POLİTEKNİK DERGİSİ

JOURNAL of POLYTECHNIC

ISSN: 1302-0900 (PRINT), ISSN: 2147-9429 (ONLINE)
URL: http://dergipark.org.tr/politeknik

Adli bilişim ve dijital delillerin windows işletim sistemi üzerinde incelenmesi

Computer forensics and examination of digital evidence on windows operating system

Yazar(lar) (Author(s)): *Bünyamin ÖNEL[1], Erdal IRMAK[2]*

ORCID[1]: 0000-0002-0239-4643

ORCID[2]: 0000-0002-4712-6861

Bu makaleye şu şekilde atıfta bulunabilirsiniz(To cite to this article): Önel B. ve Irmak E., "Adli bilişim ve dijital delillerin windows işletim sistemi üzerinde incelenmesi", ***Politeknik Dergisi***, 24(3): 1187-1196, (2021).

Erişim linki (To link to this article): http://dergipark.org.tr/politeknik/archive

DOI: **10.2339/politeknik.860163**

Adli Bilişim ve Dijital Delillerin Windows İşletim Sistemi Üzerinde İncelenmesi

Computer Forensics and Examination of Digital Evidence on Windows Operating System

Önemli noktalar (Highlights)

- *Adli Bilişim ve dijital delillerin önemi/The importance of computer forensic and digital evidence*
- *Adli bilişim süreçleri/Computer forensic processes*
- *Windows üzerinde adli bilişim analizi/Computer forensic analysis on Windows*

Grafik Özet (Graphical Abstract)

Adli bilişim ve süreçleri hakkında değerlendirmeler yapılarak, Windows işletim sistemi bileşenleri üzerinde canlı analizler gerçekleştirilmiştir./ Forensic informatics and its processes have been evaluated, and live analysis has been performed on Windows system and components.

Şekil. Çalışmanın ana hatları **/ Figure.** Outline of the paper

Amaç (Aim)

Adli bilişim ana bilim dalına daha çok teknik boyuttta katkı sağlayarak, Windows işletim sistemi bileşenleri üzerinden dijital delil elde etmektir. /To obtain digital evidence through Windows operating system and its components by contributing more technical dimensions to the Computer forensic.

Tasarım ve Yöntem (Design & Methodology)

Adli bilişim ve süreçlerinin incelenmesine müteakip, Windows işletim sistemi üzerinde adli bilişim analizleri yapılmıştır. In addition to examination of computer forensic and processes, computer forensic analyses has been carried out on the Windows operating system.

Özgünlük (Originality)

Teknik olarak Windows sisteminin doğal servisi powershell kullanılmıştır. Ayrıca ücretsiz üçüncü parti yazılımlardan yararlanılmıştır./ Powershell, native service of Windows, has been used as technically. Furthermore, free 3rd party computer forensic software has been used.

Bulgular (Findings)

PowerShell ve ücretsiz yazılımlar ile kolaylıkla adli bilişim analizi yapılabildiği tespit edilmiştir./ It has been revealed determined that computer forensic analysis can be performed easily with PowerShell and free software.

Sonuç (Conclusion)

Adli bilişim, teknik yöntemlerle ele alınmış, elde edilen sonuçlar görsellerle desteklenmiştir./ Computer forensic is handled by technical methods and results are supplied screenshots.

Etik Standartların Beyanı (*Declaration of Ethical Standards*)

Bu makalenin yazarları çalışmalarında kullandıkları materyal ve yöntemlerin etik kurul izni ve/veya yasal-özel bir izin gerektirmediğini beyan ederler. / The authors of this article declare that the materials and methods used in this study do not require ethical committee permission and/or legal-special permission.

Adli Bilişim ve Dijital Delillerin Windows İşletim Sistemi Üzerinde İncelenmesi

Araştırma Makalesi / Research Article

Bünyamin ÖNEL[1], Erdal IRMAK[2*]

[1]Hoca Ahmet Yesevi Üniversitesi, Türkiye Türkçesi ile Uzaktan Eğitim Programları (TÜRTEP), Siber Güvenlik Tezsiz Yüksek Lisans Programı, Türkiye

[2]Gazi Üniversitesi, Teknoloji Fakültesi, Elektrik Elektronik Mühendisliği Bölümü, Türkiye

(Geliş/Received : 13.01.2021 ; Kabul/Accepted : 20.02.2021 ; Erken Görünüm/Early View : 03.03.2021)

ÖZ

İnternet ve bilişim sistemleri üzerinde işlenen suçları tespit etmek amacıyla gerçekleştirilen adli bilişim incelemelerinin önemi, her geçen gün daha iyi anlaşılmaktadır. Bu minvalde suç ve suçlunun tespiti konusunda hukuka uygun dijital delillerin elde edilmesinin önemi çok büyüktür. Adli bilişim incelemelerinde, birçok farklı yöntem ile dijital deliller elde edilebilir. Özellikle bilişim sistemleri üzerinde kullanılan işletim sistemleri buna çok iyi bir örnektir. Küresel ölçekte olduğu gibi ülkemizde de gerek kişisel kullanımlarda gerekse kurumsal şirketlerde Windows işletim sistemi yaygın olarak kullanılmaktadır. Sanal dünya üzerinde işlenen suçların ve mağduriyetlerin çoğunluğu bu sistem üzerinde yaşanmaktadır. Bu nedenle çalışmada, Windows işletim sistemi üzerinde adli bilişim çalışması yapma gereksinimi duyulmuştur. Adli bilişim alanındaki güncel çalışmalar literatüre daha çok kavramsal ve hukuksal düzenleme olarak katkıda bulunmaktadır. Bu çalışmada ise metodolojik ve teknik analizler birlikte kullanılarak Windows PowerShell ve üçüncü parti yazılımlarla adli bilişim çalışması yapılması amaçlanmıştır. Böylece sistem bileşenleri üzerindeki dijital deliller, metedolojik ve teknik yöntemlerle analiz edilip, elde edilen sonuçlar görsel verilerle ortaya konulmuştur.

Anahtar Kelimeler: Adli bilişim, dijital delil, windows işletim sistemi.

Computer Forensics and Examination of Digital Evidence on Windows Operating System

ABSTRACT

The importance of computer forensic reviews carried out to detect crimes committed on the Internet and information systems is be better understood day by day. In this regard, it is very important to obtain digital evidence in accordance with the law in the detection of crime and criminals. In computer forensic investigation, digital evidence can be obtained by many different methods. Operating systems, especially those used on information systems, are a very good example. It is the most preferred Windows operating system in both personal and corporate structures in our country as it is on a global scale. For this reason, the intensity of the crimes committed and the victimization experienced in the virtual world is on this system. Therefore, this study carries out the forensic work on the Windows operating system. Current studies in the field of forensic informatics contribute to the literature mostly as a conceptual and legal arrangement. However, this paper aims to do forensic work with Windows PowerShell and third party software by using methodological and technical analysis together. Thus, digital evidence on system components has been analyzed using methodological and technical methods, and the results obtained have been presented with visual data.

Keywords: Computer forensics, digital evidence, windows operating system.

1. GİRİŞ (INTRODUCTION)

İçinde bulunduğumuz yüzyılın birinci çeyreğinde gelişen ve ilerleyen teknoloji ile birlikte, üretim ve tüketim faaliyetleri bilişim teknolojisi ve sistemlerine bir zincirin halkaları şeklinde bağlanmıştır. Özellikle teknolojik sistem yönetimi konusunda, ileri bilgi birikimine ve tecrübeye sahip insanların arasında kötü niyetli eylem yapabilecek kişilerin olabileceği aşikârdır. Bu potansiyeldeki insanların, bilişim sistemleri birimlerinde tedbirleri istismar ederek zarar verme amacında olmaları, üretim ve tüketim faaliyet zinciri üzerinde keskin olarak başarı ve başarısızlıkları şekillendirebilir. Bu insanlar kendileri için tehdit unsuru varsaydıkları kişi, kurum vb. düzenlere zarar vermek istediklerinde ilk olarak bilişim sistemlerinin bağlılıklarına ve bağlantılarına yönelmektedirler. Bu nedenle olumsuz bir durum sonrasında gerçekleştirilen aksiyonları ve suç unsurunun bulunup bulunmadığını tespit etmek amacıyla adli bilişim incelemeleri yapılır.

