T.C.
İSTANBUL ÜNİVERSİTESİ
ADLİ TIP ENSTİTÜSÜ

Danışman
Doç. Dr. E. Hülya Yükseloğlu

BULUT DEPOLAMA UYGULAMALARINI KULLANAN BİLGİSAYARLARIN ADLİ BİLİŞİM AÇISINDAN İNCELENMESİ

FEN BİLİMLERİ ANABİLİM DALI
YÜKSEK LİSANS TEZİ

İSMAİL BARBAROS

İSTANBUL- 2016

İstanbul, 17 Mayıs 2016

İ.Ü.ADLİ TIP ENSTİTÜSÜ MÜDÜRLÜĞÜ
FEN BİLİMLERİ ANABİLİM DALI BAŞKANLIĞINA

Lisansüstü Öğretim Yönetmeliğinin 36.maddesi uyarınca Enstitünüz Fen Bilimleri Anabilim Dalı'nın yüksek lisans öğrencisi İsmail BARBAROS' un

"Olay Yerinde El Konulan Bilgisayarların Bulut Bilişim Uygulamaları Açısından Değerlendirilmesi ve Bulut Depolama Uygulamalarını Kullanan Bilgisayarların Adli İncelemesi"

Adlı tezi jürimizce tetkik edilmiş ve kendisine tez savunması yaptırılmıştır.

Yukarıda adı geçen tez başlığının **"Bulut Depolama Uygulamalarını Kullanan Bilgisayarların Adli Bilişim Açısından İncelenmesi"** şeklinde değiştirilerek, tezin ve tez savunmasının kabul edilmesine oy birliğiyle karar verilmiştir.

Prof. Dr. H. Bülent ÜNER
Jüri Başkanı

Doç. Dr. E. Hülya YÜKSELOĞLU
Danışman

Doç. Dr. İsmail ÇAKIR
Üye

Yrd. Doç. Dr. Hüseyin ÇAKAN
Üye

Yrd. Doç. Dr. Y. Tunç DEMİRCAN
Üye

TEŞEKKÜR

Tez çalışmamın başlangıcından itibaren bana her konuda destek veren, yol gösteren tez danışmanım Doç.Dr. E.Hülya YÜKSELOĞLU'na,

Fikirleri ve bilimsel katkılarıyla çalışmamın en başından beri yardımlarını esirgemeyen Dr.J.Albay Salih SALA'ya

Araştırmamın laboratuvar aşamalarında değerlendirme ve görüşleriyle bana destek olan, Tarık BASTAK ve Ayhan SONDOĞAN'a,

Değerli vaktini ayırarak tezimi değerlendiren tez değerlendirme jüri üyelerime,

Tezimin tamamlanmasına yardımcı olacak tüm idari faaliyetlerde bana her türlü kolaylığı sağlayan, her sorunumu çözmeye çalışan Anabilim Dalı Sekreteri Elvan EMRAL UĞUR ile öğrenci işlerinde görevli Mehmet SALDIRAN ve Sema SARIOĞLU ÜNAL'a,

Bu tezin oluşması için bana akademik ortamı yaratan ve beni adli bilimler alanında yetiştiren Jandarma Genel Komutanlığının ve Jandarma Kriminal Daire Başkanlığının güzide personeline ve değerli komutanlarıma,

Bu bilimsel alanda yetişmeme katkı sağlayan Ahmet Serhat ŞİRİKÇİ ve diğer tüm meslektaşlarıma teşekkür ederim.

Ayrıca bana her konuda destek olan ailemle, olumlu motivasyonu, hoşgörüsü ve anlayışıyla beni bir an olsun yalnız bırakmayan, sabır gösteren ve desteğini sürekli hissettiren sevgili eşim Bilge BARBAROS'a teşekkürü bir borç bilirim.

İÇİNDEKİLER

ŞEKİL LİSTESİ

TABLO LİSTESİ

ÖZET

Bulut adli bilişimi klasik anlamda anladığımız adli bilişimden bazı fiziksel ve teknik farklıları barındırmaktadır. Bulut hizmetlerin fiziksel ve teknik farklılıkları hukuksal alanda halen tam anlamıyla standardize edilememiş olan elektronik delil kavramına, elektronik delil toplama, delillerin mahkemede geçerliliğinin sağlanmasına ve bunların bilimsel yöntemlerle yerine getirilmesi konularına yeni bir boyut getirmiştir.

Bu çalışmanın amacı adli bilişimin yeni gelişen bir alt dalı olan bulut adli bilişimin kişisel kullanıcılar tarafından en çok kullanılan örneği olan bulut bilişim depolama hizmetlerini kullanan bilgisayarlarda adli bilişimde kullanılan inceleme yöntemleri kullanılarak ne gibi deliller elde edilebileceğini ortaya koymaktır.

Bulut bilişim hizmetleri internet üzerinde bilgisayara ait kaynak ve işlevlerin (veri depolama ve işleme gibi) çevrimiçi olarak istifade edildiği hizmetler olarak bilinmektedir. Çalışmamızda öncelikle bilişimin ne olduğu ve insan hayatını nasıl etkilediği daha sonra konunun hukuki boyutu olan bilişim sistemleriyle işlenebilecek suçlar anlatılmıştır. Olay yerlerinde bilişim sistemlerinden delil elde etme gerekliliğinin her geçen gün artması nedeniyle delil toplama sistematiği vurgulanmıştır.

Klasik adli bilişimde uygulanan yöntemlere değinilmiş ve teknolojinin dinamik yapısına ayak uydurabilmek için ilk defa karşılaşılan bir bulut depolama uygulamasının nasıl inceleneceği ile ilgili bir yöntem oluşturmaya çalışılmıştır. Bulut depolama uygulamalarını kullanan bilgisayarlarda olayı aydınlatmaya yönelik hangi delillerin elde edilebileceği örnek olarak sunulmuştur.

ANAHTAR KELİMELER

Bulut Bilişim, Bulut Bilişim Depolama Hizmetleri, Adli Bilişim, Bilgisayar.

ABSTRACT

The Cloud Computing has some physical and technical differences from the classic computer forensics. The physical and technical differences of cloud services has brought a new dimension to the concept of electronic evidence, collection of electronic evidence, providing the admisibility of evidence in court which aren't still standardised in law and fulling these by scientific methods.

The aim of this study is to reveal that what kind of evidence can be obtained from computers which use the Cloud Storage Services which is the most used example by individual users of cloud computing which is the newly-emerging sub-branch of computer forensics by using survey methods which are used in computer forensics.

The Services of Cloud Computing is known as the services which are virtualised source and functions (like data storage and data processing) belong to computer by being online on internet. First of all, it is told that what is computing and how it affects human's life and then it is told that the crimes that can be commited by computing systems which is the legal dimension of subject in our study. The systematic of collecting evidence is emphasized because the necessity of obtaining evidence from computing systems in crime scenes increases day by day.

The methods and ways applied in classic computer forensics have been mentioned and a method has been mapped out about how to examine a Cloud Storage Service encountered for the first time to keep up the dynamic structure of technology-whichever evidence can be obtained which is intended to enlighten the crime in computers which use the Cloud Storage Services is presented as an example.

KEYWORDS

Cloud Computing, Cloud Storage Services, Computer Forensics, Computer.

1. GİRİŞ VE AMAÇ

Modern dünyada insanın içinde bulunduğu her türlü eylemin gelişen teknolojik ürünlerle birlikte şekil değiştirdiğine şahit olmaktayız. Alışveriş yapmak için elektronik ticaret sitelerini, haberleşme için elektronik posta veya anlık mesajlaşma/görüntülü konuşma uygulamalarını kullanmaktayız. Büyükşehirlerde iş yaşamının hızlı döngüsü içerisinde sosyalleşmek ve arkadaşlarımızla irtibat halinde olmak için sosyal medya uygulamalarına ihtiyaç duymaktayız (1),(2).

Teknolojinin bu kadar hayatımıza girmesi ile birlikte suç ve suçlulukla mücadelede de yeni alanlar ortaya çıkmıştır. Adi suçlardan tutun da cinayet, hırsızlık gibi kolluk kuvvetlerini ve yargı mercilerini meşgul eden suç türleri de elektronik veya sanal ortama taşınmış durumdadır. Klasik suçlar olarak tanımlanan bu suçların bilgisayarlar aracılığıyla işlenmesinin yanında teknolojinin kendine has yarattığı yeni suç tipleriyle mücadele gerekliliği de doğmuştur (3).

Farklı bilimsel disiplinlerin bir araya gelerek suç ve suçlulukla mücadele etmek üzere oluşturdukları yeni bir bilim dalı olan adli bilimlerin çatısı altında kendine yer bulan en yeni disiplinlerden birisi de "Adli Bilişim" olup, kısaca adli mercilerin karar vermelerine yardımcı olmak maksadıyla bilişim sistemlerinden elektronik delil etme ve bunları mahkemelere sunma süreci olarak tanımlanabilmektedir(5),(6).

Adli Bilişim sürekli bir yenilik içerisinde olan teknoloji dünyası karşısında dinamik bir yapıya sahiptir. Bu sebeple her an yeni geliştirilen bir yazılım, donanım veya sistemle suç işlenebilmektedir. Ya da mevcut yazılım, donanım veya sistemlerin versiyonları ortaya çıkabilmekte önceden uyguladığımız delil elde etme prosedürleri değişikliğe uğrayabilmektedir.

Bulut Bilişim (Cloud Computing) bilgi çağının ulaştığı son seviyeyi göstermesi bakımından daha şimdiden günümüz ve geleceğin dünyasını şekillendirmeye başlamıştır. Yaşanan hızlı değişim büyük ölçekli yapılardan (şirketler, servis sağlayıcılar, hükümetler vb.) kişisel kullanıcılara kadar herkesi kapsamaktadır(7). Bu nedenle gelişmeleri takip etmek ve başlayan değişime ayak uydurabilmek kolluk kuvvetleri ve adli merciler açısından önem arz

etmektedir. İnsanın içinde olduğu her şeyin değiştiği günümüzde teknoloji açısından bakıldığında adalet ve yargı sistemleri de doğrudan etkilenmektedir.

Bulut Bilişim hizmetlerinin yaygınlaşmaya başlaması ile birlikte, tüm sektörlerin (kanun koyucular, kolluk kuvvetleri, iş dünyası vb.) bir uyum süresine ihtiyacı bulunmaktadır. Bulut bilişimin yarattığı etkilerin sonuçları görüldükçe kanun koyucuların yasal düzenlemeleri süratle yapması, kolluk kuvvetlerinin yeni suç önleme ve suç araştırması stratejileri geliştirmesi, adli bilişim uzmanlarının standart uygulamalarla birlikte gerekirse bu hizmetlerin doğasına uygun yeni adli bilişim programları geliştirmesine ihtiyaç duyulabilecektir.

Bu tez çalışmasının amacı bulut bilişim depolama uygulamalarını kullanan bilgisayarlarda klasik adli bilişim yöntemleri ile hangi verilere ulaşılabileceğinin test edilmesi, bulut bilişim sistemlerine uygun adli bilişim yöntemleri, yazılım ve donanımlarının geliştirilmesi için geçecek sürede adli bilişim uzmanlarına kaynak oluşturacak bir yöntem ortaya koymaktır. Bu kapsamda bulut bilişim depolama uygulamaları kullanılarak işlenebilecek bir suçun soruşturulmasında el konulan bilgisayarlar üzerinde ne tür deliller elde edilebileceği, bulut depolama alanı ve içeriğindeki dosyalarla bu bilgisayarların ilişkisinin ortaya konulup konulamayacağı incelenecektir.

2. GENEL BİLGİLER

2.1 Bilişimle İlgili Kavramlar

2.1.1 Bilişim ve Bilişim Sistemleri

Bilişim Kavramı; Türkiye'de ilk kez Prof. Dr. Aydın Köksal tarafından kullanılmıştır (8). Köksal 1970 yılında "bilişim" terimini "bilmek" eyleminden ad olarak türetmiş ve 1971 yılında kurucu üyesi olduğu Türkiye Bilişim Derneğinin isminde de bu terimi kullandıklarını belirtmiştir (8),(9).

Türk Dil Kurumuna göre bilişim, "*İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik*" olarak tanımlanmaktadır (10).

