın şifrenin kırılarak piyasaya sürülmüştür (Noorunnisa vd. 2016).

2011 Haziran ayında NATO (Kuzey Atlantik Antlaşması Örgütü) üyelerinin 11.000 kayıtlı kullanıcılarının meta-data bilgileri ele geçirildi. Temmuz ayına gelindiğinde Amerika Birleşik Devletlerinde görev yapan özellikle Deniz Piyadeleri, Hava Kuvvetleri personeli ve İç işleri çalışanlarına ait bilgiler ele geçirilerek terör örgütlerine dağıtıldığı iddia edildi. Bu saldırılardan sonra birçok resmi kurum ve e-ticaret siteleri zayıf şifre kullanımını (1234, abcd gibi) yasakladı ve güçlü şifreleme algoritması (Büyük harf simge içeren en az sekiz karakterden oluşan gibi) standarttı kullanımını zorunlu hale getirmiştir (Thakur vd. 2019).

Günümüze kadar yapılan şifre kırma çalışmalarına bakıldığında halen en güvenli yöntemlerinin sözlük saldırısına veya kaba kuvvet yöntemlerine dayandığını görülmektedir (Oechslin vd 2003, Thing vd. 2009). Bununla birlikte, bu yöntemlere ek olarak Gökkuşağı tabloları oluşturmak için çok miktarda hesaplama süresi ve çaba gerektirdiğinden (Billet vd. 2006) çalışmalarda çok tercih edilmediği de görülmektedir.

2009 yılında Weir ve ark. (Weir vd. 2009, Weir vd. 2010) şifreli verileri metin yapısını kullanarak şifrelerin kırılmasını sağlayan yeni bir şifre kırma tekniği sunmuşlardır. Bu çalışma sonuçlarının John the Ripper aracından daha etkili olduğunu göstermişlerdir (Houshmand vd. 2017). Başka bir çalışmada, Zhang ve ark. (Zhang vd. 2010). Weir'in önerdiği algoritmasının mevcut şifre kırma teknikleri arasında en etkili olduğunu iddia etmişlerdir. 2011 yılında Kelley ve ark. (Kelley vd. 2012) simüle edilmiş şifreler oluşturmak ve güçlerini değerlendirmek için Weir'in algoritmasını ve Markov modelinin bir varyasyonunu uyguladı. 2012 yılında Castelluccia (Castelluccia vd. 2012) ve Narayanan (Narayanan vd. 2005), şifrelenmiş dosyaların parolasını bağlamsal sıklığına dayandığı karakter tahminlerinden oluşan bir model önermiştir. 2017 yılına gelindiğinde Houshmand (Houshmand vd. 2017) yaptığı çalışmada şifre kırmak için şifreyi oluşturan kullanıcı hakkında bilgileri kullanan bir yöntem önermiştir.

Adli bilişim şifre kırma incelemeleri, artan siber suç oranına bağlı olarak incelenecek delil miktarı ve boyutunun artması, şifre kırma sürecinin karmaşıklığına bağlı olarak işlem süreçlerinin uzaması ve kullanılan donanımın maddi boyutu gibi birçok zorluklar içermektedir. Bu süreç içerisinde şifre kırma yöntemlerinin tanımlanması, delilerin kategorize etmek ve uygun tekniklerin belirlenmesi yönelik çalışmalar yürütülmüştür. 2013 yılında Al Fahdi ve arkadaşları yaptıkları çalışmada adli incelemelerdeki dijital delilerdeki artış miktarına bağlı olarak şifre kırma işlemlerinde belirgin ölçüde artacağını öngören bir anket çalışması adli tıp uzmanları üzerinde uygulamıştır (Al Fahdi vd. 2013). 2016 yılına Harichandran ve arkadaşları benzer bir çalışmada adli tıp uzmanlarının şifre kırma işlemlerinde yasal zorluklar, teknik eğitim gereksinimleri ve yeni nesil karmaşık şifre algoritmaların zorluklarının ön gören bir anket yapılmıştır (Harichandran ve ark., 2016). Diğer bir çalışmada Lillis ve arkadaşları adli incelemelerdeki zorlukları üç ana kategoriye ayırmıştır. Bunlar; teknik zorluklar, yasa zorluklar ve kullanılan kaynak temininde yaşanan zorluklar olarak belirlemişlerdir (Lillis vd. 2016).