Dijital cihazlarla işlenen suçları tespit etmek amacıyla yapılan araştırmalar ve çalışmalar, bilişim sistemleri ve elektronik cihazların dâhil olduğu adli olaylarda adli bilişim disiplinin oluşmasını sağlamıştır. Yıllar içerisinde akademik ve teknik çalışmalar ile bu bilim alanı, devasa ekomik harcamalarla hızlı bir şekilde büyümektedir. Bu durumun önemi istatistiklere de yansımıştır. Adli bilişim incelemelerinde kullanılan yazılım, donanım ve servis hizmetlerinin ekonomik büyüklüğü 2017 yılında 4,62 milyar dolar seviyelerinde iken, 2022 yılına kadar yıllık %15,9 büyüme oranı ile 9,68 milyar dolar seviyelerine gelmesi beklenmektedir [1].

*Sorumlu Yazar (Corresponding Author)
e-posta : erdal@gazi.edu.tr

Dijital delillerin elde edilmesinde özellikle bilgisayar işletim sistemleri üzerinde yapılan incelemeler, delil niteliği taşıyabilecek verilere ulaşılabilme olanağı sağlayacaktır. İşletim sistemleri tüm arama işlemlerine, dosya işlemlerine, sistem kayıtlarına, çalışan uygulamalara, internet geçmişi ve e-posta dosyaları gibi birçok farklı yapısal verilere ulaşabilme imkânı tanımaktadır. Bu nedenle işletim sistemleri üzerinde adli bilişim incelemeleri ile dijital delil elde edebilme olanağı çok fazladır. Literatür araştırmalarında benzer akademik çalışmalar yapılmıştır. Bu çalışmalardan bazılarının alana katkıları aşağıda özetlenmiştir.

Bulut bilişim teknolojisininin adli bilişim incelemelerine getirdiği zorluk alanları [2]'de bahsedilmektedir. Buna göre, güvenlik prosedürlerinin tam olarak olgunluğa erişmemesi nedeniyle bu alandaki zorlukların devam edeceği yönünde görüşler mevcuttur. Diğer yandan bulut bilişim teknolojisinde donanımların dağıtık yapıda olması ve verilerin bu ortam üzerinde zamandan ve mekandan bağımsız olarak sürekli dinamik halde olması, hukuksal olarak hangi ülkenin yasalarına tabii olacağı gibi bilinmezlikleri doğurmuştur. Bu çalışmayla yeni bir teknoloji olan bulut bilişim üzerinde adli bilişim konusu ile farkındalık yaratılmıştır. [3]'te ise ağırlıklı olarak açık kaynak uygulamaların işlevsellikleri ve adli kopyalama (yazılımsal ve donanımsal) hakkında bilgilendirmeler yapılmıştır. Ayrıca CMK maddeleri özelinde dijital delillerin hukuksal boyutu hakkında da değerlendirmeler yapılmıştır. Böylece dijital delillerin elde edilmesi sırasında yazılımsal ve donanımsal olarak kopyalama işlemlerinin önemi ve güvenliği vurgulanmıştır.

[4] numaralı referansta olay yeri incelemelerinde elektronik delillerin toplanması aşamasında delil bütünlüğü için yapılması gereken prosedür ve işlemler (imaj alma, hash değeri, zaman damgası belirleme) hakkında çalışmalar yapılmıştır. Bu işlemler ile elektronik delillerin bütünlüğünün korunması, soruşturma ve kovuşturma süreçlerinin daha güvenilir bir şekilde ilerleyeceği belirtilmiştir. Benzer şekilde [5]'te de olay yeri incelemelerinde işletim sistemleri ve bu sistemler üzerinde çalışan kayıt defteri, geçici dosyalar, internet geçmişi ve sistem üzerinde kurulu zararlı yazılımların tespiti hakkında dijital delil elde etmeye yönelik genel bilgiler paylaşılmıştır. Bu bilgi paylaşımı ile adli bilişim ve dijital delilller hakkında bilgi edinmek isteyen bireylerin veya uzmanların bilgi seviyelerinin artırılması hedeflenmiştir.

[6] numaralı kaynakta belirtildiği üzere, bilgisayar depolama alanlarının genişlemesi nedeniyle adli bilişim sürecinde incelenecek veri boyutu da artmıştır. Bu nedenle soruşturma ve kovuşturma süreçleri uzayarak, hükmün verilmesinin ertenmesi gibi sonuçların ortaya çıktığı tespit edilmişir. Bu teknolojik değişimin süreçleri uzatması sebebiyle önceliklendirme metodu üzerine yoğunlaşılmıştır. Bu işlem olay yerinde önceliklendirme ve laboratuvar ortmanında önceliklendirme şeklinde iki kısma ayrılarak, bu süreçler içerisinde elde edilecek dijital delillerin bilimselliği hakkında değerlendirmeler yapılmıştır. Benzer bir çalışma [7]'de sunulmuş olup genel olarak adli bilişim türleri, dijital delil elde edilebilecek cihazlar, adli bilişim süreçleri, adli kopyalama, hash değeri gibi kavramlar hakkında değerlendirmeler yapılmıştır. Ayrıca ülkemizde ve dünyada hukuk sistemlerinde dijital delillerin elde edilmesi ile ilgili yasal mevzuatlar yorumlanarak tespitlerde bulunulmuştur.

Adli bilişim ve dijital delillerin incelenmesi konusunda ülkemizde yapılan çalışmalar çoğunlukla; kavramsal olarak hukuki yasal düzenlemeler ve farkındalık kazandırmaya yönelik olup, bilgisayar dijital ortam bileşenleri üzerinde, özgün teknik incelemelerde bulunulan çok az sayıda çalışma yapılmıştır. Kavramsal olarak yapılan çalışmalar; adli bilişim süreç yönetimi, adli bilişimin soruşturma ve kovuşturma süreçlerindeki yeri, Ceza Muhakemesi Kanununun 134. maddesi ve diğer ilgili madde değerlendirmeleri şeklinde ifade edilebilir.

Teknik çalışmalarda ise adli bilişim incelemeleri için üçüncü parti yazılımlar kullanılarak çalışmalar yürütülmüştür. Bu yazılımlarla genellikle teknik analizler yerine, uygulamaların nasıl kullanılacağına yönelik bilgiler paylaşılmıştır. Yapılan çalışmaların, çoğunlukla bilgisayar sabit diskleri üzerinden imaj alma işlemleri ve yüzeysel olarak sistem dosyaları incenlemesi şeklinde olduğu görülmüştür.

Yukarıda özetlenen nedenler de göz önüne alınarak sunulan bu çalışmada, günümüz bilgisayar sistemleri üzerinde en çok kullanılan Windows işletim sistemine yönelik olarak kavramsal açıklamalarla beraber teknik boyutta adli bilişim inceleme süreci ele alınmıştır. Tüm bunlarla beraber adli bilişim anabilim dalına katkı sağlamak amacıyla, metodolojik ve teknik boyutta dijital delillerin, ağırlıklı olarak işletim sisteminin doğal servisleri kullanılarak da elde edilebileceği görülmüştür.

Çalışmada öncelikle konu kavramsal çerçevede akademik araştırmalar yapılarak adli bilişim, adli bilişim süreçleri ve işletim sistemi ile ilgili genel değerlendirmeler yapılmıştır. Çalışmanın ana yapısını oluşturan, Windows işletim sistemi üzerinde adli bilişim ve dijital delil incelemeleri için öncelikle sisteminin hangi bileşenleri üzerinde analizler yapılabileceği tespit edilmiştir. Daha sonra çalışmaya özgünlük katan işletim sisteminin doğal uygulaması olan PowerShell kullanılarak ve açık kaynak ücretiz dağıtım adli bilişim yazılımlarından da faydalanarak dijital delil elde etme süreci gösterilmiştir. Son olarak elde edilen bulgular yorumlanarak öneriler getirilmiştir.

2. ADLİ BİLİŞİM (COMPUTER FORENSICS)

Günümüzde internet ve internet medyalarının bu denli yüksek kullanımı, bu mecraların konforlu yaşam tarzına katkı sağlamasının yanında, gerçek hayatta yaşanan adli olayların sanal dünyanın kendine has özelliklerine bürünüp insanların yaşantısına dâhil olmasını sağlamıştır. Böylelikle sanal merciler üzerinde meydana gelen adli olaylarda, adli bilişim bilişim ve dijital delillere ihtiyaç duyulmuştur. Adli bilişim; suç-ceza sistemi içerisinde suç ve suçlunun var olup olmadığının tespiti konusunda bilişim sistemleri ve diğer elektronik cihazlar üzerinden hukuka uygun olarak elde edilen delilleri, adli makamlara

bir rapor şeklinde sunan anabilim dalı olarak açıklanabilir. Adli bilişim ve dijital delil kavramlarının ortaya çıkmasıyla suç ve delil kapsamı genişlemiş olup, yeni sürece uygun tanım ve tespitlerin kriminoloji bilimi özelinde desteklenmesi elzem hale gelmiştir.