Akarslan'da Tavukçuoğlu'nun "Bilişim Terimleri Sözlüğünde" aynı şekilde yukarıdaki tanımı kullandığını ve *"bilgi olgusunu, bilgi saklama, erişim dizgileri, bilginin işlenmesi, aktarılması ve kullanılması yöntemlerini, toplum ve insanlık yararı gözeterek inceleyen uygulamalı bilim dalıdır. Disiplinler arası özellikler taşıyan bir öğretim ve hizmet kesimi olan bilişim bilgisayarı da kapsayarak bilişim ve bilgi erişim dizgelerinde kullanılan her türlü araçların tasarlanması, geliştirilmesi ve üretilmesiyle ilgili konuları da kapsadığını"* aktarmıştır (11).

Bilgisayar ve bilgisayar ağlarını anlatan bilişim bu alandaki en üst kavramdır. Bilişimin temelini bilgisayar ve benzeri elektronik makineler oluşturur. Bilgisayar en basit şekliyle "girdi", "süreç", ve "çıktı" işlemlerini gerçekleştiren bir yapıya sahiptir. Bilgisayarların birbirleriyle iletişim kuracak şekilde bağlanmasıyla ağ bağlantısı (network) meydana gelmektedir. Dünya çapındaki en büyük ağ bağlantısı ise internettir (12).

Bir veya birden fazla üniteden oluşan ve belirli bir sonuca ulaşmak için işbirliği sistemiyle çalışan ve güvenlik araçlarıyla da korunan bütüne ise "**Bilişim Sistemi**" denmektedir (13).

2.1.2 Bilişim Sistemlerinin gelişimi

Bilişim sistemlerinin geliştirilmesinin temelinde hızlı ve kolay yoldan hesap yapabilme ihtiyacı yatmaktadır. Bu ihtiyacın neticesinde geliştirilen bir çok alt sistemin zamanla bir

araya getirilmesiyle insan beynin yapamayacağı karmaşıklıktaki hesaplamaları yapan makineler geliştirilmiştir. Bu makineler sanılanın aksine tek bir bilim insanın ortaya çıkardığı buluşlar şeklinde olmamıştır. Genellikle bir amaç için bir araya gelmiş proje grupları ya da bilim insanları tarafından zaman içerisinde geliştirilen alt sistemlerin tuğla bir duvar örmeye benzetebileceğimiz şekilde birbiri üzerine eklenmesiyle bu makineler oluşturulmuşlardır (14).

Amerikan ordusunun topçu atışlarının hesaplanmasında kullanılan ENIAC (Electronic Numerical Integrator and Calculator) elektronik devrelere sahip ilk bilgisayar olarak kayıtlara geçmiştir (14). Alan Turing ise İkinci Dünya Savaşı sırasında Almanların şifreli haberleşme cihazı ENIGMA'nın şifrelerini kırmak için "Bombe" adı verilen elektromekanik bir makine geliştirerek şifreleri hızlı bir biçimde kırmaya yardımcı olmuştur (15).

İlk bilgisayarlar ana merkezden bilgi alışverişi yapıyordu daha sonra aynı anda iki bilgisayarın ana merkezle iletişim halinde olabilmesi için geliştirilen iletişim protokolleri ile ağ kavramı ortaya çıktı. İhtiyaçların artmasıyla birlikte dosya aktarım protokolü (File Transfer Protocol-FTP) ve aktarım denetim protokolünün geliştirilmesiyle çok sayıda kullanıcı ana bilgisayara (sunucu) bağlanabilir hale geldi (16).

Günümüzde bu protokollerin geliştirilmesi sonucu küresel olarak bilgisayarların birbirine bağlanabildiği ağa ise internet denmektedir. Amerika Birleşik Devletleri Soğuk Savaş sırasında Sovyetlerin uzay yarışında öne geçmeleri üzerine uzay teknolojileri alanında ileri çalışmalar yapmak amacıyla İleri Araştırma Projeleri Ajansını (Advanced Research Project Agency-ARPA) kurmuştur. Bu ajansın ana görevi olan Sovyetlerin teknolojik üstünlüğünü yenmenin yanısıra uzay araştırmaları, balistik füze savunması gibi görevleri de bulunmaktaydı. O günlerde bilgisayarların aynı anda sisteme girişi desteklememesi araştırmaların uzamasına neden oluyordu. Bu çalışmalarda görev alan bilim insanlarını tek bir ağda toplayarak birbirleriyle iletişim halinde olmaları fikrinden İleri Araştırma Projeleri Ajansı Ağı (Advanced Research Project Agency Network-ARPANET) kuruldu (16).

İnternetin atası olarak tabir edilen ARPANET'in temel görevi Sovyetlerin olası bir nükleer saldırısında haberleşmenin kesilmemesinin sağlanması ve bilim insanlarının birbirleriyle iletişiminin devamını sağlamaktı. Önceleri askeri amaçlarla kullanılan bu ağ daha sonra üniversitelerin kullanımına açılmıştır. 1989 yılında "*world wide web"* teknolojisinin ve 1990

yılında en temel dosya transfer protokolü olan "*http*" protokolünün geliştirilmesiyle ARPANET yerini bildiğimiz anlamda internete bırakmıştır (14).

İnternetin gelişmesine paralel olarak bilgisayarların taşınabilir hale gelmesi, cep telefonlarının mini bilgisayar özelliği kazanması sayesinde bugün artık gelinen noktada kullanıcılar verilerine internet bağlantısı olan her yerden bilgisayarlarıyla veya mobil cihazlarıyla erişebilmektedir.

2.1.3 **Bulut Bilişim** (Cloud Computing)

Bulut şekli bugüne kadar şematik çizimlerde interneti tanımlamak için kullanılmış ve onun belirli bir şekle sahip olmadığını tasvir etmiştir. Günümüzde ise artık bulut; bilgisayara ait tüm işlevlerin (bilgisayar sabit diskleri, sunucular, yazılımlar vb.) kendi bilgisayarımızda değilde sanal ortamda bulunması ve bunların internet ağı aracılığıyla istenilen yer ve zamanda kullanılmasını anlatmaktadır.

Bulut bilişimde işlemci, veri depolama vb. bilgisayar kaynaklarının elektrik, su, telefon hizmetini büyük merkezlerden satın almak gibi açıklayabiliriz (17).

Bulut bilişim en basit tanımıyla bilgisayara ait tüm hizmetlerin internet üzerinden sağlanması olarak açıklanabilir, ancak bu tanım elmanın yarısıdır. Diğer yarısı ise bu sanal bilgisayar hizmetlerine internet aracılığıyla farklı noktalardan ulaşılmasıdır. Yani ofisimizde hazırladığımız bir belgeyi eve geldiğimizde düzenlemeye devam edebilir, iş arkadaşlarımızla paylaşıma açabilir ve böylece izin verdiğimiz takdirde onlarında düzenlemesine değiştirmesine olanak tanıyabiliriz. İnternet üzerinde depoladığımız tüm dosyalarımıza herhangi bir yere bağlı kalmadan erişebiliriz (18).

Teknolojik gelişmeler bugüne kadar bilişim kaynaklarını dev terminallerin yer aldığı merkezi noktalardan mini bilgisayarlara hatta kişisel bilgisayarlara doğru uzaklaştırma eğilimindeyken, bugün daha ucuz ve güçlü işlemciler ile daha hızlı ve her yerde bulunan ağların bir araya gelmesiyle oluşturulan büyük veri merkezleri bilişim dünyasını tekrar merkezileştirmektedir (1).

Bulut bilişimin genel kabul görmüş bir tanımı bulunmamaktadır (17). Akademik çalışmaların çoğunda en geniş kabul gören ve Amerikan Teknoloji ve Standartlar Enstitüsünün (National Institute of Standards and Technology-NIST) yaptığı tanımlamaya göre: "Bulut Bilişim çok az yönetim çabası ve servis sağlayıcı etkileşimi olan çabuk kiralanıp bırakılabilen ayarlanabilir bilişim kaynaklarının (ağlar, sunucular, veri depolama alanı, uygulamalar ve hizmetler vb.) bulunduğu bir havuza istenilen anda uygun ağ bağlantısı sağlanan bir modeldir." (19)

2.1.3.1 Bulut Bilişimin Karakteristik Özellikleri

Her ne kadar ortak bir tanım üzerinde fikir birliği oluşmamış olsada en geniş kabul gören bu tanımlamaya göre bulut bilişimin beş karakteristik özelliği bulunmaktadır (17), (19).

- *İsteğe bağlı kendin kullan servis (On demand self-service);* Bir tüketicinin bilgisayar hizmetlerini tek taraflı olarak servis sağlayıcılarla etkileşime ihtiyaç duymadan istediği anda otomatik olarak temin edebilmesidir. Otomatik satış makinesine benzeyen bu özellikte satış temsilcisi olmadan müşteriler istediği yiyecek veya içeceklerden hangilerinin mevcut olduğunu ve ücretlerini camlı bölmeden görerek tercihleri doğrultusunda satın alabilmektedir. Bulut bilişimde son kullanıcılar bir arayüz sayesinde hangi hizmetin sunulduğunu ve ücretini görerek tercih ettikleri hizmeti kullanabilmektedirler (20).

- *Geniş ağ erişimi (Broad network access);* Hizmetlerin ağ üzerinden standart mekanizmalar ile farklı platformlardan (ör. Mobil cihazlar, tablet bilgisayarlar, dizüstü bilgisayarlar ve iş istasyonları) kullanılabilmesidir. Tüm hizmetlere internet erişimi olan her yerden ulaşılarak zamana ve mekana bağlılık azalmaktadır. Aslında bu özellik iş yerindeki sisteminize her yerden ulaşabilmekle sınırlı değildir. Farklı işletim sistemlerini, internet tarayıcıları (Firefox, Internet Explorer, Chrome, Safari) ve platformları kullanabilmeye olanak sağlamaktadır. Çünkü Bulut Bilişim tek bir sisteme veya firmaya bağlı değildir (21).

- *Kaynak havuzu (Resource pooling);* Servis sağlayıcının bilgisayar kaynaklarının bir havuzda toplanıp birden fazla tüketiciye hizmet edecek şekilde onların talepleri doğrultusunda farklı fiziksel ve sanal kaynakların dinamik olarak tahsis edilerek kiralanmasıdır. Hizmetlerin kesintisiz sürmesi için kaynakların talep eden tüketiciye sunularak talepte bulunulmadığında boşta kalmasının önüne geçilmektedir. Örneğin otoyollar

ve servis araçları gibi hizmetler herkesin kullanımına açıktır ve ücretleri ödendiğinde kullanılabilmektedir. Herkese ait servis aracı olmadığı gibi kendimize ait bir yolumuzda yoktur. Bu mantıktan hareketle herkese ayrı kaynak ayırmaktansa mevuct kaynakları istenilen zamanda kiralamak bunların atıl kalmasının önüne geçmektedir (22).

- *Hızlı esneklik/elastikiyet (Rapid elasticity);* Tüketicinin hizmetleri istenilen her anda otomatik olarak kullanabilmesi ve bunu sanki sınırsız kaynak kullanıyormuş gibi yapabilmesidir. Kullanılmayan kaynaklar diğer tüketicilerin kullanımına açık olduğu için tıkanmalar yaşanmadan hizmet verilmektedir. Spor salonunda mevcut aletleri istediğimiz zaman kullanabiliriz, kullanılmadığı zaman tüm aletler spor yapmak için gelen diğer herkese açıktır, istediğimiz anda diğer aletleri kullanabilmemiz esnek kullanım ile mümkün hale gelmektedir (23).

- *Ölçeklenebilir hizmet (Measured service);* Bulut sistemler servis tipine göre otomatik olarak kaynak kullanımını kontrol ve optimize edebilen ölçüm yeteneklerine sahiptir. Böylece kullanım miktarına göre ödeme yapılmakta ve ihtiyaçlara cevap veren en az kaynak kullanımı sağlanmaktadır. Kontörle çalışan telefonlara benzetebileceğimiz bu özellikle kullanım miktarımıza göre (süre veya kota) ödeme yapılabilmektedir (24).

2.1.3.2 Bulut Bilişim Servis Modelleri

Bulut bilişimde en yaygın kullanılan hizmet veri depolama alanı olsa da sunulan farklı seviyelerdeki hizmetleri tanımlamak için servis modelleri kullanılmaktadır. Servis modelleri hizmet gruplarına göre üç kategoride ele alınmaktadır.