Adli bilişim incelemeleri dışında bilgisayar sistemleri üzerinde penetrasyon testi veya hesap kurtarma işlemlerinde şifre kırma işlemlerine ihtiyaç duyulmaktadır (Lehto ve Neittaanmäki. 2018). Özellikle adli bilişim incelemeleri gerçekleştirebilmek için özel şifre kırma programları kullanılmaktadır (Hassan, 2019). Adli incelmelerde şifre kırmak için en basit yöntem kapsamlı bir deneme veya kaba kuvvet saldırısı yöntemi kullanmaktır (Raza vd. 2012). Bu çalışmada seçilen adli vaka örneğinde şifre kırma işlemi kaba kuvvet saldırı yöntemi kullanan özel bir program kullanılmıştır.

Adli incelemelerde şifre kırmak için kullanılan başka bir yöntem ise potansiyel şifrelerin oluşan bir tablo (Hellman tabloları veya Gökkuşağı tabloları gibi) kullanmaktır (Hellman, 1980; Wang vd.2013). İlk uygulamalarda başarı oranı yüksek olsada günümüzde kullanılan şifrelerin boyutu ve karmaşıklığının artması önceden hesaplanmış bir tablo ile şifre kırma işleminin başarısını son derece düşürmekte neredeyse imkansız hale getirmiştir. Diğer bir yöntem ise sözlük saldırılarıyla şifreleri kırmak üzerinedir. Bu yöntemde de kullanıcıların eğilimlerini (ad, soyad, memleket, futbol takımı vb.) test etmekten oluşmaktadır. Bir önceli yöntem olan tablo hazırlamasındaki zorluklar sözcük saldırısı yönteminde de olması nediyle adli bilişim incelemelerinde tercih edilmemektedir (Aggarwal vd. 2018). Modern şifre kırma yöntemleri özellikle makine öğrenmesi yönteminden faydalanarak hazırlanmış otomatikleştirilmiş programlar vasıtasıyla gerçekleştirilmektedir (Dürmuth vd. 2015). Bu yöntemin temelinde şifre kırma programlarının azalan olasılıklarla kaba kuvvet saldırısı mantığın dayanmaktadır (Hitaj vd. 2019). Günümüzde kaba kuvvet saldırısı yöntemini kullanan programlar adli bilişim incelemelerinde adli bilişim

uzmanları tarafından şifre kırma incelemelerinde yaygın olarak tercih edilmektedir (Kanta vd. 2020). Benzer olarak bu çalışmada seçilen vaka örneği incelemelerinde kaba kuvvet saldırısı yöntemini kullanan PKF programı aracılığıyla gerçekleştirilmiştir.

5. ÖRNEK OLAY İNCELEMESİ

Bu çalışmada tüm analizler, Windows 10 Pro yazılıma sahip 2xXeon Gold 5118 /32GB / 256GB M.2 SSD sahip Dell Precısıon T7920 marka iş bilgisayarı ile yapıldı. Şifre kırma analizlerde "Passware Kit Forensic (PKF) V. 2019.2.0 (Ücretsiz sürümü)" programlarıyla yapılmıştır. Seçilen örnek adli bir olay olması (gerçek bir saldırı örneği) nedeniyle incelenecek şüpheli bilgisayarda bulunan verilere zarar vermemek ve delil bütünlüğünü koruma için öncelikle şüpheli bilgisayarın imal kopyası alınmıştır. İmaj kopyası alam işleminde uluslararası adli inceleme standartlarında kullanılan Forensic Toolkit (FTK) Imager (Ücretsiz sürümü) programı tercih edilmiştir.

İmaj kopyası alındıktan sonra analiz aşamasına geçilmiştir. Analiz aşamasında ilk adım olarak iş bilgisayarında analiz ortamının oluşturulması gereklidir. Analiz ortamı; incelenen delilerin olası saldırılarından iş bilgisayarının etkilenmemesi için gereklidir. Adli incelemelerde analiz ortamı sanal makine tercih edilmektedir. Sanal makine modunda çalıştırılan iş bilgisayarı incelemeler tamamlandıktan sonra ilk haline geri getirilebilmektedir. Bu çalışmada analiz ortamı Virtual Machine (VM) tercih edilmiştir.