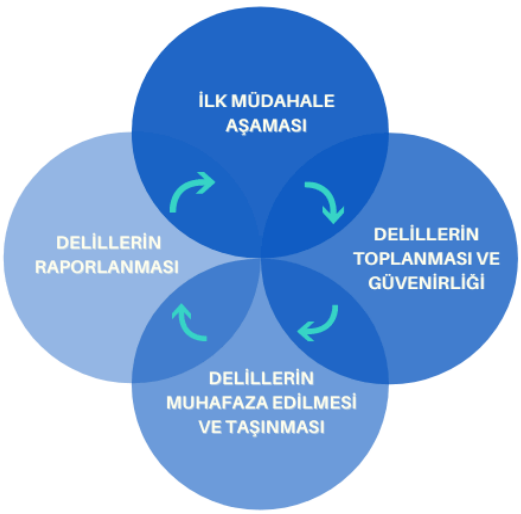
2.1. **Adli Bilişimin Temel Amacı** (The Main Purpose of Computer Forensics)

Yargılama süreçlerinde dijital delillere ihtiyaç duyulması halinde, adli bilişim çalışmaları başlatılır. Bu süreç boyunca adli bilişim çalışmalarında temel amaç, hukuka uygun dijital delillerin elde edilip adli makamlara bir rapor halinde sunulmasıdır. Yapılan çalışma sadece, dijital delilleri teknik yöntemlerle elde edip, adli makamlara sunulmasıdır. Hüküm yetkisi tamamen adli makamların inisiyatifindedir.

2.2. **Adli Bilişim Süreçleri** (Computer Forensics Processes)

Adli bilişim süreci; yargı makamlarının suç ve suçlunun tespitinde gerekli olabilecek dijital delillere ihtiyaç duyması halinde, kolluk kuvvetleri veya diğer uzman görevliler tarafından yürütülen adli bilişim çalışmaları, şeklinde açıklanabilir.Kolluk kuvvetlerine yansıyan kriminal olaylarda delillerin elde edilmesi ve açığa çıkartılması için olay yeri incelemesi sırasında yapılması gereken kurallar bütünü, benzer şekilde adli bilişim çalışmalarında da geçerli olduğu söylenebilir. Adli bilişim safhalarının, doğru ve eksiksiz yönetilmesi elde edilen dijital delillerin adli makamlar tarafından kabul görmesinde çok önemli bir aşamadır.

Bu minvalde adli bilişim süreç yönetimi için temel amaç, soruşturma sürecinden başlayıp kovuşturma sürecinin sonuna kadar geçen süre içerisinde, hukuka uygun olarak dijital delillerin elde edilmesi, bütünlüğünün korunması ve doğru şekilde muhafaza edilerek, yargı makamlarına bir rapor eşliğinde delillerin sunulmasıdır. Adli bilişim süreçleri ile ilgili detaylı bilgilere [8] numaralı kaynak üzerinden ulaşılabilir. Şekil 1'de adli bilişim sürecinde izlenmesi gereken adımlar genel olarak belirtilmiştir.



Şekil 1. Adli bilişim süreçleri (Computer forensics processes)

2.2.1. **İlk müdahale aşaması** (First intervention phase)

Bu aşamada, adli bilişim konusunda uzman kolluk kuvvetleri veya dış kaynak adli bilişim uzmanları olay yerine intikal ettiklerinde yapılması gereken işlemleri kapsamaktadır. İlk aşama sürecini başka bir şekilde ifade etmek gerekirse, dijital delillerin elde edilmesi için olay yeri aramasında yapılması gereken işlemler şeklinde de ifade edilebilir.

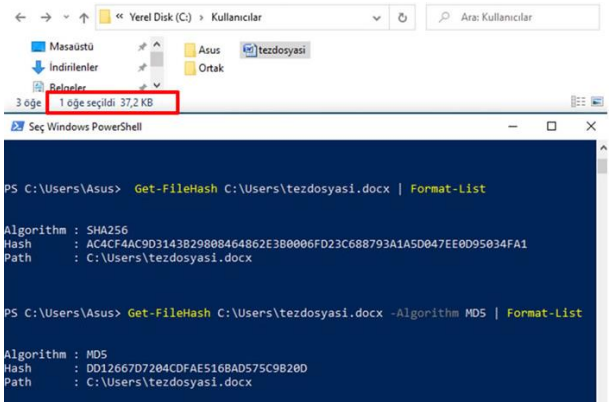
2.2.2. **Dijital delillerin toplanması ve güvenirliği** (Collection and reliability of digital evidence)

Dijital delillerin toplanmasından başlayıp, adli makamlara ulaşıncaya kadar geçen süreçte orijinal yapılarının korunmuş olması, yasal olarak kullanılmalarında ki en önemli parametrelerden biridir. Dijital delil orijinalliğinin korunduğunun ispatı, Hash değeri (algoritması) imzası ile tespit edilebilir. Deliller üzerinde herhangi bir değişiklik yapılıp yapılmadığını kontrol etmek amacıyla Hash değeri hesaplatılır ve böylece üzerinde çalışılan verilerin orijinali ile aynı olup olmadığının doğruluğu kontrol edilmiş olur [9]. Günümüz teknolojinde güvenilir ve en çok kullanılan Hash algoritmaları Md5 (Message-Digest Algoritm) ve SHA (Secure Hash Algoritm) olarak öne çıkmaktadır [10].

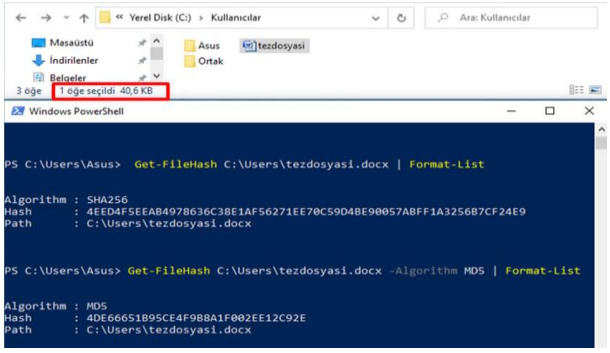
Windows işletim sistemleri üzerinde doğal sistem uygulaması olan PowerShell yardımı ile herhangi bir dosya için Hash değeri oluşturulabilir. Bu şifreli hesaplama değeri, özellikle 3. parti yazılımlara gerek kalmadan son derece güvenli bir şekilde üretilebilir. Örnek olarak, bu çalışma kapsamında PowerShell üzerinde Sha ve Md5 algoritmalarını kullanarak tezdosyasi.docx isimli Word belgesi için Hash değeri üretilmiştir. Sha için Get-FileHash parametresi kullanılmıştır [11]. Şekil 2 üzerinde gösterildiği gibi tezdosyasi.docx belgesinin dosya yolunu göstererek Format-List parametresi ile Hash değerinin gösterilmesi sağlanmıştır. Get-FileHash kullanılarak oluşturulan Sha değeri Windows üzerinde varsayılan olarak 256 bit şeklinde tanımlanmıştır. Sha ile Hash değerini ürettikten sonra PowerShell üzerinde diğer bir değer üretme algoritması olan Md5 ile tezdosyasi.docx belgesi için farklı bir Hash değer imzası üretilmiştir. Yine aynı şekilde Sha Hash değeri için kullanılan Get-FileHash parametresiyle birlikte ek olarak dosya uzantısını belirttikten sonra -Algorithm parametresi kullanılır. Bu parametre, Md5 Hash değeri için özgün bir komut olarak kullanılmaktadır. Tezdosyasi.docx belgesi içersinde yapılan ufak değişiklikler sonucu yeni Hash değeri hesaplamasında farklı bir değerin ortaya çıktığı görülmüştür. Şekil 3'te gösterildiği gibi, yeni Hash değerleri belirtilmiştir.

Dijital delilin orjinal olduğunu ispatlanması adına veriler üzerinde Hash değeri imzası üretilmekteydi. Bu duruma ek olarak elde edilen dijital delile ilk ulaşılma zamanı (zaman damgasının) belirlenmesi büyük önem arz etmektedir. Zaman damgası ve Hash değer üretimi ile veriler üzerinde ikili kontrol noktası oluşturularak, dijital delilin güvenirlik seviyesi artırılmış olacaktır. Verilere zaman damgası eşleştirmesi yapılırken dikkat edilmesi gereken en önemli husus, sistem saatinin doğruluğunun

tespit edilmesidir. Özellikle bir ağ yapısına dâhil olarak çalışan bilgisayarlar, sunucular üzerinde belirlenen zaman bilgisine göre sistem saatini gösterir. Bu durumun daha veriye ilk ulaşılma zamanında tespit edilmesi ve buna göre küresel zaman bilgisinin belirlenmesi oldukça önemlidir.