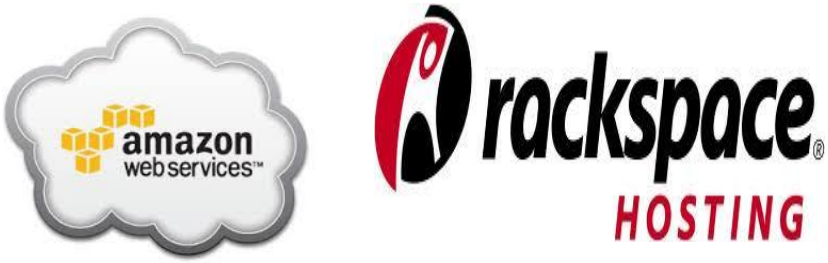
- *Servis Olarak Yazılım (Software as a Service, SaaS)*; Tüketicilerin herhangi bir program kurulumuna ihtiyaç duymadan internet tarayıcıları sayesinde yazılım üreticilerinin bulut bilişim altyapısını destekleyen programlarına erişimine olanak sağlayan hizmeti tanımlamaktadır (25). Bu sayede örnek olarak internet tabanlı elektronik posta hizmetlerini verebiliriz. Tüketiciler hizmetin geri planındaki depolama aygıtları, sunucular ve işletim sistemi gibi öğeleri denetleyememekte ve değişiklik yapamamaktadırlar (26), (27).

Şekil 1: Servis olarak Yazılım Örnekleri

- *Servis olarak Platform (Platform as a Services, PaaS)* Tüketici servis sağlayıcının sunduğu alanda kendi uygulamasını geliştirebilmekte ve kurup çalıştırabilmektedir. Bu platform tüketicinin uygulaması ile birlikte kullanacağı servisleri ve gerekli teknolojik altyapıyı da (programlama dilleri, kütüphaneler ve diğer servisler) içermektedir. Tüketici sadece kendi uygulaması üzerinde değişiklik yapabilmekte, bunun dışındaki platform altyapısını oluşturan bileşenler üzerinde herhangi bir kontrol ve yönetim yetkisi bulunmamaktadır (25),(26),(27).

Şekil 2: Servis olarak Platform Örnekleri

- *Servis olarak Altyapı (Infrastructure as a Service, IaaS)* Altyapının bir bulut servisi olarak sunulması modelinde müşteri ihtiyacı olan işlemci, depolama, ağ kaynağı ve diğer temel bilişim kaynaklarını kendisi yapılandırabilmekte ve bunların üzerine ihtiyacı olan işletim sistemi ve uygulamaları kurabilmektedir (25),(26).



Şekil 3: Servis olarak Altyapı Örnekleri

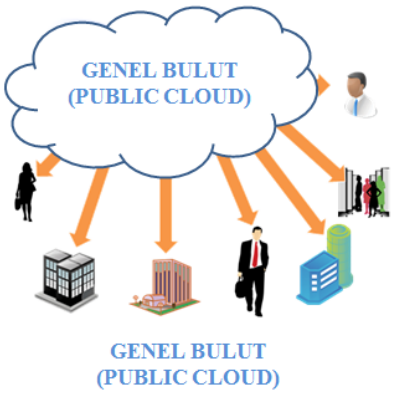
Bu üç hizmet modeli temel hizmetleri tanımlamaktadır. Veri depolama hizmeti artık başlı başına bir hizmet alanı haline geldiğinden Servis Hizmeti Olarak Altyapı (IaaS) olarak sınıflandırmanın yanında bazı kaynaklarda Servis Hizmet Olarak Depolama (Storage as a Service- StaaS) gibi isimlendirmelere de ratlanılmaktadır (28).

Önümüzdeki dönemde bu hizmetlerden adli bilim/bilişim uzmanlarının yararlanması da olası görünmektedir. Servis sağlayıcılarının kolluk kuvvetlerine sağlayacağı bir hizmetle Forensic as a Servis (Servis Hizmeti Olarak Adli Bilişim) hizmeti suç soruşturmalarında özellikle bilişim suçlarında büyük oranda destek sağlayabilecektir (29).

2.1.3.3 Yerleştirme Modelleri

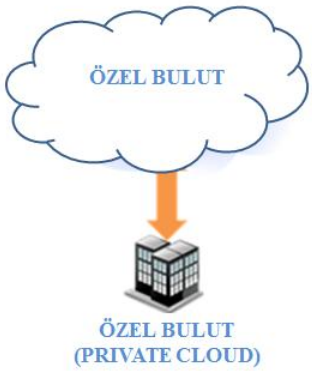
Yukarıda saydığımız bulut hizmetlerinin bir veya birkaçının birleştirilmesiyle hizmet modelleri oluşturulabilmektedir. Kullanıcıların ihtiyaçlarına göre çeşitli yerleştirme modelleri bulunmaktadır. Yerleştirme modelleri hizmetin kullanılma biçimlerine göre sınıflandırılmaktadır (7).

a. Genel Bulut (Public Cloud): Bulut altyapısının herkese ya da büyük endüstri grubuna açık olduğu yapıdır. Servisi veren yazılım, veri depolama (data storage) gibi kaynakları sağlar ve internet üzerinden halkın erişimine açıktır (7).



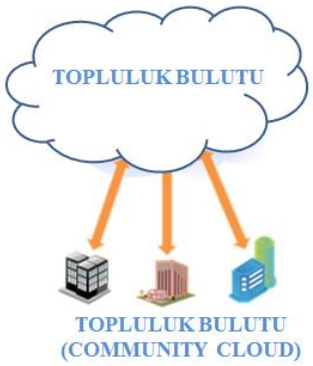
Şekil 4: Genel Bulut

b. Özel Bulut (Private Cloud): Bir kurum ya da firmanın kendi oluşturduğu ya da kiraladığı buluttur. Bulut altyapısı yalnızca firma için çalışmakta, firmanın kendisi tarafından ya da bir servis sağlayıcı tarafından yönetilmektedir (7), (30).



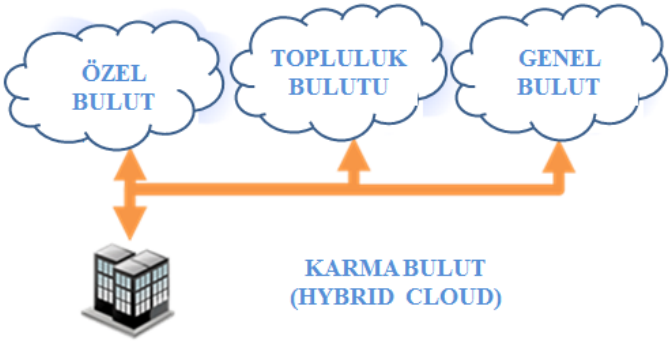
Şekil 5: Özel Bulut

c. Topluluk Bulutu (Community Cloud): Özel buluta benzemekle birlikte, topluluk bulutu belirli bir iş kolunun (sağlık, medya, özel sektör) ortak amaçlarına, ihtiyaçlarına ve güvenlik gereksinimlerine yönelik olarak düzenlenmiş buluttur. Bulut altyapısı birkaç organizasyon ya da firma tarafından paylaşılır, böylece aynı tarzda idare edilen organizasyonlar firmalar desteklenir (7), (30).



Şekil 6: Topluluk Bulutu

d. Karma Bulut (Hybrid Cloud): İki veya daha fazla bulut modelinin kompozisyonudur. Bulutlar kendi özelliklerini kaybetmeden yazılımın ve verinin taşınmasına izin verecek şekilde standardize edilmiş ya da özel teknoloji ile bağlanmıştır (7), (30).



Şekil 7: Karma Bulut

Bilişim ve buna bağlı sistemler bilginin en önemli güç olduğu günümüz toplumunda hayatın her alanında kendine yer bulmaktadır. Geride bıraktığımız yüzyıl bu sistemlerin keşfini sağlamış olsa da asıl etkiyi bilgi toplumu olma yolunda bilişim sistemlerinin yaygınlaşması sağlamıştır. Ekonomik ve ticari hayat, sosyal yaşam, kamu düzeni, eğitim ve hukuk sistemlerinin bu kavramlar çerçevresinde yeni bir düzene geçmeye başladıkları görülmektedir.

2.2 Bilişim Suçları ve Bilişim Sistemlerinin Suçun Aydınlatılmasında Kullanımı

İnsanlar arasındaki mesafeleri kaldırıp, iletişim ve sosyal yaşamı farklılaştıran bilişim sistemleri aynı zamanda öngörülmeyen sorunlara da sebep olabilmektedir (16).

Dünyanın farklı yerlerindeki insanların birbirleriyle iletişim kurabilmesinin yanında, bu insanlar birbirlerine karşı hukuki sorunlara yol açabilecek eylemlerde de bulunabilmektedirler. Bu sebeple klasik olay yeri, fail ve mağduru aynı zaman ve mekana bağlı olarak birbirine ilişkilendirmede yeni bir boyut kazanmıştır. Suç eylemlerinin bilişim alanında veya bilişim sistemleriyle işlenmesi ise bilişim suçu kavramını ortaya çıkarmıştır (31).

Temelinde bilgisayarı barındıran ama bilgisayar ağları ve interneti de içine alan bu sanal dünyada yaşanan hukuki problemleri günümüz hukuk normları ile ele almak bazı güçlükler yaratmaktadır. Örneğin Çin'de bulunan bir suçlunun internet protokol adresini (Internet Protocol Address- IP Address) gizleyerek Hollanda üzerinden Almanya'daki bir kişiye gönderdiği elektronik posta (e-posta) ile bu kişinin bilgisayarındaki verileri şifreleyerek fidye istemesi durumunda hangi ülkenin ceza yasalarını uygulayacağımız ya da hangi ülkede delil

toplayacağımıza karar vermek güç olmaktadır. Ya da Hindistan'daki bilgisayarından çocuk pornografisi içeren video ve resimleri Rusya'daki bir servis sağlayıcının sunucu (server) bilgisayarı aracılığıyla tüm dünyada farklı ülkelerdeki kişilerle paylaşan bir kişinin eyleminde suç yerinin tespitinde zorluklar bulunmaktadır.

İnternetin getirdiği imkanlardan dolayı bilişim suçlarının yerel nitelikte olması düşünülmemekte sınıraşan bir kavram olarak bu suçlarla mücadelede uluslararası işbirliği ve koordinasyon ön plana çıkmaktadır (32).

Devletlerin gizli kalmasını bekledikleri bilgileri içerden veya dışardan elde eden kişilerin bunları açıklamaları uluslararası ilişkileri ciddi anlamda etkileyecek boyutlara ulaşmıştır. Ayrıca kişisel verilerin, mali kayıtlar ve kredi kartı bilgilerini barındıran veritabanlarının kamu veya özel kurumlardan ele geçirilmesi de telafisi mümkün olmayan maddi veya manevi zararlara sebep olabilmektedir. Son dönemde yaşanan Wikileaks Skandalı[1], Panama'daki bir hukuk bürosundan gizli belgelerin sızdırılması[2] ve Türkiye'deki bazı vatandaşların kimlik bilgilerinin çalınması[3] olayları karşı karşıya olunan durumun ciddiyetini ortaya koymaktadır.

Devletler bir yandan iç hukuk sistemlerinde kanun koyucular ve kamu düzenini sağlamakla görevli kurumlar aracılığıyla bu alanda yaşanan sorunlara çözüm getirmek amacıyla yeni suç tanımları, suç önleme stratejileri ve cezai yaptırımları hukuk sistemlerine entegre etmeye çalışmakta diğer yandan uluslararası alanda işbirliğini geliştirmektedirler (33).

Bu kısımda öncelikle uluslararası alanda bilişim suçlarıyla mücadelede uluslararası örgütlerin başını çektiği işbirliği çalışmaları daha sonrasında ise mevzuatımızda yapılan düzenlemelerin neler olduğu incelenecektir.

Uluslararası örgütlerin konuya yaklaşımına bakıldığında;

Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun Mayıs 1983'teki Paris Toplantısı'nda "*bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir*

[1] http://www.bbc.com/news/technology-10757263 [Erişim Tarihi : 01.05.2016]
[2] http://www.bbc.com/turkce/haberler/2016/04/160406_panama_belgeleri_siber_saldiri [Erişim Tarihi : 01.05.2016]
[3] http://www.bbc.com/turkce/haberler/2016/04/160404_50_milyon_veri_turkiye [Erişim Tarihi : 01.05.2016]

sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış" **bilişim suçu** olarak tanımlanmıştır (34).

Birleşmiş Milletlerin 10'uncu kongresinde bilişim suçları ve bilgisayar ağlarıyla ilgili suçları konu alan bir çalıştayda bilişim suçları, dar ve geniş anlamda olmak üzere iki kategoride ele alınmıştır (35).

a. **Dar anlamda bilişim suçları (Bilgisayar Suçları):** Bilişim sisteminin doğrudan kendisini ilgilendiren güvenliğini veya işlediği veriyi hedef alan kanun dışı eylemler **dar anlamda**,

b. **Geniş anlamda bilişim suçları (Bilgisayarla İlişkili Suçlar):** Klasik suç eylemlerinin işlenirken bilişim sistemlerinin (bilgisayar sistemleri ve ağları) kullanılması ise **geniş anlamda bilişim suçlarına** örnek olduğu belirtilmiştir (35)(2),(36).