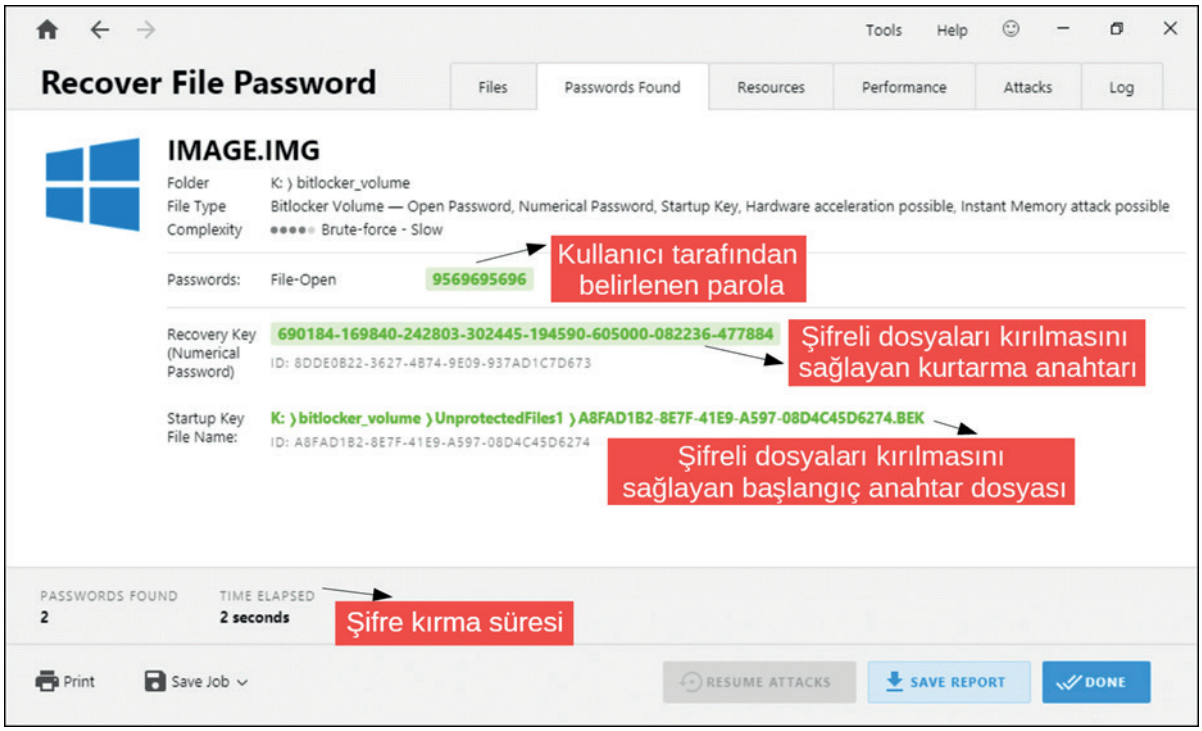
Analiz ortamı kurulduktan sonra FTK Imager ile E02 formatında alınan imaj kopyası canlandırıldığında tüm bölümlerin şifreli olduğu görülmüştür (Şekil 8).

Şekil 8. Dosyaların "BitLocker" kullanarak şifrelendiğini gösteren ekran görüntüsü.

Bitlocker, Windows işletim sistemlerinde kullanılan sistemde bulunan verileri ve dosyaları güvenli şekilde şifreleme yöntemidir. BitLocker, diğer dosya şifreleme yöntemlerinden farklı olarak, sitemdeki sürücünün tamamını şifrelemektedir. Kullanıcı sürücü içerisine bir veri ya da dosya eklendiğinde BitLocker otomatik şifreleme işlemini gerçekleştirmektedir. Böylece kullanıcı ağ üzerinden üçüncü kişilere veriler ya da dosyalarını paylaşsa da şifreli şekilde iletilir ve şifreler ancak yetkili kişi tarafından parolası girilerek açılmaktadır.

Şüpheli bilgisayardaki dosyaların şifreli olduğu ve şifreleme türü tespit edildikten sonra şifre kırma aşamasına geçilmiştir. Şifre kırmak için şifreleme türü olan "BitLocker" hangi programlar ile kırılabileceği yönünde açık kaynak araştırması yapılmıştır. BitLocker, SHA-256 ve AES gibi oldukça karmaşık şifreleme algoritmasına sahiptir (Milo vd. 2011; Beşkirli vd. 2019). 2019 yılında Agostini ve Bernaschi, BitLocker yöntemiyle şifrelenmiş dosyaların şifrenin kırılması ve erişim sağlanması üzerine vaka analizi çalışması yapmışlardır (Agostini, Bernaschi. 2019). Çalışmada Windows işletim sistemine sahip bilgisayarda BitLocker yöntemiyle şifrelenmiş dosyaların şifrelerini kırmak için geliştirdikleri "bitcracker" isimli bir program önermişlerdir. Çalışma sonuçları başarılı olsa da önerilen kullanılan bitcracker şifre kırma programının yeterliliği konusunun tartışmalı olduğu ve geliştirilmesi yönünde daha fazla çalışmalar yapılması gerekliliğini belirtmişlerdir. 2015 yılında Kumar yapmış olduğu çalışmada adli incelemelerde sıklıkla karşılaşan bir durum olan disk üzerinde veya bir bölümündeki dosyaların şifreli olması halinde Passware Kit Forensic (PKF) programının kullanılabileceğini önermiştir.