Şekil 2. Sha ve md5 hash imza değeri (Sha and md5 hash signature value)



Şekil 3. Deney seti (Experimental setup)

2.2.3. Dijital delillerin muhafaza edilmesi ve taşınması (Preservation and transportation of digital evidence)

Veri depolama cihazları, Usb bellekler ve artık günümüzde bulut bilişimin gelişmesiyle beraber kullanımları yavaş yavaş sonlanan DVD belleklerin muhafaza edilmesi ve güvenli bir şekilde taşınması son derece kritiktir. Bu depolama birimlerinin hassasiyetleri nedeniyle dış etkenlerden gelebilecek manyetik etkiye maruz kalma ve ortam sıcaklığındaki keskin değişimler zarar görmelerine ve veri kayıplarına neden olabilir. Bu gibi etkileri ortadan kaldırmak veya sınırlandırmak adına; faraday çantası, antistatik baloncuklu delil zarfları ve kağıt kaplı antistatik delil zarfları gibi bazı ekipmanlar mevcut olup, [12] numaralı kaynaktan konuyla ilgili detaylı bilgiler alınabilir.

2.2.4. Dijital delillerin raporlanması (Reporting of digital evidence)

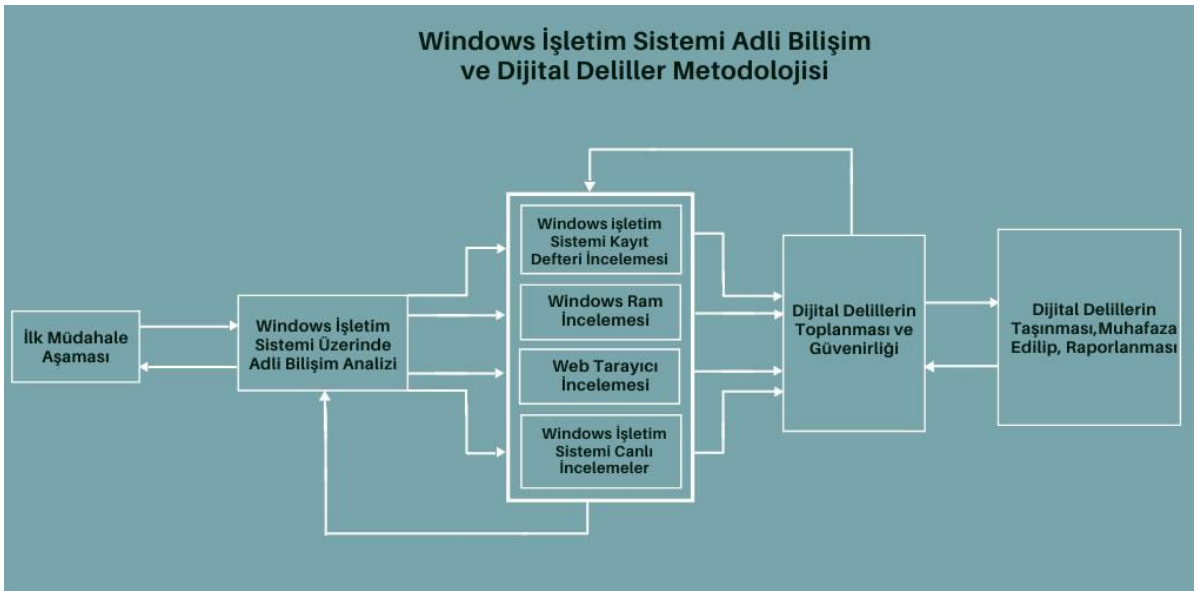
Dijital delil incelemelerinden sonra elde edilen sonuçlar, adli bilişim uzmanlarının da değerlendirmelerini içeren bir rapor halinde adli makamlara sunulur. Teknik incelemelerde çok fazla mesleki terim kullanılması adli makamlarca raporların doğru olarak değerlendirilmesine engel teşkil edebilir. Bu nedenle ilgili raporlar hazırlanırken, tarafların anlayabileceği sadelik ve açıklıkta olması önemlidir. Varsayımlarda bulunmak bir rapordaki en belirgin zayıflıktır [13]. Adli bilişimciler tarafından dijital delillerin analiz edilmesi ile hazırlanan rapor, tamamen bilimsel ve teknik çalışmalarla hazırlandığı için kesinlik ifadeleri içermesi elzemdir. Kesin ifadeler içermeyen bir rapor bulanık olarak addedilerek, tarafların itirazları sonucu adli bilişim süreçlerinin en başına dönülmesi gibi durumlar ortaya çıkabilir.

3. WINDOWS İŞLETİM SİSTEMİNDE ADLİ BİLİŞİM ANALİZİ

(COMPUTER FORENSICS ANALYSIS ON THE WINDOWS OPERATING SYSTEM)

İşletim sistemi, kullanıcıların elektronik cihazları kontrol etmelerini ve bu cihazların farklı donanım özelliklerini etkileşimli şekilde kullanmalarını sağlayan çekirdek yazılım bütünü şeklinde ifade edilebilir. Windows, günümüzde yoğun kullanılan işletim sistemlerinden biridir. Bu durumun nedenleri olarak; birçok donanım üreticisi ile olan anlaşmalar, şirketlere ve son kullanıcıya verilen servis destek ağının gelişmiş olması, geliştirilen uygulamaların çoğunun Windows altyapılı işletim sistemlerinde sorunsuz çalışıyor olması ve kullanım alışkanlıkları gibi sebepler gösterilebilir. Bundan ötürü adli olaylarda incelenen bilgisayarlardaki aktivitelerin genellikle Windows işletim sistemi üzerinden gerçekleştirilmiş olması muhtemel olup bu çalışmada da Windows işletim sistemi üzerinde yoğunlaşılmıştır.

Şekil 4'te çalışmanın metodolojisi diyagram halinde gösterilmiştir.



Şekil 4. Çalışma metodolojisi (Methodology of the study)

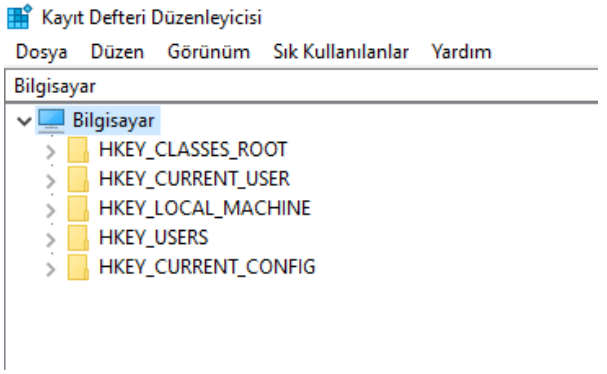
3.1. Kayıt Defteri İncelemesi (Registry Examination)

Kayıt defteri, Windows işletim sisteminin düzgün bir şekilde çalışmasını sağlayan, bileşenlerle ilgili tüm işlem kayıtlarının tutulduğu, yerel sistemin veritabanı şeklinde açıklanabilir. Yapısal olarak Şekil 5 üzerinde gösterildiği gibi beş önemli bölümden oluşmaktadır. Windows işletim sistemi üzerinde gerçekleştirilecek adli bilişim incelemelerinde kayıt defteri bileşenleri üzerinden elde edilecek veriler çok kıymetlidir. Kullanıcı bilgileri, tarayıcı bilgileri, sistem üzerinde oturum açma süresi ve saat bilgisi, bilgisayara takılmış harici depolama aygıtları gibi birçok bileşenle ilgili veriye buradan erişilebilir.

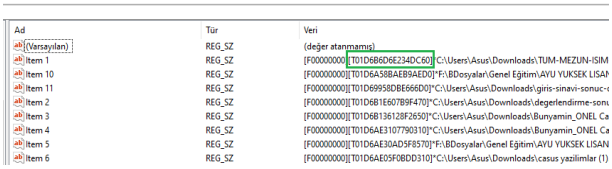
3.1.1. Microsoft ofis belgelerinin incelenmesi (Examination of microsoft office documents)

Kayıt defterinde, işletim sistemi üzerinde yapılan birçok işleme dair veri izleri tutulmaktadır. Son yapılan aktiviteler bir liste halinde kayıt defteri üzerinde Mru denilen dosya içerisinde tutulmaktadır. Mru (Most Recently Used); Windows işletim sistemi üzerinde en son açılan dosyaların bulunduğu dizin, dosya yolu ve son açılış zaman bilgisi gibi verilerin listelendiği yerdir [14]. Şekil 6'da gösterildiği gibi ilgili dizin takip edildiğinde en son açılan Excel belgelerinin bulunduğu Mru listesine ulaşılmaktadır. Benzer şekilde diğer Microsoft ofis araçlarının da Mru listelerine kayıt defteri üzerinden ulaşılabilir. Burada ilgili Excel belgesinin son açılış zaman bilgisi heksadesimal yani on altılık düzende verildiği için anlamsız halde gözükmektedir [15].