Bilişim alanında yaygınlaşan suçlarla mücadele kapsamında devletlerin ortaya koydukları iradenin bir ürünü de Avrupa Konseyi Siber Suç Sözleşmesidir (Convention on Cybercrime). Bilişim dünyasının sınır tanımayan yapısı devletlerin ulusal güvenliklerini tehdit eden gelişmelerin ve siber saldırıların artması, uluslararası suçluların yakalanması konusunda ortaya çıkan yardımlaşma ihtiyacı ve ortak bir ceza politikası oluşturma çabaları sözleşmenin çıkış kaynağını oluşturmaktadır (36).

Avrupa Siber Suçlar Sözleşmesine göre tanımı yapılan suç eylemleri:

a. Bilgisayar verileri ve sistemlerinin gizliliği, bütünlüğü ve kullanılabilirliği (erişilebilirliği) ile ilgili suçlar;

(1) **Yetkisiz Erişim** (Madde 2)
(2) **Yasadışı Dinleme** (Madde 3)
(3) **Verilere Müdahale** (Madde 4)
(4) **Sisteme Müdahale** (Madde 5)
(5) **Cihazların Kötüye Kullanımı** (Madde 6)

b. Bilgisayarla ilişkili suçlar;

(1) **Bilgisayarla ilgili dolandırıcılık suçları** (Madde 7)

(2) **Bilgisayarla ilgili sahtecilik suçları** (Madde 8)

c. İçerikle ilişkili suçlar

(1) **Çocuk pornografisiyle ilişkili suçlar** (Madde 9)

ç. Telif hakları ve bununla bağlantılı konulara ilişkin suçlar

(1) **Telif hakları ve bununla bağlantılı konulara ilişkin suçlar** (Madde 10) (37).

Sözleşmenin 3'üncü Bölümünde yukarıda sayılan suçlarla ilgili uluslararası işbirliğinin nasıl uygulanacağı açıklanmaktadır. Bu kapsamda taraflar sözleşme hükümleri çerçevesinde birbiriyle yardımlaşma içerisinde olacaklarını taahhüt etmektedirler (36). Ülkelerin işbirliğini sağlayabilmesi için mevzuatlarının uyumlu olması gerekmektedir. Suç konusu eylem işbirliği talep edilen ülkede suç değilse işbirliği yapılamamaktadır (12).

Görüldüğü üzere uluslararası örgütler bilişim suçları kavramını gelecekte ortaya çıkabilecek ihtiyaçlara da cevap verebilmesi maksadıyla genel olarak tanımlamaya çalışmışlardır.

Ülkemizde ise bilişim suçlarıyla mücadeleye ilişkin mevzuata bakıldığında ilk düzenlemenin 765 sayılı Türk Ceza Kanununda (TCK) "Bilişim Alanında Suçlar" başlığı altında yapıldığı görülmektedir. 1995 yılında 5846 sayılı Fikir ve Sanat Eserleri Kanununda (FSEK) 4110 sayılı yasayla yapılan değişiklik sonucu bilgisayar programlarına karşı yapılan eylemler ile 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanununda elektronik imzaların sahte olarak üretilmesi suç sayılmıştır. 01 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı TCK'da "Bilişim Alanında Suçlar" başlığı altında bilişim suçları tanımlanmıştır. Ayrıca yasanın başka maddelerinde de bazı suçların bilişim sistemleriyle işlenmesi suçun nitelikli hali olarak yaptırıma bağlanmıştır (34).

5237 sayılı Türk Ceza Kanuna baktığımızda;

a. Sadece bilişim sisteminin kullanılmasıyla işlenebilen suçlar (doğrudan ya da dar anlamda veyahut gerçek bilişim suçları) "Bilişim Alanında Suçlar" başlığı altında toplanmıştır.

(1) **Bilişim sistemine girme** (Madde 243)

(2) **Sistemi engelleme, bozma, verileri yok etme veya değiştirme** (Madde 244)

(3) **Banka veya kredi kartlarının kötüye kullanılması** (Madde 245)

(4) **Tüzel kişiler hakkında güvenlik tedbiri** (Madde 246) (4).

b. Bir bilişim sisteminin kullanılması mecbur olmamakla birlikte, bazı suçların nitelikli hali olanlar;

(1) **Hırsızlık** (TCK md. 142/2-e) ,

(2) **Dolandırıcılık** (TCK md. 158/1-f), (4)

c. Yine bir bilişim sisteminin kullanılması zorunlu olmamakla birlikte söz konusu sistemin suçta vasıta olabileceği suçlar ise;

(1) **Haberleşmenin Gizliliğini İhlal** (TCK md. 132),

(2) **Haberleşmenin Engellenmesi** (TCK md. 124),

(3) **Eğitim ve Öğretimin Engellenmesi** (TCK md. 112),

(4) **Kamu Kurumu veya Kamu Kurumu Niteliğindeki Meslek Kuruluşlarının Faaliyetlerinin Engellenmesi** (TCK md. 113),

(5) **Hakaret ve Sövme** (TCK md. 125),

(6) **Müstehcenlik** (TCK md. 226),

(7) **Kumar Oynanması İçin Yer ve İmkân Sağlanması** (TCK md. 228),

(8) **Suç İşlemeye Tahrik** (TCK md. 214),

(9) **Cinsel Taciz** (TCK md. 105) gibi suçlardır (4).

5846 sayılı Fikir ve Sanat Eserleri Kanununda 07.06.1995 yılında 4110 sayılı kanun ile yapılan değişiklikle bilgisayar programları eser kapsamına alınmış ve bu alandaki oluşabilecek ihlaller yaptırıma bağlanmıştır. Bu kanuna göre;

(1) **Mali, Manevi ve Bağlantılı Haklara Tecavüz Suçları** (Madde 71)

(2) **Koruyucu Programları Etkisiz Kılmaya Yönelik Hazırlık Hareketleri** (Madde72)

tanımlanmış ve suç sayılmıştır. Bu kapsamda bir eserin hak sahibinin izni olmadan elektronik ortamlarda paylaşılması ve dağıtılması 71'inci maddeyle, bilgisayar programlarının veya bir

eserin bulunduğu medyayı kopyalamaya karşı koruyan yazılımları etkisiz hale getirme eylemleri ise 72'nci madde ile suç kapsamına almıştır (38).

Elektronik ortamda saklanan ve iletilen bilgilerin güvenilirliğinin sağlanması açısından en önemli kimlik doğrulama aracı olan elektonik imza ile ilgili olarak 5070 sayılı Elektronik İmza Kanununda;

(1) **İmza Oluşturma Verilerinin İzinsiz Kullanımı** (Madde 16)

(2) **Elektronik Sertifikalarda Sahtekârlık** (Madde 17)

suç olarak tanımlanmıştır (38).

Günümüzde bilişim sistemleri hayatımızın her alanına girmiş durumdadır. Herkesin çoğunlukla kullandığı bir cep telefonu bulunmakla birlikte bilgisayarlar başta olmak üzere her türlü bilişim sistemi gündelik işlerimizde rutin olarak kullandığımız cihazlar olmuşlardır. Bu sebeple kolluk personeli suç işlemek için kullanılmış olmasa bile bilgisayarlar, cep telefonları vb. cihazlardan yararlanarak çeşitli olayları aydınlatmaya çalışmaktadır. Suçla mücadelede olduğu kadar diğer adli, idari ve mali sorunların çözümünde, olay yerinin yeniden canlandırılmasında bilişim tekonolojilerinden faydalanılmaktadır. Eskiden bir intihar olgusunda olay yerinde intihar mektubu aranırken şimdi bilgisayarında internette "kolay ölüm şekilleri" veya "acısız intihar yöntemleri" gibi kelimeleri aratıp aratmadığı, sosyal medya paylaşımları ve cep telefonundan yaptığı yazışmaları ön plana çıkmaktadır. İş yerinden hırsızlık, kavga, trafik kazaları gibi olaylarda ise güvenlik kameralarından azami istifade edilmektedir. Burada bahsedilen sistemlerinde dolaylı olarak bilişim sistemleri olması suçun kolaylaştırıcısı olarak kullanılmasa bile titizlikle ele alınarak, delil elde etme prosedürlerine göre müdahale edilmelerini zorunlu kılmaktadır.

2.3 Olay Yeri İncelemesi

Suç kastının eyleme dönüştüğü yerden başlayıp failin izlediği yollar ile neticenin gerçekleştiği yere kadar olan alanlar olay yeri kavramının içindedir. Olay yeri fail ve mağdurun bağlantısını ortaya koyan, olayın oluş şeklini anlamamıza yardım eden ve maddi delillerin tespit edilebileceği en önemli yerdir. Olay yeri sınırları çok keskin bir alan olmayabilmektedir. Olayın türüne göre boyutu ve sayısı çeşitlilik gösterebilmektedir (39). Bilişim suçları, insan ticareti ve uyuşturucu ticareti gibi coğrafi uzaklıkların fazla olduğu farklı yargı yetkisine sahip

yerlerde de başlayıp bitebilmektedir. Edmond Locard'ın "Her Temas İz Bırakır." prensibi çerçevesinde suç soruşturmasının olay yerinde başladığı kabul edilmektedir (32), (39).

Meydana gelmiş bir adli olayın aydınlatılması maksadıyla suçun işleniş şeklini anlamamıza yardımcı olacak şekilde ve fail, mağdur ile olay yeri arasındaki bağı ortaya koyabilecek tüm bulguların bilimsel ve teknik usullerle araştırılması sonucunda delil niteliği taşıyabilecek olanlarının toplanması, kayıt altına alınması ve incelenmek üzere kriminal laboratuvarlara gönderilmesi olay yeri incelemesinin esasını oluşturmaktadır. İnsan haklarına saygı fikrinden hareketle ilkel delil elde etme yöntemleri yerine olayların soruşturulmasında bilimsel ve sistematik olarak elde edilecek delillerle faile ulaşmak olay yeri incelemesinin ana gayesidir(39),(40).

Olay yerinde sorumluluğu olan görevlileri ilk müdahale ekibi (emniyet ve asayişle görevli kolluk personeli), soruşturma sorumlusu (cumhuriyet savcısı), olay yeri inceleme uzmanları, itfaiye ve sağlık personeli vb. olarak gruplandırmak mümkündür (40). Listeye olayın türüne göre başka görevlilerde dahil olabilmektedir.

Bir suç soruşturması olayın haber alınmasıyla başlar. Olaya ilk müdahale genellikle suçun önlenmesi amacıyla kolluk personeli veya hayati tehlikeye maruz kalmış kişilere yardım eden sağlık personeli, itfaiye vb. tarafından yapılmaktadır. Olay yerine ulaşan kolluk personelinin öncelikli görevi suçun işlenmesinin önüne geçmektir. Daha sonra olay yerlerini tespit etmek ve suçun oluş şekli ve faili tespite yönelik işlemler gerçekleştirmektir. Maddi gerçeğin ortaya çıkarılması ve failin suçluluğunu kanıtlayacak masum kişilerin ise suçsuzluğunu ortaya koyacak delillerin toplanması için belirlenmiş ve genel kabul görmüş kurallar sistematik olarak uygulanmalıdır(39).

Olayın haber alınmasından sonra olayın cinsine göre genellikle bölgeye en yakın genel kolluk görevlileri veya sağlık personeli vb. ulaşır. Bu personel aşağıdaki adımları izleyerek olay yerine müdahale eder.

a. Olayla ilgili ilk bilgileri (haber alındığı zamanı, olay yerine ulaşılma zamanı vb.) not etmek
b. Olay yerine ulaşılmasıyla birlikte devam eden suç eylemi varsa bunu engellemek,

c. Olay yerinde hayati tehlikeye maruz kalan kişilere yardım etmek/edilmesi için sağlık görevlilerine haber vermek,
d. Devam eden tehlike durumu mevcutsa (yangın, patlayıcı madde vb.) ilgili birimlere haber vererek müdahale edimesini sağlamak,
e. Bölgenin güvenliğini sağlamak, delillerin kaybolmasını veya bozulmasını önlemek için tedbir almak,
f. Soruşturma sorumlusu ve olay yeri inceleme birimlerine yardımcı olmak ve çalışmalarını kolaylaştırmak için gerekli diğer tedbirleri almak.