Yapılan araştırma sonucu adli analizlerde de sıklıkla kullanılan Passware Kit Forensic (PKF) ücretsiz sürümü kullanılabileceği sonucuna varılmıştır. İnceleme bilgisayarına PKF yüklendikten sonra PFK'in "files" sekmesinden alınan imaj kopyası eklendi. İmaj kopyadaki şifrelerin kırılması için "Combine Attacks" (içerisinde sözcük saldırısı ve kaba kuvvet saldırısı bulunan) sekme seçilerek şifre kırma süreci başlatılmışıdır. Analiz sonucunda "BitLocker" ile şifrelenmiş sürücü başarılı şekilde şifresi kırılmıştır (Şekil 9).



Şekil 9. Passware Kit Forensic (PKF) programıyla şifreli dosyaların şifre kırılma işlemi ekran görüntüsü.

Şekil 9'da PKF programıyla şifreli dosyaların başarılı bir şekilde kırıldığını görülmektedir. Şifre kırma işlemi sonucunda kullanıcı tarafından belirlenen parola "9569695696" tespit edilmiştir. Ayrıca şifreli dosyaların kırılmasını sağlayan kurtarma anahtarı ise "690184-169840-242803-302445-194590-605000-082236-477884" 48 haneden oluştuğu anlaşılmıştır. Bu sonuç BitLocker yöntemiyle şifrelenen dosyalarıda potansiyel şifrelerin oluşan bir tablo (Hellman tabloları veya Gökkuşağı tabloları gibi) hazırlanması ve denenmesinin uygun bir yöntem olmadığı sonucuna varılabilir. Dahası PKF programı incelenen vaka örneğindeki şifreyi (geçen süre: 2 saniye) oldukça kısa bir sürede başarıyla tamamladığı görülmektedir.

6. SONUÇLAR

Bilgi teknolojilerin kullanımı ve bilginin kullanılmasının artmasıyla yeni sorunların da beraberinde getirilmiş özellikle bilginin güvenli olarak saklanması yetkisiz kişilerin erişimine geçmemesi için güvenlik önlemleri alınması zorunlu hale

getirmiştir. Bilginin öneminin artmasıyla saldırganlarda bilgiyi ele geçirmek için yeni yöntemler geliştirmekte her geçen gün yeni saldırı türlerini piyasaya sürmektedir. Bu durum, e-ticaret şirketler, resmi devlet kurumları ve kişisel kullanıcılar bu saldırılara engel olmak ve yetkisiz kişilerin erişimini engellemek için yeni tedbirler alamaya zorlamaktadır. Alınan bu tedbirler (yeni şifreleme yöntemlerinin zorluk ve karmaşıklığı) bazı durumlarda şifreli verilere ulaşılmasının zorlaştırmakta hatta kırılması onlarca yıl zaman alabilmektedir. Özellikle şifrelerin unutulması ya da adli incelemelerde şifreli verilerin incelemesi sürecine verilere ulaşılmasında büyük bir engel oluşturmaktadır.

Bilgi sistemleri veya dosyaların şifreleme yöntemler ve kullanılan algoritmalar çok çeşitlilik göstermekle birlikte karşılaşan olaylara yönelik herkes tarafından kabul gören bir şifre kırma yöntemi bulunmamakla birlikte bazı durumlarda sadece tek bir olaya uygulanabilir bir yaklaşım geliştirilmesi gerekebilmektedir. Bu durum şifre kırma sürecinin en büyük problemlerinden birisidir.