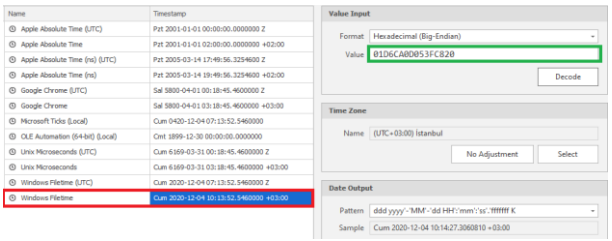
Şekil 6 üzerinde yeşil çerçeve ile gösterilen heksadesimal kodu, üçüncü parti bir yazılım olan Dcode.exe uygulaması ile çözümleyerek zaman bilgisi anlamlı hale getirilebilir. Örneğin Şekil 6' da incelenen dosyanın kodu kullanılarak tarih bilgisinin elde edilmesi, Şekil 7'de verilmiştir.



Şekil 5. Kayıt defteri bölümleri (Registry sections)



Şekil 6. Excel belgesinin dosya yolu ve mru değer gösterimi (File path and mru value representation of an excel document)

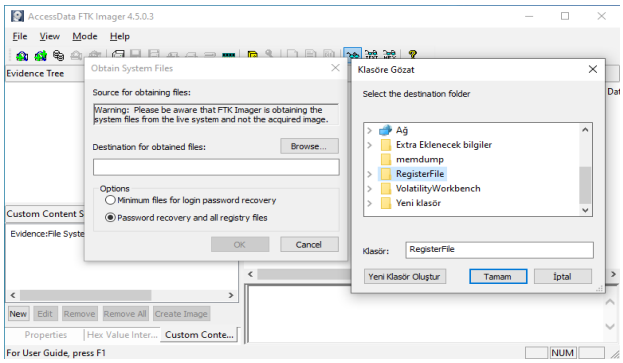


Şekil 7. Heksadesimal kod ile tarih bilgisi elde etme (Obtaining date information with hexadesimal code)

3.1.2. Kayıt defterinin Register Viewer ile görüntülenmesi (Displaying the registry with Register Viewer)

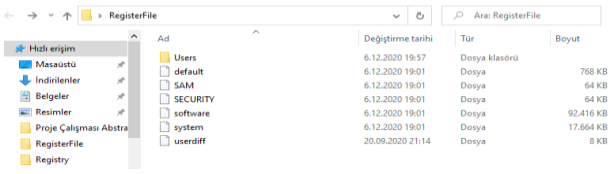
Şekil 8'de gösterildiği gibi Access Data Ftk Imaj uygulaması ile kayıt defteri dosyaları RegisterFile isimli klasöre birebir kopyalanmıştır. Bu işlem sonrası artık Access Data Register Viewer uygulaması ile bu dosyaların analiz işlemleri sorunsuz yapılabilir. Şekil 9'da gösterildiği gibi Kayıt defteri üzerinde yedekli olarak tutulan dosyaların imajı alınarak bir klasör içine birebir kopyalanmıştır. Burada kayıt defterine göre daha az bileşen gözükmesinin nedeni, sistem üzerinde gerçekleşen tüm olay kaydı ve kullanıcı bilgilerinin bu dosyalarda tutuluyor olmasıdır. Dosyaların incelenmesi ile işletim sistemi üzerinde gerçekleşen birçok olay kaydı açığa çıkarılmış olacaktır.

Özellikle Sam (Security Accounts Manager), güvenlik hesap yöneticisi, şeklinde tanımlanan dosya, kullanıcı bilgilerini barındırır. "C: \\ WINDOWS \\ system32 \\ config" adresi içerisinde yer almaktadır. İşletim sistemi üzerinde oturum açmaya çalışıldığında, daha önceden belirlenen parola bilgisi burada mevcuttur. Oturum açma sırasında girilen parola Sam dosyası içinde daha önce oluşturulmuş parola ile eşleşerek, doğru olması durumunda sisteme dâhil olmaya izin verir. Doğru olmayan bir parola girilmiş ise, yanlış parola girildiği uyarısını verir [16]. Şekil 10 üzerinde Access Data Ftk Imager ile Sam dosyası gösterilmiştir. Her bir satır için 16 oktetten oluşan heksadesimal format yapısı, içerik olarak 3 kısımdan oluşmaktadır. Anlamsal olarak soldan başlayarak 0-3 kısmı başlığın, 4-5 anahtar isim yapısının ve 8-15 verilerin ilgili satır özelinde son yazma zaman bilgisini belirtmektedir. Bu yapı içerisinde adli incelemelerde çok önemli olabilecek bazı kısaltma verileri bulunmaktadır. Bunlar, Nk: Anahtar isimleri, Vk: Anahtar veri değerleri, Sk: Windows güvenlik anahtarı gibi kısaltmalardır [17]. Sam dosyası üzerinde ilgili anahtar harfler aratıldığında Şekil 11 üzerinde gösterildiği gibi heksadesimal değerler bulunacaktır. Windows işletim sistemi üzerinde oturum açmış her kullanıcı için Ntuser.dat dosyası mevcuttur. Kullanıcıların sistem üzerinde yaptığı işlemler, gizli olarak bu dosya içerisinde tutulur. Yapılan değişiklikler, kullanıcı oturumu kapattığı sırada bu dosyaya kaydedilmektedir [18].

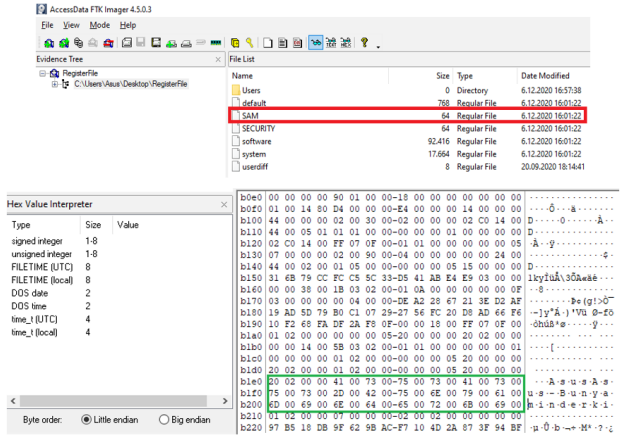


Şekil 8. Kayıt defteri imaj dosyası (Image file of the registry)

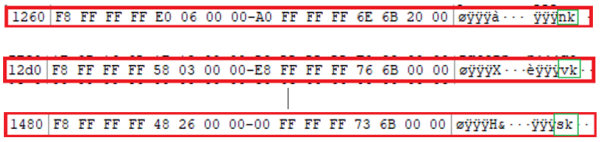
Diğer yandan Sam dosyasından bulunan sistem üzerinde işlem yapan kullanıcıların, en son hangi tarihte giriş yaptıkları ve diğer aktivite verileri Şekil 12 üzerinde gösterildiği gibi anlamlı hale getirilebilir. Kayıt defteri üzerinden imajı alınan dosyalardan biri de sistem dosyasıdır. Bu dosya içerisinde işletim sistemi üzerinde kullanılan ve kullanılmış depolama aygıt bilgilerine ulaşılabilir.