İlk ekibin genel olarak yapması gereken bu faaliyetler olayın durumuna göre şekillenmektedir (39),(41).

İlk ekibin müdahalesinden sonra soruşturma sorumlusu (Cumhuriyet savcısı veya adli kolluk personeli) ile olay yeri inceleme uzmanlarının olay yerini değerlendirme ve delil toplama aşamasına geçilir. Bu aşamada;

a. Olay yerine ilk ulaşan ekiple görüşülerek ilk bilgiler alınır.
b. Alınmış olan güvenlik tedbirleri yeniden değerlendirilerek olayın türüne göre gerekirse genişletilir birden fazla olay yeri mevcutsa yeni bölgeler güvenlik bölgesine dahil edilir.
c. Delil niteliği taşıyan bulgular tespit edilir, bozulmamaları için gerekli önlemler alınır. Deliller numaralandırılır.
d. Deliller usulüne uygun olarak sistematik bir şekilde toplanır. Bu esnada gözle görülmeyen delilleri (parmakizi, vücut sıvıları, elektronik deliller vb.) toplamak için gerekli tedbirler alınır.
e. Toplanacak deliller öncelikle bulundukları ilk durumda daha sonra olay yerinin genel perspektifi içindeki konumunu belirtecek şekilde ve son olarakta ölçekli fotoğraflanmalıdır.
f. Numaralandırılmış deliller kayıt altına alınarak delil teslim zincirine dahil edilir. Delil teslim zincirinin ilk halkası delili toplayan olay yeri inceleme uzmanlarıdır. Delil teslim zinciri bir delilin olay yerinden mahkemeye kadar geçecek süre içerisinde takip edilebilmesi açısından önemlidir.
g. Kayıtları tamamlanan deliller bozulmaya en yatkın olandan başlanarak bir sistematik dahilinde toplanır.

h. Her delil kendine has şekilde paketlenir. Kriminal laboratuvarlara gönderilmesi sürecinde zarar görmemesi ve bozulmaması için genellikle özel olarak üretilmiş (Biyolojik deliller kağıt veya karton paketlerde, elektronik deliller antistatik torbalara konulduktan sonra uygun ebattaki karton kutularda vb.) delil paketlerine konulur.
i. Deliller en seri yoldan incelenmek üzere kriminal laboratuvarlara gönderilir.

Olay yeri incelemesinde delil toplanmasıyla ilgili maddelerin ön plana çıktığı bu safhada Olay Yeri İnceleme Uzmanlarının olay yeri krokisinin çizilmesi, olay yerinin ayrıntılı fotoğraflanması, video çekimi yapılması ve yapılan işlemlerin belirten olay yeri inceleme raporu (tutanak) hazırlanması vb. görevleri de bulunmaktadır (39).

Her olay yeri kendine has özelliklere sahiptir. Ayrıca olayın veya suçun türüne göre elde edilecek delillerde çeşitlilik göstermekte çeşitli nesneler olayın aydınlatılmasına katkı sağlamaktadır. Olay çeşitliliğinin artması beraberinde delil çeşitliliğini de getirmiştir. Artık kolluk personeli olayın çözümünde ve suçluya ulaşmada teknolojinin getirdiği yeniliklerden de faydalanmaktadır. Olay yerini gören bir güvenlik kamerası, ya da mağdurun cep telefonu kayıtları çok değerli birer delil kaynağı haline gelmiştir. Ayrıca klasik anlamda işlenen suçların yanında bilişim sistemleriyle işlenen suçlarda eklenmiştir. Bu tür olaylarda toplanan bu tür fiziksel delillerin içeriğinde suçu aydınlatmaya yönelik elektronik delillerde mevcuttur (42).

2.3.1 Elektronik Delil Kavramı

Bilişim sistemlerinin tanımı yapılırken verileri işleme ve gönderme özelliğine sahip cihazlar olduğundan bahsedilmişti. **Veri**; Avrupa Konseyi Siber Suç Sözleşmesinde "*Bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan yazılımlar da dahil olmak üzere, bir bilgisayar sisteminde işlenmeye uygun nitelikteki her türlü bilgi*"; 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un tanımlar başlıklı 2'nci maddesinde de; "*bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer*" olarak tanımlanmıştır (14). Buradaki veri kavramı aslında bilgisayarın temelini oluşturan 1'ler ve 0'lara dayanmaktadır.

1948 yılında Dr. Claude Shannon tarafından matametik formüllerinin bağlantı süreçlerini ikili kod (binary code) olarak başlıklandırılmasından beri bilgisayar ve elektronik hesaplamalar bu

yöntemle yapılmaktadır. Bilgisayardaki ikili sayma sistemi (0) ve (1) rakamlarına dayanır. Bilgisayarda bir program çalıştırıldığında bilgisayar işlmcisi aslında bu programı (0)'lar ve (1)'lerin çevirisi olarak okur. Bu rakamlardan herhangi birisine "bit" denilmektedir. 8 "bit"in biraraya gelerek en küçük anlamlı veri olan "byte" oluşmaktadır. Bilgisayardaki elektronik yapılarda, sıfırlar ve birlerin elektronik bir oluşumudur (12).

Serbest elektron hareketlerini konu edinen ve eksi yüklü elektronların hareketlerinden faydalanarak donanım yapma bilimine "elektronik" denilmektedir. Radyo, televizyon, bilgisayar gibi pek çok cihaz bu bilim sayesinde geliştirilmiştir. "Dijital" ise ingilizce sayısal anlamına gelen "digital" kelimesinin dilimize yerleşmiş şeklidir. Elektronik bilimi; analog (örneksel) ve dijital (sayısal) olarak ikiye ayrılmaktadır. Analog temelli devrelerde sinyal değeri her an farklıdır ve sonsuz ara değer oluşabilmektedir. Dijital (sayısal) devrelerde ise elektrik akımının ya geçmesi (1 ile ifade edilir.) ya da geçmemesi durumu (0 ile ifade edilir) söz konusudur. Buradan da anlaşılacağı üzere elektronik kavramı dijital (sayısal) yapıyı da içine alacak şekilde daha geniş bir kavramdır. Bu sebeple bilişim sistemlerinden elde edilen delillere elektronik deliller denmesi daha doğru bir tanımlama olacaktır (12).

Elektronik bir cihazda depolanan, oluşturulan veya bu cihaz vasıtasıyla taşınan, iletilen, soruşturma ve kovuşturma açısından hukuki bir değer taşıyan verilere "Elektronik Delil" denilmektedir (43). Elektronik deliller yapısı gereği insanın duyu organları ile tespit edilecek ve yorumlanabilecek formda değildirler. Bu veriler bilgi işleme özelliğine sahip elektronik cihazlar tarafından oluşturulduklarından muhakeme esnasında yine böyle bir cihaz tarafından duyu organlarımızla algılanabilecek bir hale getirilmelidirler. Burada önemli husus, klasik delillerden farklı olarak soyut bir yapıya sahip olan elektronik delillerin, delil niteliğini haiz olan formu/durumu bilginin bilgisayar ekranındaki görüntüsü değil, elektronik ortamdaki bilginin kendisidir (44). Bilgisayar ekranındaki görüntü aslında bizim yorumlayabilmemize olanak sağlayan kullanıcı arayüzüdür.

Duyu organlarımızla algılayamadığımız ve tespit edemediğimiz elektronik delilleri daha iyi anlamak açısından özelliklerine bakarsak, elektronik dellilller;

a. *Görünmez yapıdadır*; DNA veya bazı yüzeylerdeki parmakizleri gibi gözle görülebilir yapıda değildirler.

b. *Yargı yetkisi sınırlarının dışına kolaylıkla ve çabucak çıkabilen yapısıyla sınıraşan bir yapıdadır;*
c. *Kolaylıkla değiştirilebilir, zarar görebilir veya yok edilebilir;*
d. *Zamana duyarlı olabilmektedir* (42).

Bazı deliller zamana bağlı olarak sistem tarafından otomatik olarak silinebilmektedir. Örneğin internet geçmişi kayıtları belli bir zaman aralığında kayıt tutmaya ayarlanmış ise bu sürenin sonunda eski kayıtlar ya silinecek ya da üzerine yeni kayıtlar yazılarak ulaşılamaz hale gelebilecektir (7).

Elektronik delil içeren tüm fiziksel deliller dikkatle müdahale edilmesi gereken hassas yapıdadırlar. Bu deliller toplanırken öncelikle fiziksel olarak bozulmasını engelleyecek gerekli tedbirler alınır. Diğer aşamada ise delil toplama prosedürlerine uygun olarak toplanır ve elektronik delilleri tespite yönelik oluşturulmuş yöntemler uygulanarak delil elde edilir (31).

Elektronik delillerin bozulmadan ve değişikliğe uğramamış şekilde toplanması mahkemede ispat değeri kazanması açısından önemlidir. Mahkemelerde delil değerini koruyabilmesi için elektronik delilin;

a. *Gerçeklik* (Authenticity): Araştırılan suçla ilişkili ve orijinal olması,
b. *Güvenilirlik* (Reliability): Delilin elde edilmesinde güvenilir prosedürlerin kullanılması,
c. *Tamlık* (Completeness): Delil suçluluğu da suçsuzluğu da kanıtlayabilmeli,
d. *İnanılırlık* (Believable): Mahkeme tarafından inanılabilir ve anlaşılabilir olmalı,
e. *Kabul olunabilir* (Acceptable)*:* Yasal yollardan elde edilmiş olması,

gerekmektedir (17).

2.3.2 Elektronik Deliller Bakımından Olay Yerlerinin Değerlendirilmesi

İster bilişim suçlarının ister diğer adli olayların (cinayet, cinsel taciz, kayıp şahıs, trafik kazası, uyuşturucu ticareti vb.) çözümünde yardımcı delil olarak toplansın elektronik deliller her türlü soruşturmada kolluk kuvvetleri, savcılar ve mahkemelere olayın çözümünde ve olayın yeniden canlandırılmasında yardımcı olmaktadır. Bilişim sistemleri ile oluşturulan veri ve kayıtlar olayın ne zaman meydana geldiği, kurban veya failin kim olduğu birbiriyle nasıl

bağlantılı oldukları, kimlerle irtibatta oldukları ve hatta failin suç işleme saikinin ne olduğunu dahi ortaya çıkarabilecek çok değerli bilgileri içermektedir (32).

Bir suç soruşturmasında olay yerinde elektronik delil edebilmek için öncelikle elektronik veri depolamaya müsait fiziksel deliller toplanmalıdır. Elektronik veri içerebilecek fiziksel deliller bilgisayarlar, cep telefonları, tablet bilgisayarlar, hafıza kartları, taşınabilir bellekler, fotoğraf makinaları, yazıcılar vb. örnek verilebilir. Bu cihazların her birinden elde edilebilecek deliller olay türüne göre çeşitlilik göstermektedir.

Bilgisayarlar ve içerisindeki sabit disklerden, taşınabilir diskler, taşınabilir bellekler, optik medyaların Yoğun Disk (Compact Disc-CD), Çok Amaçlı Sayısal Disk (Digital Versatile Disc-DVD) içerisinden;

- Çeşitli belgeler, resimler, ses ve görüntü dosyaları,
- İnternet geçmişi,
- E-posta ve sohbet bilgileri,
- Silinmiş dosyalar ve silinmiş disk alanları,
- Şifrelenmiş dosyalar,
- Dosya türleri ve tarih bilgileri (oluşturma, erişim, değiştirme, silme tarih bilgileri vb),
- Sistem kayıt bilgileri (Registry, Event Log vs),
- Kötü amaçla hazırlanmış zararlı yazılımlar (Truva atı, bot-net, keylogger vs.),
- Sanal disk alanları,
- Korsan yazılım, film ve müzik dosyaları,
- Optik medyaların oluşturulma tarihi.

Veri yedekleme birimleri içerisinden;

- Veri tabanı dosyaları yedekleri,
- E-posta sunucu dosyaları yedekleri,
- Sistem kayıtlarının yedekleri.

Modeline göre değişiklik göstermekle birlikte cep telefonları içerisinden;

- Adres ve telefon bilgileri,

- Kişisel bilgiler,
- Ajanda kayıtları ve notlar,
- Mesaj bilgileri, Silinmiş Mesajlar (Gelen,Giden),
- Son arama listesi (Cevapsız, arayan, aranan),
- Kablosuz Uygulama Protokolü (Wireless Application Protocol-WAP), Genel Paket Radyo Servisi (General Packet Radio Service-GPRS) geçmişi, internet erişim kaydı,
- Resim, görüntü ve ses kayıtları,
- Kablosuz erişim noktaları,
- Uluslararası Mobil Cihaz Kodu (International Mobile Equipment Identity-IMEI) numarası.