Şifrelemiş verilerin kırılması için yöntemler geliştirilmeye devam etse de mevcut uygulamaların başarı oranı halen tartışma konusudur. Kullanılan yöntem ve şifre kırma programları kadar şifre kırma için kullanılan iş bilgi ayarlarının donanım özellikleri de süreci etkileyen önemli bir etkendir. Bu çalışmada şifreleme saldırıları, yöntemleri ve kullanılan en popüler şifre kırma programları ele alınarak gerçek bir adli inceleme örneği üzerinde şifre kırma süreci detaylı olarak incelenmiştir. Seçilen adli vaka örneği "BitLocker" yöntemi kullanılarak şifrelenmiş olduğu tespit edildikten sonra şifrenin kırılması için yapılan açık kaynak araştırma sonucunda PKF programı şifre kırma işlemlerinde kullanılabileceği öngörülmüştür ve PKF şifre kırma programı tercih edilmiştir. Yapılan şifre kırma işlemleri sonucunda adli vaka örneğinde başarıyla şifrenin kırılmasıyla sonuçlanmıştır. Seçilen adli vaka örneğinde kullanılan yöntemin ve seçilecek şifre kırma programının tercih edilirken adli uzmanları ve diğer araştırmacılar tarafından tekrarlanabilir olması için ücretsiz programlar kullanılmasına özellikle dikkat edilmiştir. Sonuç olarak çalışma sonuçlarıyla adli bilişim uzmanlarına ve bu alanda yapılacak akademik çalışmalara katkı sağlayacağı düşünülmektedir. Adli vaka analizlerinde kullanılan şifre kırma yaklaşımları benzer olmakla beraber farklılıklarda içerebilmektedir. Bu nedenle çalışmanın farklı örneklerle tekrarlanması faydalı olacağı düşünülmektedir.

Hakem Değerlendirmesi: Dış bağımsız.
Çıkar Çatışması: Yazar çıkar çatışması bildirmemiştir.
Etik Komite Onayı: Etik komite onayı alınmıştır.
Finansal Destek: Yazar bu çalışma için finansal destek almadığını beyan etmiştir.
Teşekkür: Yazar, bu çalışmanın analiz kısımlarının hazırlanmasında altyapı desteği sağlayan Çankırı Karatekin Üniversitesi Eldivan Sağlık Hizmetleri Meslek Yüksek Okulu Birimine teşekkür eder.

Peer-review: Externally peer-reviewed.
Conflict of Interest: The author has no conflict of interest to declare.
Ethics Committee Approval: This study approved by an ethical committee
Grant Support: The author declared that this study has received no financial support.
Acknowledgement: The author would like to thank Çankırı Karatekin University Eldivan Health Services Vocational School Unit for providing infrastructural support in the preparation of the analysis parts of this study.

Kaynaklar/References

Al Fahdi, M., Clarke, N. L., & Furnell, S. M. (2013, August). *"Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions."* In 2013 Information Security for South Africa (pp. 1-8). IEEE.

Aggarwal, S., Houshmand, S., & Weir, M. (2018). *"New technologies in password cracking techniques."* In Cyber Security: Power and Technology (pp. 179-198). Springer, Cham.

Agostini, E., & Bernaschi, M. (2019). *"BitCracker: BitLocker meets GPUs"*. arXiv preprint arXiv:1901.01337.

Beşkirli, A., Özdemir, D., & Beşkirli, M. (2019). *"Şifreleme Yöntemleri ve RSA Algoritması Üzerine Bir İnceleme"*. Avrupa Bilim ve Teknoloji Dergisi, 284-291.

Bhanot, R., Hans, R. (2015). "*A review and comparative analysis of various encryption algorithms."* International Journal of Security and Its Applications, 9(4): 289-306.

Billet O., Gilbert, H. (2006). *"Cryptanalysis of rainbow."* Security and Cryptography for Networks, 4116:336-347.

Castelluccia C., Durmuth M., Perito, D. (2012). "*Adaptive password-strength meters from Markov models."* Proc. of the Network and Distributed System Security Symposium.

Dass, A.S., Prabhu, J. (2020). *"Hybrid coherent encryption scheme for multimedia big data management using cryptographic encryption methods."* International Journal of Grid and Utility Computing, 11(4):496-508.

Dürmuth, M., Angelstorf, F., Castelluccia, C., Perito, D., & Chaabane, A. (2015, March). *"OMEN: Faster password guessing using an ordered markov enumerator"*. In International Symposium on Engineering Secure Software and Systems (pp. 119-132). Springer, Cham.

Guddeti, P., Dharavath, N. (2020). *"Analysis of password protected Document."* COMPUSOFT: An International Journal of Advanced Computer Technology, 9(7): 3762-3767.

Harichandran, V. S., Breitinger, F., Baggili, I., & Marrington, A. (2016). *"A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later."* Computers & Security, 57, 1-13.

Hassan, N. A. (2019). *"Digital Forensics Basics: A Practical Guide Using Windows OS."* Apress.