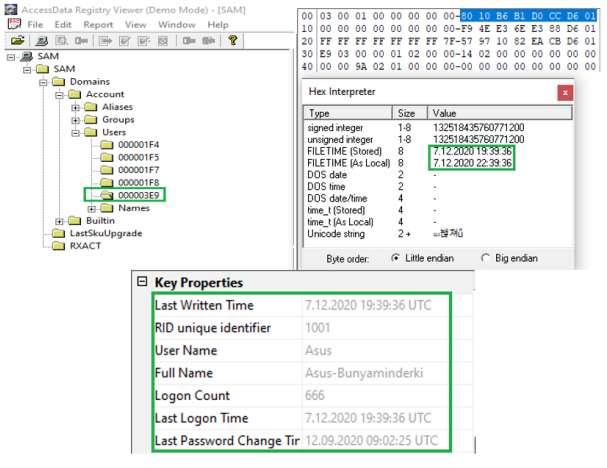
Şekil 9. İmaj dosyaları (Image files)



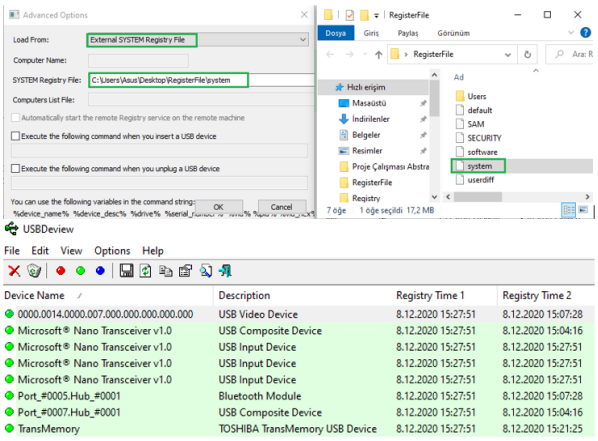
Şekil 10. Sam dosyasının heksadesimal formatta görüntülenmesi (View of sam file in hexadesimal format)



Şekil 11. Kısaltma verileri (Abbreviation data)



Şekil 12. Sisteme son giriş zamanı (System log in info)



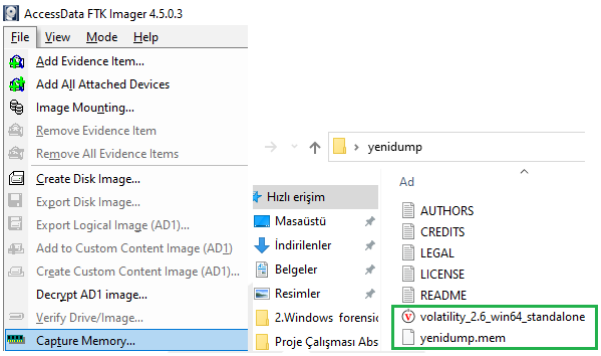
Şekil 13. Usbdeview üzerinde kayıt defteri sistem dosyasının gösterilmesi (Monitoring the registry system file on a Usbdeview)

Özellikle bilgisayar üzerinde kullanılmış Usb belleklerin geçmiş bilgileri bu dosya içerisinde tutulmaktadır. Üçüncü parti bir yazılım olan Usbdeview ile kayıt defteri üzerinden çekilen sistem dosyası detaylı olarak incelenebilir. İlgili uygulama üzerinde opsiyonlar>gelişmiş opsiyon seçenekleri takip edilerek, Şekil 13 üzerinde gösterildiği gibi istenilen tarihte sistem üzerinde kullanılmış Usb depolama birimleri görüntülenebilmektedir.

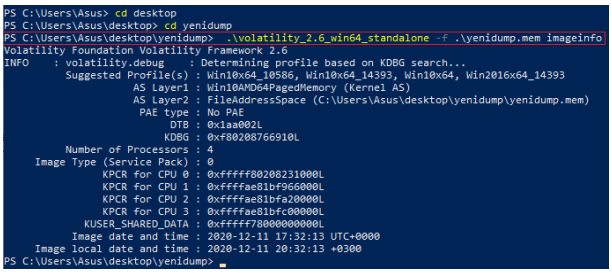
3.2. Ram İncelemesi (Ram Analysis)

İşletim sisteminin ana dosyaları üzerinde yapılan değişiklikler, sistem üzerinde çalıştırılmış uygulamalar, kullanıcıların açtığı dokümanlar, çevrimiçi olarak web site erişimleri, mail adres bilgileri gibi adli bilişim incelemelerinde kritik öneme sahip birçok veri kalıntısına, ram üzerinde yapılan analizlerle ulaşılabilir. Windows işletim sisteminin doğal uygulaması olan PowerShell üzerinde, elde edilen ram imaj dosyasının incelenmesi için Volatility Framework dosyası gereklidir. Python programlama dili ile yazılan açık kaynak kütüphane olan Volatility, Ram analizi incelemelerinde çok önemli bir rol oynamaktadır [19].

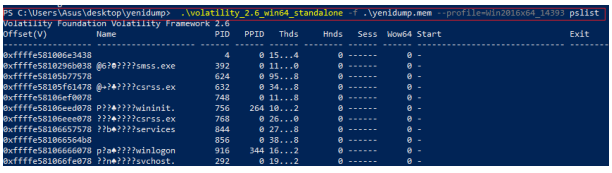
Volatility Framework dosyasına ulaşmak için [20] numaralı kaynaktaki bağlantı adresi kullanılabilir. Şekil 14 üzerinde gösterildiği gibi Ftk Imager uygulaması aracılığı ile Ram imajı ve daha önce belirtilen bağlantı yolu ile Volatility Framework dosyası elde edilerek yenidump isimli bir klasörün içine kopyalanmıştır. Elde edilen Ram imajı, Volatility Framework yardımı ile PowerShell üzerinde analiz etmeye hazır hale gelmiştir. Şekil 15'te, imaj dosyası olan yenidump.mem dosyası ve Volatility Framework dosyasının yolu gösterilmiştir. Burada –f ve imageinfo parametreleri kullanılarak geniş analizler için işletim sistemi sürüm bilgisi elde edilmiştir. Pslist parametresi ile işletim sistemi üzerinde çalışan sistem dosyalarının veya 3. parti uygulamaların tespiti gerçekleştirilir. Şekil 16 üzerinde Pslist ile görüntülenen uygulamaların bir kısmı gösterilmiştir.



Şekil 14. Ram imajının ve Volatility Framework gösterilmesi (Monitoring ram image and Volatility Framework file)



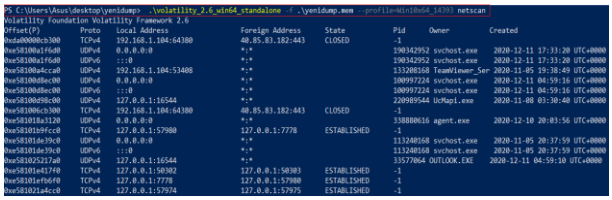
Şekil 15. PowerShell üzerinde ram imajının gösterilmesi (Showing ram image on PowerShell)



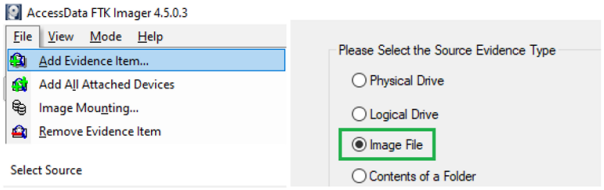
Şekil 16. Pslist parametresi ile çalışan servislerin gösterimi (Monitoring active services with pslist parameter)

Şekil 17 üzerindeki görselde kullanılan Netscan parametresi ile Windows sistem dosyalarının ve kullanıcıların başlattıkları üçüncü parti uygulamaların, Tcp ve Udp protokolleri aracılığı ile başlama ve sonlanma zaman bilgileri elde edilebilir. OSI referans modeli katman 4 üzerinde çalışan bu protokoller, verinin bir uçtan diğer bir uca ne şekilde gönderileceği ile ilişkilidir. Adli incelemelerde özellikle elektronik posta gönderim zamanı, sosyal medya uygulamalarının ve diğer çevrimiçi çalışma esnekliğine sahip uygulamaların başlangıç ve bitiş zaman bilgileri çok kıymetli verilerdir. NetScan parametresi ile elde edilen bu verilerin tek başına değerlendirilmeyip, Windows işletim sisteminin diğer bileşenleri üzerinde yapılan adli bilişim çalışmalarına doğrudan katkı sağlayacak olması unutmamalıdır. Burada dikkat edilmesi gereken nokta Utc+0000 zaman diliminin İstanbul konumuna göre 3 saat geride olmasıdır.

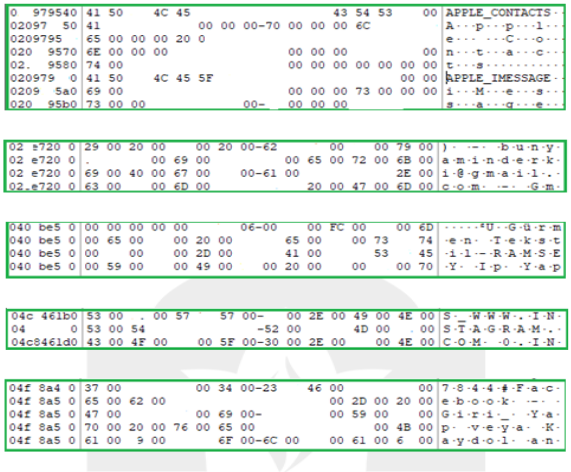
Adli bilişim incelemeleri sırasında mail bilgilerini, ziyaret edilen web sitelerini, özellikle sosyal medya hesapları üzerinde yaşanılan zorbalık girişimlerini tespit etmek mümkündür. Şekil 18 üzerinde Ftk Imager ile belirtilen yollar izlenip, ram imajı uygulamaya tanıtılır.