SIM kartlar içerisinden;

- Entegre Devre Kartı Kimliği (Integrated Circuit Card Identifier-ICCID) ve Uluslararası Mobil Kullanıcı Kimliği (International Mobile Subscriber Identity-IMSI) numaraları,
- Rehber bilgileri,
- Arama kayıtları,
- Mevcut ve silinmiş kısa mesajlar (Short Message Service-SMS).

Hafıza kartları içerisinden;

- Çeşitli belgeler, resimler, ses ve görüntü dosyaları,
- Şifrelenmiş dosyalar,
- Silinmiş dosyalar ile disk alanları,
- Dosya türleri ve tarih bilgileri (oluşturma, erişim, değiştirme, silme),
- Rehber bilgileri ve mesajlar (Cep telefonu içerisinden çıkarılmışsa tespit edilebilir).

El bilgisayarları (tablet) içerisinden;

- Çeşitli belgeler, resimler, ses ve video dosyaları,
- Elektronik posta ve sohbet kayıtları,
- İnternet geçmişi kayıtları,
- Erişim şifreleri ve kullanıcı adları,
- Silinmiş dosyalar ve silinmiş disk alanları,
- Şifrelenmiş dosyalar,

- Dosya yetkileri ve tarihleri (oluşturma, erişim, silme vb.),
- Sistem kayıt bilgileri (Registry, Event Log vb.),
- Zararlı yazılımlar (Truva atı, keylogger vb.),
- Sistem üzerinde yüklü yazılımlar,
- Adres ve telefon bilgileri,
- Ajanda kayıtları ve yapılacaklar listesi,
- Kısa mesaj (SMS) kayıtları,
- GPRS ve Küresel Konumlama Sistemi (Global Positioning System-GPS) erişim kayıtları.

GPS cihazları içerisinden;

- Koordinat bilgileri,
- Kayıtlı rota bilgileri,
- İşaretli yerleşim noktaları,
- İzlenen güzergâh bilgileri.

Manyetik kart kopyalama cihazları içerisinden;

- Cihazın şifresi,
- Cihaz içerisinde kayıtlı diğer veriler.

Yazıcı ve faks cihazları içerisinden de çeşitli bilgiler tespit edilebilmektedir. Elde edilebilecek bilgiler cihazın marka ve modeline göre değişiklik gösterebilmektedir. Genel olarak;

- Yazıcılar üzerinde son yazdırılan belgeler ile yazım tarih ve adetleri,
- Faks cihazlarında ise son gönderilen ve alınan belgenin kopyası,
- Gönderim ve alım tarihleri, kaç adet gönderim ile kaç adet alım yapıldığı ve kayıtlı kullanıcılar tespit edilebilmektedir.

Network Cihazları içerisinden;

- Ağdaki kullanıcı bilgileri,
- Ağ yapılandırma bilgisi,

- Erişim ve yönlendirme bilgileri,
- Erişim denetim listeleri,
- Cihazların fiziksel adresleri [Ortam erişim kontrolü adresi (Media access control address-MAC Address)],

Dijital kameralar ve fotoğraf makineleri içerisinden;

- Görüntü (video, resim) ve ses kayıtları,
- Cihazın tarih ve saat ayarları,
- Silinmiş veriler.

Tespit edilebilmektedir (6)(41),(42),(43). Her olay ve suçta aranacak deliller değişiklik göstermektedir. Ayrıca yukarıda örnek olarak sayılan cihazlardan elde edilebilecek delillerin yanısıra internet ve ağ bağlantısı olan cihazların bulut bilişim hizmetlerini kullanması yönünden de değerlendirmek gerekir. Bilgisayarlara ait her kaynağı internet bağlantısı üzerinden sunması sebebiyle bulut bilişim uygulamalarının bulunduğu bilgisayarların ağ geçmişi ya da ağ tarayıcısı önbelleğinde yer alan bilgilerden de delil elde edilebilmektedir. Bu bilgiler; dosya ismi, ilgili bulut kullanıcı ismi, dosyanın oluşturulduğu zaman, dosyanın son güncellendiği zaman, bulut adresi(cloud path), dosyanın kapasitesi ve algoritma imzası olabilecektir (44).

Olay yerinden delil toplanırken mutlaka yapılan her işlem kayıt altına alınmalıdır. Bu kayıt işlemi delil teslim zincirine göre delile ilk müdahaleden başlar, delile nasıl el konulduğunu, değişmemesi ve bozulmaması için ne gibi önlemler alındığını, elekronik delilin birebir kopyalanması esnasında hangi donanımlar ve yazılımlar kullanıldığını içermelidir. Kayıtların bir zaman çizelgesine uygun olarak tutulması geriye dönük olarak yapılan tüm işlemlerin takibini kolaylaştıracağı gibi raporlama aşamasına da katkı sağlayacaktır (45).

Olay yerine ulaşan olay yeri inceleme uzmanlarının elektronik delilleri toplama konusunda yetkinliği yoksa bu delilleri toplamak için ya adli bilişim uzmanlarının olay yerine davet edilmesi gerekir ya da sadece fiziksel olarak delillere el konulması gerekir. Hem elektronik delillerin toplanması hem de elektronik delil içeren her türlü delilin fiziksel olarak toplanması gerektiği durumlarda her ikisi içinde uygulanması gereken bir takım prosedürler bulunmaktadır.

2.4 Olay Yerlerinde Bulunan Bilişim Sistemlerine Müdahale Edilmesi

Bilişim alanındaki olay yeri kavramına bakıldığında ya bilişim suçlarının işlendiği olay yerleri ya da diğer olayların meydana geldiği olay yerlerinde bulunan bilişim delilleri aklımıza gelmektedir. Her iki durumda da bu delillere müdahale edecek uzmanların bu konuda eğitim almış olması ve bilgili olması gerekmektedir.

Elektronik delillerin hassas yapıda olması sebebiyle bunların tespit edilmesi ve toplanması için oluşturulmuş "İyi Uygulama Rehberlerine" bağlı kalınarak işlemler yapılmalıdır (42). Aksi takdirde delilin kaybına veya istemeden bile olsa tahrifine neden olunabilmektedir (44).

İlk aşamada klasik olay yeri incelemesinde yapılacak tüm uygulamalar titizlikle uygulanır. Olay yerinin değerlendirmesi yapılır ve gereken önlemler alınır.

a. Fiziksel delil toplanırken öncelikle olay yerinde bulunan kişiler elektronik delil ihtiva edebilecek tüm cihaz ve medyalardan uzaklaştırılmalı, kimsenin bu cihazlara müdahale etmesine izin verilmemeli,
b. Olay yerindeki tüm elektronik cihazlar ve veri depolama medyaları (taşınabilir olanlar dahil) tespit edilmeli, bu cihazların bulundukları durumun (bilgisayar açıksa kapanmaması vs.) değişmemesi için tedbir alınmalı,
c. Bilgisayar ekranı açıksa kapatılmaz herhangi bir tuşa basmadan (klavye ve mouse ile işlem yapılmaması dahil) varsa ekran görüntüsü fotoğraflanmalı,
d. Kablo bağlantıları, güç kaynakları tespit edilmeli bağlantılar fotoğraflanmalı ve bu bağlantılar etiketlenmeli,
e. Olay yerinde sadece faillerin/şüphelilerin bulunmayabileceğinden hareketle olay yerinde bulunan kişilerle mülakat yapılarak elde edilebilecek tüm bilgiler (bilgisayar adları, açılış parolaları, kullanıcı adları, otomatik çalışan uygulamalar, e-posta adresleri, internet bağlantı türü, uzak depolama hizmeti bulunup bulunmadığı gibi) toplanmaya çalışılmalıdır (42).

Bu aşamadan sonra delilleri toplama aşamasına geçilir. Kendine has özellikleri olan elektronik delillerin de faklı yöntemlerle toplanması, incelenmesi ve bir sonuç çıkarılması kaçınılmazdır. Sistematik olay yeri incelemelerinin bilimsel yöntemlerle icra edilmesinin bir

sonucu olarak elektronik delillerin toplanması ile ilgili bir takım usuller ve "İyi Uygulama Rehberleri" oluşturulmuştur. Bir sonraki aşamada ise bu rehberlerin standardize edilmeleri gerekliliği tartışılmaya başlanmıştır.

Olay yeri incelemelerinde delil toplama standardı için Uluslararası Standartlar Teşkilâtının (International Organization for Standardization-ISO) ISO/IEC 17020 standardı günümüzde genel kabul görmektedir. Ülkemizde bu standarda göre akredite edilmiş bir kurum veya olay yeri inceleme birimi bulunmamaktadır. Jandarma Kriminal Daire Başkanlığı ile TÜRKAK bu standart kapsamında Jandarma Olay Yeri İnceleme Timlerini akredite etmeyi planlamaktadır.

Bilişim delilleri için ise ISO/IEC27037 standarına göre delil toplama, saklama işlemleri uygulanmalıdır. Elektronik delile müdahale eden veya toplamakla görevlendirilen tüm birimlerin bu standarda ve gerekliliklerine göre hareket etmesi uygun olacaktır.

Çünkü toplanacak delillerin mahkemelerce yargılamaya etki edebilmesi için bu delillerin ve toplanma yöntemlerinin bilimsel olarak açıklanabilir ve genel kabul edilebilir olması gerekmektedir. Bu hususta 1923 yılındaki Frye v. United States davası ve 1993 yılındaki Daubert v. Merrell Dow Pharmaceuticals davaları Anglo-Amerikan hukukunun yargısal içtihatları açısından önemli bir kilometre taşıdır (44),(46).

Frye davasını hukuk literatürüne sokan olay James Frye'ın işlediği öne sürülen bir cinayet davasında girdiği yalan makinesi testi sonucunun Frye'ın suçsuz olduğunu göstermesine rağmen mahkeme tarafından testin yargılamaya dahil edilmemiş olması ve kararın temyiz yeri olan üst derece mahkemesinin delillerin bilimselliği konusunda vermiş olduğu içtihattır. Bu içtihat hem yalan makinesi testinin hem de bilirkişilerin mahkemelere sunacağı raporların bilimselliğine dair tanımlama getirerek adli soruşturmalarda delil olarak kullanılacak bir tekniğin ilgili olduğu bilimsel camiada genel kabul görmüş olması gerektiğini belirtmiştir. Günümüzde "Frye Standardı" olarakta bilinen bu tanımlamaya göre "bir tekniğin bilimselliğinin ölçütü, o tekniğin ilgili olduğu bilimsel camiada genel kabul görüp görmemesidir." (47).

Bu standartla birlikte Amerika'da yargılama alanında tartışmalara neden olmuş bir diğer olayda ise Jason Daubert ve kardeşinin bir ilaç şirketi ile yaşadıkları hukuk mücadelesi

sonucunda Birleşik Devletler Yüksek Mahkemesi tarafından yargıçların delillerin bilimselliğini kabul edip etmemelerine yönelik somut bir yöntem sunulmuştur. Buna göre;

a. Mahkemede savunulan teori veya teknik, test edilebilir olmalıdır.
b. Bu teori veya teknik ilgili bilimsel camiada değerlendirilmiş ve bilimsel bir platformda yayımlanmış olmalıdır.
c. Ayrıca mahkeme savunulan tekniğin potansiyel hata oranını dikkate almalıdır.
d. Delilin kabul edilebilirliğini önemli ölçüde etkileyen diğer bir hususta savunulan teori veya tekniğin bilimsel camiada genel kabul görmüş olmasıdır (47).

Adli bilişim incelemelerinde ise kullanılacak yazılımların gerçek sonuçları verip vermediği, tekrar eden incelemelerde aynı sonuçlara ulaşılıp ulaşılmadığı bu yazılımların kullanılmadan önce doğrulanması ile mümkündür. Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology- NIST) tarafından başlatılan bir proje Adli Bilişim Yazılımları Test Projesi (Computer Forensics Tool Testing Project-CFTT) kapsamında adli bilişim alanında kullanılan açık veya kapalı kaynak kodlu yazılımlar inceleme türlerine göre test edilmekte ve etkinlikleri karşılaştırılmaktadır (46),(48). Delillerin bilimsel olması ve delil elde etmeye yarayan yazılım ve donanımların test edilmesi mahkemeye sunulacak her türlü delilin bir insanın suçluluğu ve suçsuzluğunu ortaya çıkarması açısından önemli olduğu değerlendirilmektedir.