Hellman, M. (1980). *"A cryptanalytic time-memory trade-off."* IEEE transactions on Information Theory, 26(4), 401-406.

Hitaj, B., Gasti, P., Ateniese, G., & Perez-Cruz, F. (2019, June). *"Passgan: A deep learning approach for password guessing."* In International Conference on Applied Cryptography and Network Security (pp. 217-237). Springer, Cham.

Hur, U., Park, M., Kim, G., Park, Y., Lee, I., Kim, J. (2019). *"Data acquisition methods using backup data decryption of Sony smartphones."* Digital Investigation, 31:200890.

Houshmand S., Aggarwal S. (2017). *"Using personal information in targeted grammar-based probabilistic password attacks."* In: IFIP International Conference on Digital Forensics. 285-303.

Kara, İ. (2019). *"Kaba Kuvvet Saldırı Tespiti ve Teknik Analizi."* Sakarya University Journal of Computer and Information Sciences, 2(2): 61-69.

Kaya, Ö. F., Öztürk, E. (2017). *"Veri ve Ağ Güvenliği İçin Uygulama ve Analiz Çalışmaları."* Istanbul Ticaret Universitesi Fen Bilimleri Dergisi, 16(31): 85-102.

Kelley P.G., Komanduri S., Mazurek M.L., Shay R., Vidas, T., Bauer, L., ... Lopez, J. (2012). *"Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms."* In 2012 IEEE symposium on security and privacy, 523-537.

Kanta, A., Coisel, I., & Scanlon, M. (2020). *"A survey exploring open source Intelligence for smarter password cracking."* Forensic Science International: Digital Investigation, 35, 301075.

Kumar, S. (2015). *"Digital Evidence-Technical Issues."* Advances in Computer Science and Information Technology (ACSIT). 2(11) 42-47.

Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). *"Current challenges and future research areas for digital forensic investigation."* arXiv preprint arXiv:1604.03850.

Lehto, M., & Neittaanmäki, P. (Eds.). (2018). *"Cyber Security: Power and Technology"* (Vol. 93). Springer.

Saračević, M. H., Adamović, S. Z., Miškovic, V. A., Elhoseny, M., Maček, N. D., Selim, M. M., & Shankar, K. (2020). *"Data Encryption for Internet of Things Applications Based on Catalan Objects and Two Combinatorial Structures."* IEEE Transactions on Reliability.

Oechslin, P. (2003). *"Making a faster cryptanalytic time-memory trade-off,"* Advances in Cryptology, 617-630.

Raza, M., Iqbal, M., Sharif, M., & Haider, W. (2012). *"A survey of password attacks and comparative analysis on methods for secure authentication."* World Applied Sciences Journal, 19(4), 439-444.

Thing V.L.L., Ying H.M. (2009). *"A Novel Time-Memory Tradeoff Method for Password Recovery."*

Noorunnisa, N.S., Afreen, D.K.R. (2016). *"Review on Honey Encryption Technique."* International Journal of Science and Research, 2319-7064.

Madsen W. (1998). *"Encryption debate rages again."* Network Security, 5: 8-9.

Milo, F., Bernaschi, M., & Bisson, M. (2011). *"A fast, GPU based, dictionary attack to OpenPGP secret keyrings."* Journal of Systems and Software, 84(12), 2088-2096.

Thakur, S., Singh, A.K., Ghrera, S.P., Elhoseny, M. (2019). *"Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications."* Multimedia tools and Applications, 78(3):3457-3470.

Narayanan A., Shmatikov V. (2005). *"Fast dictionary attacks on passwords using time-space tradeoff,"* Proc. of the 12th ACM Conference on Computer and Communications Security, 2005.

Zhang Y., Monrose F., Reiter M.K. (2010). *"The security of modern password expiration: An algorithmic framework and empirical analysis."* In Proceedings of the 17th ACM conference on Computer and communications security, 176-186.

Wang, X. J., Liao, X. F., & Huang, H. Y. (2013). *"Improvement of rainbow table technology based on number cutting of reduction function."* Comput. Eng, 7, 36.

Weir M.S., B. Aggarwal de Medeiros., Glodek B. (2009). *"Password cracking using probabilistic context-free grammars,"* Proc. of the 30th IEEE Symposium on Security and Privacy, 391-405.

Weir M., Aggarwal S., Collins M., Stern, H. (2010). *"Testing metrics for password creation policies by attacking large sets of revealed passwords."* In Proceedings of the 17th ACM conference on Computer and communications security, 162-175.