Şekil 17. Netscan ile tcp ve udp bağlantılarının görüntülenmesi (Monitoring tcp and udp connections via netscan)



Şekil 18. Ram imajının dosya yolu gösterimi (File path representation of ram image)

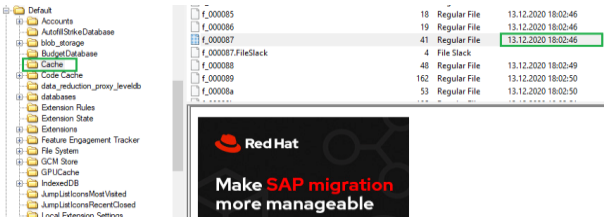


Şekil 19. Web site aktiviteleri (Web site activities)

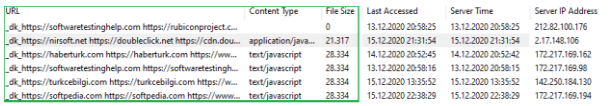
Görüntülenen ram imajı üzerinde canlı analiz yapıldığı için bilgi güvenliği nedeniyle heksadesimal kodların bir bölümü silinmiştir. Şekil 19'da, kullanıcı veya kullanıcılar tarafından ziyaret edilen sosyal medya hesapları, alışveriş siteleri, elektronik posta adresleri ve diğer web sayfaları birkaç örnek ile gösterilmiştir. Özellikle imaj üzerinde yapılacak aramalarda mail adreslerini bulmak elzemdir. Çünkü birçok noktada geçen aynı mail adresinin, tespit edilen sosyal medya hesapları ile ilişkilendirilmiş olması muhtemeldir.

3.3. Web Tarayıcı İncelemesi (Browser Examination)

Windows işletim sistemi üzerinde adli bilişim için incelemesi gerektiren bileşenlerden biri de web tarayıcılarıdır. Kullanıcıların internet üzerinde yaptığı birçok aktivite web tarayıcıları ile gerçekleşmektedir. Bu nedenle sistem üzerinde ki bu bileşen, delil incelemeleri açısından çok önemli bir yer tutmaktadır.



Şekil 20. Önbellek dosyasının görüntülenmesi (Displaying the cache file)



Şekil 21. Chrome cache view ile tarayıcı geçmişi görüntüleme (Viewing browser history with Chrome cache view)

Windows kayıt defteri üzerinde bulunan veri tabanında, web tarayıcılarına ait veriler de saklanmaktadır. Önbellek dosyası içerisinde saklanan verilere Ftk Imager ile erişmek mümkündür.

Örnek olarak en çok kullanılan tarayıcılardan olan Google Chrome'a ait veriler elde edilebilir. Bu amaçla; C:\user\[Operating System Username]\AppData \Local \Google\ Chrome\User Data\ Default\Cache dosya yolu izlenerek önbellek dosyasına ulaşılabilir.

Şekil 20' de, Ftk Imager ile Crome Web tarayıcısının önbellek dosya yolunu belirterek içerisinde bulunan dosyalara erişilmiştir.

Tarayıcı incelemelerinde farklı bir yol olarak üçüncü parti yazılımlarla da birçok önemli veriyi elde etmek mümkündür. CromeCacheView uygulaması bunlardan biridir.

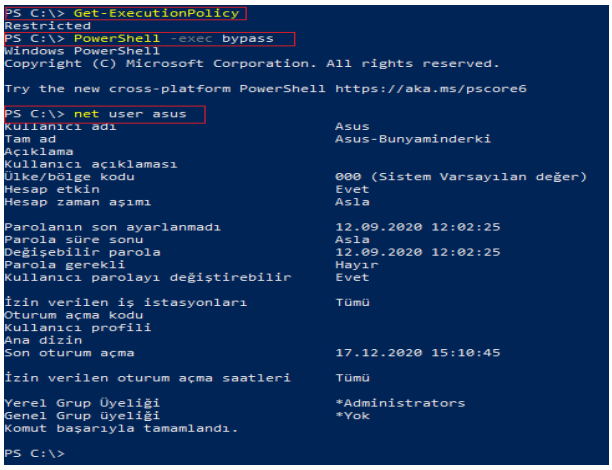
Şekil 21 üzerinde gösterildiği gibi farklı Web siteleri ve bu sitelerin üzerinde barındığı sunuculara en son erişilme zaman bilgileri gösterilmiştir. Ayrıca Web site verilerinin çekildiği sunucuların ip adres bilgileri de elde edilmiştir.

3.4. Windows İşletim Sistemi Üzerinde Canlı İncelemeler (Live Examination on the Windows Operating System)

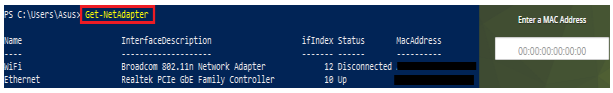
Olay yeri incelemeleri sırasında açık olan bilgisayar üzerinde o an bazı kritik verilerin elde edilmesi gerekebilir. Bu durumlar da Windows işletim sistemi doğal uygulamaları olan PowerShell ve komut satırı araçlarının kullanımı son derece önemlidir [21].

Şekil 22 üzerinde gösterildiği gibi Get-ExecutionPolicy komutu ile PowerShell üzerinde yetki seviyesi görüntülenmiştir. PowerShell – Exec bypass ile sınırlı yetki durumu kaldırılıp yazılan tüm komutların hata vermeden çalışması sağlanmıştır.

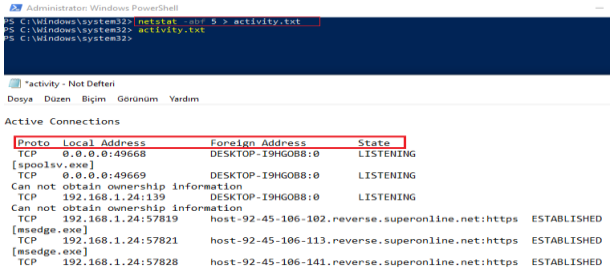
Net User [Kullanıcı İsmi] komutu yazıldığında belirtilen kullanıcı ile ilgili son oturum açma bilgisi, parola değiştirilme tarihi ve kullanıcının yetki seviyesi gibi önemli bilgiler elde edilir.



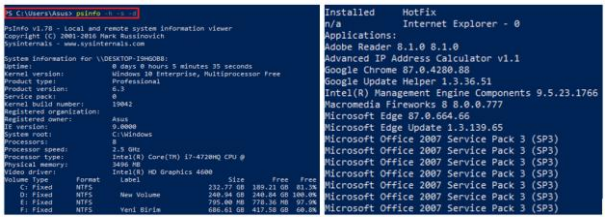
Şekil 22. Kullanıcı oturum bilgileri (User session information)



Şekil 23. Ağ bağdaştırıcılarının görüntülenmesi (Displaying network adapters)



Şekil 24. Activity.txt dosyasının gösterilmesi (Monitoring the activity.txt file)



Şekil 25. Sistem bilgileri ve üçüncü parti uygulamalar (System information and third party applications)

Bilgisayarlar, internet bağlantıları için ağ bağdaştırıcılarına ihtiyaç duyarlar. Genellikle bir bilgisayar üzerinde kablosuz ve kablolu olmak üzere iki ağ bağdaştırıcısı bulunur. Bu çoklu kullanımların en önemli nedeni Vmware ve Hyper-v gibi sanallaştırma uygulamaları üzerinde yapılan çalışmalarda ağ bağlantıları için farklı fiziksel ağ bağdaştırıcılarına ihtiyaç duyulmasıdır. İşletim sistemi üzerinde sanallaştırma uygulamalarının olduğu tespit edilmişse, mutlaka ağ bağdaştırıcılarını ve bunlara ait Mac adreslerini tespit etmek gerekir.

Şekil 23 üzerinde gösterildiği gibi PowerShell üzerinde Get-NetAdapter komutu ile ağ bağdaştırıcılar görüntülenmiştir. Ayrıca elde edilen Mac adresleri [22] numaralı kaynak üzerinden sorgulatıldığında, fiziksel olarak ağ bağdaştırıcısının bulunduğu bilgi işleme cihazı tespit edilebilmektedir.