Adli bilişim alanında uygulanacak deney yöntemlerinin güvenilirliği açısından kullanılacak yazılım ve donanımların test edilmiş olmasının yanısıra deney yöntemlerinin de standart hale getirilmesi için çalışmalar sürmektedir. Ülkemizdeki kriminal laboratuvarların da üyesi olduğu Avrupa Adli Bilim Enstitüleri Ağı (European Network of Forencis Science Intitutes-ENFSI) ISO/IEC 17025 Deney ve Kalibrasyon Laboratuvarlarının Yeterliliği kapsamında üye laboratuvarların tamamının akredite olmasını beklemektedir (49).

Bu kapsamda Jandarma Kriminal Daire Başkanlığına bağlı Bilişim Teknolojileri İnceleme Şube Müdürlükleri, Emniyet Genel Müdürlüğü Kriminal Dairesi Başkanlığına bağlı Ses, Görüntü ve Data İnceleme Şube Müdürlüğü ve Adli Tıp Kurumu Fizik İhtisas Dairesine bağlı Bilişim ve Teknoloji Suçları Şubelerinin ilgili laboratuvarları ISO/IEC 17025 Deney ve Kalibrasyon Laboratuvarlarının Yeterliliği kalite standardına göre Türk Akreditasyon Kurumu

(TÜRKAK) tarafından akredite edilmeye başlanmıştır (50). Akredite olan kurumlar ve deney yöntemleriyle ilgili güncel bilgiye TÜRKAK internet sitesinden ulaşılabilmektedir (51).

2.5 Adli Bilişim

Adli Bilimlerin çatısı altında kendine yer bulan en yeni disiplinlerden birisi olan Adli Bilişimin ortaya çıkmasındaki temel etmen suçluların eylemlerini daha kolay gerçekleştirip daha zor tespit edileceklerini sağlayan teknolojik ürünler ve sistemleri keşfetmeleridir. Aslında temel amacı insan hayatını kolaylaştırmak olan teknolojik ürünlerin suçluların da eylemlerini teşvik etmesinden ve kolaylaştırmasından daha doğal bir durum beklenemezdi (12).

Adli Bilişim (Computer Forensics) yabancı bir terim olarak dilimize girmiş olup bilgisayar, cep telefonu, CD/DVD, taşınabilir bellek ve veri depolama özelliği olan tüm elektronik cihazlar üzerinde bulunan sayısal delillerin tespit edilmesi, analizi ve raporlandırılması süreci olarak tanımlanabilir (32).

Adli bilişimin ne olduğunu anlamak için bu yeni kavramın uygulamada yapılmış olan tanımlarını incelemek faydalı olacaktır.

Karagülmez'e göre "Adli bilişim, bilgisayarın sabit disk sürücüsünün otopsi işlemini yapmaktır. Çünkü bilişim suçu sonrasında, bilişim sisteminde (özellikle sabit disk sürücüsünde) çeşitli seviyelerde depolanan bilgiler, uzman ekiplerce, özel yazılım araçları ve tekniklerle bulunup gömülü bilgi keşfedilmeye çalışılmaktadır." (12).

Berber ise Adli Bilişimi, "Potansiyel yasal delillerin elde edilmesi amacıyla bilgisayar inceleme ve analiz teknikleri kullanılarak yapılan bir uygulama" şeklinde tanımlamaktadır (5).

Şirikçi ve Akarslan'a göre; "Adli bilişim, elektromanyetik ve elektrooptik ortamlarda muhafaza edilen veya bu ortamlarca iletilen ses, görüntü, veri, bilgi veya bunların birleşiminden oluşan her türlü bilişim nesnesinin, mahkemede sayısal delil niteliği taşıyacak şekilde tanımlanması, elde edilmesi, saklanması, incelenmesi ve mahkemeye sunulması çalışmaları bütünüdür." (11),(52).

Adli bilişim incelemeleri belirli safhalardan oluşmaktadır. Bunlar;

- Tanımlama (Identification)
- Toplama (Collection)
- Düzenleme (Organization)
- Sunum (Presentation) aşamalarıdır (11),(43).

2.5.1 Adli Bilişimin (Aşamaları) Safhaları

Adli bilişimin olay yerinde başladığını düşünürsek; olay yerindeki mevcut bulguların mahkemelerce delil olarak kabul görmesi için belli kriterlere sahip olması gerekli olup elektronik delillerde ancak uygun prosedürler uygulanırsa delil değeri kazanmaktadır. Aksi takdirde yapılan bu çalışmalar hiçbir anlam ifade etmeyecektir (5). Bu prosedürleri genel olarak delil toplama, delillerin analizi (incelenmesi), sonuçların değerlendirilmesi ve elde edilen sonuçların raporlanması olarak safhalara ayırmak mümkündür (52).

Elektronik verilere delil niteliği kazandırarak değerlendirme ve yorumlama yapılabilmesi için belli prosedürlere bağlı olarak bu işlem basamakları sırasıyla uygulanmalıdır (6).

2.5.1.1 Toplama (elde etme) aşaması

Bu aşamada delil niteliği taşıyabilecek nesnelerin toplanması ve uygun şekilde paketlenerek incelenmek üzere kriminal laboratuvarlara gönderilmesini kapsar. Bu aşamada dikkat edilmesi gereken husus olay yerine müdahale eden ilk ekibin delillerin bozulmasını önleyecek şekilde tespit etmesidir. Bilinçsizce ve uzman olmayan kişilerce yapılacak müdahaleler delillerin geçerliliğini yitirmesine de neden olabilmektedir. Bu aşamada toplanan deliller kayıt altına alınarak delil teslim zinciri oluşturulur ve delile ilk müdahaleden itibaren yapılan işlemler geriye dönük olarak takip edilebilir (32).

Delilleri toplama aşamasında bilgisayarın açık veya kapalı olmasına göre farklı yöntemler uygulanmalıdır. Bilgisayar açıksa, ekrandaki görüntüler fotoğraflanır ve kayıt altına alınır. Bilgisayar açık ancak ekran karanlık veya ekran koruyucu varsa fare hareket ettirilerek masaüstü görüntüsü tespit edilerek fotoğraflanır ve kayıt altına alınır. Eğer ekran kapalıysa ekranın elektrik bağlanıtısı kontrol edilerek ekran açılır, fotoğraf ve kayıt işlemleri yapılır. Bu işlemler yapıldıktan sonra adli bilişim uzmanı tarafından yapılacak bir değerlendirmeye göre

ihtiyaç duyulması halinde açık sistemlerden delil toplama yöntemleri uygulanabilir. Bu yöntemler genellikle bilgisayara ait uçucu verilerin toplanması, geçici bellek kopyasının[4] alınması, çalışan süreçlerin ve açık ağ bağlantılarının tespit edilmesidir. Açık sistemlerden delil toplanırken az da olsa sistem üzerinde değişiklik yapılmaktadır. Bu değişikliklere neden olacak her türlü işlem kayıt altına alınmalı, toplanan delillerin geçerliliğinin sağlanabilmesi açısından hangi adli bilişim yazılımlarının kullanıldığı belirtilmelidir (11).

Bilgisayar ekranı açılmazsa, masaüstü görüntülenemezse bilgisayarın elektrik bağlantısı prizden itibaren kesilir ve bilgisayarın kapalı olduğu durumlardaki işlemler geçekleştirilir. Bu işlemler genellikle hedef bilgisayarın sabit diskleri sökülerek yazma korumalı olarak birebir kopyalama cihazı veya inceleme bilgisayarına bağlanıp birebir kopyalarının alınması şeklinde uygulanmaktadır. Bilgisayarın kopyası olay yerinde alınamıyorsa kablo bağlantıları fotoğraflanır, tüm çevre birimleri etiketlenerek toplanır ve işlemler kayıt altına alınarak delil teslim zinciri başlatılır. (11).

5271 sayılı Ceza Muhakemesi Kanunu 134'üncü maddesi kapsamında elektronik deliller toplanırken elektronik veri içeren bulguların birebir kopyaları (imaj) alınır. Tüm incelemelerin orijinal delillerin zarar görmemesi için birebir kopyalar üzerinde yapılması esastır. Bu sayede delilin değiştirilmediği, herhangi bir müdahaleye maruz kalmadığı teyit edilmiş olur (6). Kopya alma işlemi için donanımsal bir cihaz veya adli bilişim bilgisayarı üzerindeki bir yazılım vasıtasıyla yapılmaktadır. Birebir kopyaların algoritma imzaları (hash değeri) kopyalama esnasında tespit edilmektedir. Bu değer alınan kopyanın bütünlüğünü ve değiştirilmeden kriminal laboratuvara ulaştırıldığının ya da incelenen kopyanın daha sonra tekrar incelenmesi durumunda ilk halinin bozulmadığının sağlamasını yapmak için kullanılmaktadır (11). Delilin el koyma esnasında alındığı şekliyle korunduğunun en büyük kanıtı birebir kopya alma esnasında oluşturulan algoritma imzasıdır. Algoritma imzası (hash değeri) delilin parmakizi gibidir ve hesaplama yöntemleri sebebiyle her delil için farklı değerler almaktadır. Adli bilişim standardı olarak uygulamada genellikle Mesaj Özeti (Message Digest-MD5) veya Güvenli Özetleme Algoritması (Secure Hash Algorithm-SHA256) gibi algoritmalar kullanılmaktadır (32).

[4] Rastgele Erişimli Bellek (Random Access Memory-RAM)

2.5.1.2 Analiz Aşaması

Kriminal laboratuvarlarda (veya adli bilişim laboratuvarlarında) yürütülmesi esas olan bu aşamada; suç türüne göre adli mercilerin inceleme isteğine göre uygulanacak yöntemler tespit edilir. İnceleme isteğinin doğru tahlil edilmesi ile el konulan ve kopyası alınmış olan delillerin incelemesi hızlı bir şekilde tamamlanabilecektir. Delilin daha önce birebir kopyası alınmamışsa yani delil fiziksel olarak toplanmışsa incelemeye birebir kopya (imaj) alınarak başlanır. Eğer birebir kopya alınmışsa elimize gelen kopyanın algoritma imzası (hash değeri) tespit edilerek olay yeri incelemesindeki algoritma imzası teyit edilir (6).

Delil bütünlüğünün korunduğu tespit edildikten sonra inceleme safhasına geçilir. Adli bilişim uzmanları incelemeyi talep eden makamın inceleme istek yazısına uygun olarak aşağıdaki yöntemlerden uygun olanlarını seçerek olayın oluş şeklini açıklamaya yarayacak delilleri tespit etmektedirler.

- Dosya Türüne Göre İnceleme
- Anahtar Kelime Aranması Yöntemiyle İnceleme
- Mevcut Dosyaların Tespit Edilerek İncelenmesi
- Silinmiş Verilerin Kurtarılması
- Dosya Tarih ve Zaman Bilgileri İncelemesi
- Şifreli Dosyaların İncelenmesi
- İnternet Geçmişi İncelemeleri
- Elektronik Posta İncelemeleri
- Dosyaların Algoritma İmzalarına Göre İncelenmesi
- İşletim Sistemi İncelemesi (3),(6),(53)

Bu yöntemler ve daha fazlası kriminal laboratuvarlarda en iyi uygulama rehberleri temel alınarak oluşturulmuş deney yöntemleridir. Bu yöntemlerin uygulanması sonucunda ortaya çıkan veriler analiz edilerek bir sonraki aşamada değerlendirme ve raporlamaya dayanak teşkil edecek olanlar ortaya çıkarılmaya çalışılmaktadır.

2.5.1.3 Sonuçların değerlendirilmesi (Kriminal inceleme)

Sonuçlar değerlendirilirken hangilerinin suçu aydınlatmada adli makamlara yardımcı olacağına ve hangilerinin delil niteliği taşıdığına karar verilir. Burada önemli nokta inceleme isteğinde bulunan adli mercilerin sordukları soruların eksiksiz yanıtlanmış olmasıdır. Bu aşamada ortaya konan hususlar raporlama aşamasında adli bilişim uzmanı tarafından yazılı olarak sunulmalıdır. Kriminal incelemelerin birbirinden bağımsız en az iki uzman tarafından yapılması sonuçların doğruluğu açısından bir denetleme mekanizmasıdır. Elde edilen sonuçlar ve deliller veri depolama birimlerine (CD, DVD veya Taşınabilir Bellek vb.) kaydedilerek uzmanlık raporuyla birlikte inceleme makamına gönderilmektedir (6).