Canlı analiz sırasında, incelenen bilgisayar üzerinde ağ ve internet bağlantı aktivitelerinin görüntülenmesi, daha önceden veya anlık olarak kurulan bağlantılar hakkında bilgi edinilmesini sağlayacaktır. Bu işlem için en çok kullanılan parametre Netstat komutudur. Özellikle kurulan ip bağlantıları, açık veya kapalı Port durumları hakkında bilgi edinmede son derece önemli bir komuttur. C:\Windows \System32\ konumunda bulunan Activity.txt dosyası içerisinde, kurulan ip bağlantıları saklanmaktadır.

Şekil 24'te gösterildiği gibi, netstat -abf 5 > activity.txt komutu ile activity.txt dosyasından veriler çekilir. Daha sonra Ctrl + C ile verilerin çekilme işlemi durdurulur. Bir alt satırda Activity.txt yazılarak çekilen veriler bu dosyanın içerisinde kullanıcıya gösterilir. Açılan dosyada, protokol tipi, yerel ip adresi ve bağlantı kurulan genel ip adres bilgileri görüntülenmiştir.

Şekil 25'te görüleceği üzere, sistem üzerinde Psinfo parametresi ile oturumun en son açılış zamanından itibaren geçen süre, disk kapasite bilgileri ve en önemlisi işletim sistemi üzerinde yüklü olan üçüncü parti uygulamaların görüntülenmesi sağlanabilir.

4. SONUÇ VE DEĞERLENDİRMELER
(CONCLUSION AND EVALUATIONS)

Bu çalışmada adli bilişim, adli bilişim süreçleri ve Windows işletim sistemi üzerinde anlamlı verilerden dijital delil elde edilme teknikleri üzerinde durulmuştur. Bu amaçla birçok sistem bileşeni incelenerek, yoğunluklu olarak delillerin nerelerde aranılmasına yönelik analizler yapılmıştır. Rastgele erişimli bellek ve kayıt defteri imaj dosyaları, canlı analizler yapılarak değerlendirilmiştir. Kayıt defteri incelemeleri sırasında, Sam ve sistem dosyası içerisinde ne tür verilerin saklandığına dair somut bilgiler paylaşılmıştır. Bazı imaj dosyaları üzerinde üçüncü parti yazılım kullanılmadan, Windows işletim sistemi doğal uygulaması olan PowerShell ile de bu incelemelerin yapılabileceği tespit edilmiştir. Böylelikle adli bilişim inceleme süreçlerinde daha hızlı ilerlemeler sağlanacaktır. Yapılan incelemelerle birlikte sadece işletim sistemi üzerindeki analizler sonucu birçok farklı dijital delile ulaşılabileceği görülmüştür.

Teknik olarak dijital delil elde etmek için Windows işletim sistemi üzerine sunulan bu çalışmanın alana katkı sağlayacağı değerlendirilmektedir. Dijital delillerin işletim sistemleri üzerinden sorunsuz ve bütünlüğünün korunarak elde edilmesi, yapılacak teknik çalışmalarla son derece bağlantılı hale gelmiştir. Bununla birlikte adli bilişim anabilim dalına katkı sağlamak ve bu alanda çalışanların teknik yetkinliklerinin geliştirilmesi amacıyla Linux sürümleri ve Mac OS üzerinde de

çalışmalar yapılabilir. Diğer yandan yapılacak benzer akademik çalışmalar ile adli bilişimin sadece bilgi güvenliği ve hukuksal farkındalıklardan ibaret olmadığı, aynı zamanda son derece teknik ve metodolojik çalışmaları da içerdiği daha fazla ortaya konulmuş olacaktır.

ETİK STANDARTLARIN BEYANI
(DECLARATION OF ETHICAL STANDARDS)

Bu makalenin yazarları çalışmalarında kullandıkları materyal ve yöntemlerin etik kurul izni ve/veya yasal-özel bir izin gerektirmediğini beyan ederler.

YAZARLARIN KATKILARI (AUTHORS' CONTRIBUTIONS)

Bünyamin ÖNEL: Teknik çalışmaları ve canlı uygulamaları gerçekleştirerek sonuçları analiz etmiştir.

Erdal IRMAK: Kavramsal inceleme ve teorik analizi gerçekleştirerek sonuçları değerlendirmiş ve yorumlamıştır.

ÇIKAR ÇATIŞMASI (CONFLICT OF INTEREST)

Bu çalışmada herhangi bir çıkar çatışması yoktur.

KAYNAKLAR (REFERENCES)

[1] ***https:// www.interpol.int/fr/content/download/14458/ file/Interpol%20Review%20Papers%202019tr***, "Interpol International Forensic Science", (2019).

[2] Ekmekçi A., Kuğu E., Temiztürk M., "Adli bilişim ezberlerini bozan bir düzlem: bulut bilişim", ***Uluslararası Bilgi Güvenliği Mühendisliği Dergisi,*** 2(1): 8–14, (2016).

[3] Çatalkaya H., Karaman M., Koca E., "Elektronik Kopyanın (Adli İmaj) Alınmasında Açık Kaynak Uygulamalarının Güvenirliği", ***Uluslararası Bilgi Güvenliği Mühendisliği Dergisi***, 1(2): 15–19, (2015).

[4] Başlar Y., "Elektronik Delilin Toplanması ve Muhafazası", ***Hacettepe Hukuk Fakültesi Dergisi***, 10 77–107, (2020).

[5] Kılıç M.S., Çakır H., "Bilişim Suçlarına İlişkin Elektronik Delil Elde Etme Yöntemlerine Genel Bir Bakış", ***Polis Bilimleri Dergisi***, 15(3): 23–44, (2013).

[6] Değirmenci O., "Adli Bilişimde Önceliklendirme(Triyaj) Yönteminin Ceza Muhakemisi Hukuku Açısından Değerlendirilmesi", ***Bilişim Hukuku Dergisi***, 2(1): 47–79, (2020).

[7] Bucak Y., "***Adli Bilişim ve Türk Ceza Muhakemesi Hukukunda Bilgisayarda Arama***", Yüksek Lisans Tezi: Üsküdar Üniversitesi Bağımlılık ve Adli Bilimler Enstitüsü, (2019).

[8] Özen M.,Özocak G., "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (Cmk M. 134)'', ***Ankara Barosu Dergisi***, 1(1): 52–55, (2015).

[9] Akarslan, H., "***Bilişim Suçları***", Seçkin Yayıncılık, Ankara, (2012).

[10] Say, K., "***Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvar da İncelenmesi***", Yüksek Lisans Tezi: Ankara Üniversitesi Sosyal Bilimler Enstitüsü, (2019).

[11] ***https://docs.Mic rosoft.Com/en-us/powershell/module/ microsoft.powershell.utility/get-filehash?view=power shel l-7.1*** "Get-FileHash (Microsoft.PowerShell.Utility)-PowerShell." (2020).

[12] ***https://www.Adlibilisimuzmani.com/elektronik- delille rin-paketlenmesi-tasinmasi-ve-muhafazasi*** "Elektronik Delillerin Paketlenmesi, Taşınması ve Muhafazası" (2020).

[13] Orta, M., "***Bilişim Suçlarında Adli Analiz***", Doktora Tezi: Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, (2015).

[14] ***https://www.thewindowsclub.com/clear-most-recently-used-mru-list*** "Clear Most Recently Used (MRU) Lists in Windows 10 Office" (2020).

[15] ***https://en.wikipedia.org/wiki/Hexadecimal***, "Hexadeci mal" (2020).

[16] ***https://www.top-password.com/blog /tag/win dows-sam-registry-file***, "Security Accounts Manager" (2020).

[17] ***https://docs.microsoft.com/en-us/previous-versions//cc 750583(v=technet.10)?redirectedfrom=MSDN***, "Inside the Registry" (2020).

[18] ***https://www.howtogeek.com/401365/what-is-the-ntuser .dat -file/#:~:text=DAT***, "What Is the NTUSER.DAT File in Windows?" (2020).

[19] ***https://en.wikipedia.org/wiki/Volatility_(me mory _for ensics)***, "Volatility (Memory Forensics)" (2020).

[20] ***https://www.volatilityfoundation.org/releases***, Volatility Framework" (2020).

[21] Kızılçınar, S ve Ciylan B., "Windows Sistemlerinde Post Exploitation İşlemleri İçin Bir Araç Geliştirilmesi", ***12. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı***, Ankara, 94-99, (2019).

[22] ***https://macvendors.com***, "Find Mac Address" (2020).