2.5.1.4 Raporlama (Sunum)

Sunum (Presentation) olarakta adlandırılan raporlama aşamasında uygulamada en az iki adli bilişim uzmanı tarafından "Bilirkişi Raporu"[5] düzenlenmektedir. Adli mercilere sunulmak üzere hazırlanan rapor;

a. Teknik bilgi sahibi olmayan kişiler tarafından anlaşılacak şekilde olmalı,
b. Teknik terimler az olmalı ve mutlaka açıklanmalı,
c. Soruşturmayla ilgili bilgileri içermeli,
d. İncelemeye verilen deliller tanımlanmalı, (delilin markası, modeli, seri numarası, kapasitesi, algoritma imzası ve doğrulanmış algoritma imzası vb.)
e. İncelemede kullanılan deney yöntemleri belirtilmeli,
f. Kullanılan adli bilişim yazılımları ve versiyonları belirtilmeli, (kullanılan yazılım ve donanımların adli bilişim için özel olarak geliştirilmiş delil üzerinde değişiklik yapmayan veya en az değiklik yapması tercih edilmelidir.)
g. Yapılan işlemler sırasıyla yazılmalı,

Delilin alınan birebir kopyası tekrar incelenmesi gerekebileceği için raporla birlikte talep makamına gönderilmelidir (6).

---

[5] Jandarma Kriminal Daire Başkanlığı laboratuvarlarında **"Uzmanlık Raporu"**
Kriminal Polis Laboratuvarlarında **"Ekspertiz Raporu",**
Adli Tıp Kurumunda **"Bilirkişi Raporu"** olarak adlandırılmaktadır. Birbirine benzer bu isimler zaman içerisinde kurumlar tarafından değiştilebilmektedir. Ancak hukuk sistemimizde inceleme yapan kişiler bilirkişi olarak adlandırıldığından "Bilirkişi Raporu" denmesinin daha doğru olacağı değerlendirilmektedir.

2.5.2 Bulut Sistemleri Kullanan Bilgisayarların Adli İncelemesi

Bulut adli bilişimi, bulut sistemler üzerinde meydana gelmiş olayların yeniden canlandırılması amacıyla elektronik verilerin tanımlanması, toplanması, saklanması, incelenmesi ve raporlanması için bilimsel yöntemlerin, teknolojik uygulamaların ve kanıtlanmış yöntemlerin uygulanmasıdır (54).

Bulut sistemler bilgisayara ait tüm işlevlerin ve klasik anlamda anladığımız çoğu verinin sanal ortamda bulunduğu yapılardır. Bulut sistemler ve ürünler yaygınlaşmadan önce kullanıcılar tüm verilerini kendi bilgisayarları üzerinde ya da depolama birimlerinde saklama eğilimindeydiler. Ancak yeni çıkan ürünler bu durumu tümüyle tersine çevirmeye başlamıştır. Artık herkes istediği içerikleri (resim, metin, ses, video vs.) internet üzerinde depolamakta ve en önemlisi paylaşabilmektedir.

Bulut hizmetlerini kullanan bilgisayarların incelenmesinde klasik adli bilişim yöntemlerinden daha fazlası gerekmektedir. Bu hizmetler yerel bilgisayarların yanısıra internet bağlantısıyla uzaktaki bir sunucuda da delil barındırmaktadır. Daha önce de ifade edildiği gibi üç temel bulut hizmeti *Yazılım Hizmeti Olarak Bulut* (SaaS), *Platform Hizmeti Olarak Bulut* (PaaS) ve *Altyapı Hizmeti Olarak Bulut* (IaaS) bulunmaktadır. Ayrıca bu hizmetlere en yaygın olarak bilgisayarlar, tablet bilgisayarlar ve cep telefonları aracılığıyla ulaşılmaktadır (55).

Klasik adli bilişimde bilgisayarlardan delil toplanırken öncelikle bilgisayarın açık olup olmamasına göre değerlendirme yapılır. Açık bir bilgisayarda öncelikle uçucu veriler tespit edilir ve toplanmaya çalışılır. Daha sonra bilgisayarın elektrik bağlantısı kesilerek kapalı bir bilgisayarda yapılacak delil toplama adımları uygulanır (42). Bulut depolama uygulamalarını kullanan bilgisayarlarda ise ilk aşamada bilgisayar analiz edilirken bulut servis sağlayıcıların uygulamalarının bulunup bulunmadığı da araştırılmalıdır. Bilgisayar açıksa tespit edilecek uçucu veriler sayesinde parolalar, kullanıcı oturum bilgileri veya yetkileri tespit edilebilmektedir. Elde edilen bu bilgiler sayesinde bulut depolama alanındaki verilere erişim sağlanabilmekte burada bulunan delillere ulaşılabilmektedir (55).

Bulut sistemler delil araştırması yapılırken klasik adli bilişimde uygulamaya alıştığımız tekniklerin kullanılmasında bu sistemlerin doğal bazı özelliklerinden ötürü zorluk

çekilmektedir. Bulut sistemler yapısı gereği kullanıcı verilerini kaybolmaması için birden fazla sunucuya yedeklendiğinden verileri tek bir merkezden toplamak mümkün olmayıp, bu sunucuların farklı coğrafi konumlarda olabilmelerinden ötürü delil toplanırken yasal sınırlamalarla karşılaşılmaktadır (7).

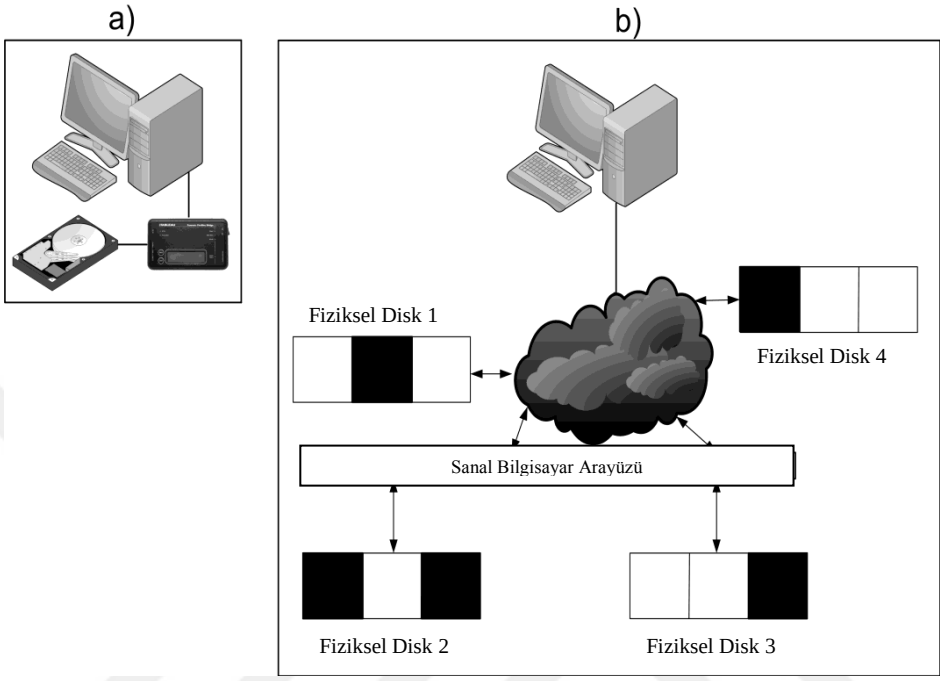
Ayrıca halihazırda adli bilişim incelemelerinde kullanılan yazılım ve donanımlar klasik anlamda fiziksel olarak elimizde olan delillerin incelenmesi üzerine tasarlanmışlardır. Bu yazılımlardan bazıları kurumsal veya bireysel ağlar üzerinden de uzaktan birebir kopya almaya veya delil toplamaya imkan sağlamaktadır. Ancak bu işlemin gerçekleştirilmesi için hedef sisteme (bilgisayar, sunucu vb.) küçük bir yazılım yüklenmesi gerekmektedir (7). Verilerin değişikliğe uğrayacağı bu yöntemin delil bütünlüğünün sağlanması açısından sorunlar çıkarmaktadır.

Bulut sistemlerden bir diğer delil elde etme yöntemi ise şüphelinin oturum açma bilgileri ile sisteme giriş yapmaktır. Bu yöntemde internet üzerinden gerçek sisteme bağlanılmakta olup herhangi bir yazma koruması olmadan klasik adli bilişimde kapalı bir bilgisayarı açmayla eşdeğer şekilde verileri değiştireceği değerlendirilmektedir. Bu iki yöntemde şüphelinin kullandığı sisteme müdahaleyi içerdiğinden mahkemede verilerin değiştirildiğini iddia edilmesi riskini taşımaktadır.

Bu yöntemler ve benzerleri sayesinde bulut sistemler üzerinde depolanan verilerin kopyalarının alınabildiğine yönelik çalışmalar mevcut olup, bu işlemlerin bazı sakıncaları bulunmaktadır.

a. Öncelikle delilin bütünlüğünün sağlaması yapılamamaktadır.
b. Sisteme yazma koruması olmadan erişim sağlanmaktadır.
c. Bulut sistemlerden delil toplamaya yönelik yazılımlar yaygın değildir.
d. Kullanılan yöntemler, yazılım ve donanımların değerlendirilmesi ve onaylanmış yöntemler olarak kabul görmüş değildir.
e. Buluttaki fiziksel alanın tamamı birebir kopyalanması büyük ölçekli sistemlerde Pratik bir uygulama olmamaktadır.
f. Alınan kopya silinmiş alanları içermediğinden klasik adli bilişimde anladığımız birebir kopya olmamaktadır.

g. Ayrıca bulut üzerinde bulunan veriler sunucular üzerinde birden fazla yere kopyalanabildiklerinden alınan kopyanın tam olup olmadığı kesin olarak ifade edilememektedir (7),(56).



Şekil 8: (a) Klasik birebir kopyalama (b) Bulut ortamında kopyalama (56)

Önümüzdeki dönemde bu işlemlerin mahkemelerce kabul edilebilir yasal prosedürlere uygun olarak yapılmasına imkan sağlayacak yazılımların üretilmesi veya bulut hizmeti veren servis sağlayıcılar tarafından adli birimlere yönelik delil toplama hizmetinin kolluk personeline özel bir arayüz aracılığıyla bulut üzerinden sağlanması muhtemeldir. Ancak bu geçiş sürecinde suçluların işledikleri eylemlerle ilgili kolluk personelini yasal olarak sıkıntıya düşürmeyecek bazı yöntemlerin geliştirilmesine geliştirilen yöntemlerin ise sistematik hale getirilmesine ihtiyaç duyulmaktadır.

Mevcut zorluklara rağmen şüpheliden elde edilen bilgisayarlar çok çeşitli deliller ihtiva edebilmektedir. Hem yasal sorunlar yaşamamak hem de servis sağlayıcıların kullanıcılarının verilerini paylaşmama durumlarının üstesinden gelmek amacıyla, adli bilişim uzmanları bulut hizmetlerini kullanan bir bilgisayardan delil toplarken öncelikle el konulan bilgisayar üzerinden delil toplamalı ve bu delillerle bulut depolama alanından herkese açık ortamda ulaşılabilen verilerle ilişkilendirmeye çalışmalıdır. Bu ilişkilendirme soruşturma konusu bulut

depolama alanına el konulan bilgisayardan oturum açılıp açılmadığı, soruşturma konusu dosyaların yüklenip yüklenmediği tespit edilerek yapılabilir.

3. GEREÇ VE YÖNTEM

Bu tez çalışması Kasım 2015-Mayıs 2016 dönemi arasında İstanbul Jandarma Kriminal Laboratuvarı Bilişim Teknolojileri İnceleme Şube Müdürlüğünde yapılmış olup; bulut depolama uygulamaları kullanılarak işlenebilecek bir suçun soruşturulmasında el konulan bilgisayarlar üzerinde ne tür deliller elde edilebileceği, bulut depolama alanı ve içeriğindeki dosyalarla bu bilgisayarların ilişkisinin ortaya konulup konulamayacağı incelenmiştir. İncelemeler test senaryoları üzerinden yapılmıştır.

3.1. Materyal

Halihazırda servis sağlayıcılar tarafından sunulan bulut depolama hizmetlerinin sayısının çok çeşitli olmasından dolayı hepsini incelemek yerine ülkemizde son dönemde kişisel kullanıcı sayısını trafik uygulamaları, elektonik posta hizmeti gibi hizmetlerle artıran Yandex firmasının bulut depolama hizmeti Yandex.Disk örnek olarak seçilmiştir. Uygulama test senaryoları dahilinde VMware sanallaştırma programıyla oluşturulmuş Windows 7(64 bit) ve Windows 8.1 (64 bit) işletim sistemlerine sahip sanal bilgisayarlar üzerinde test edilmiştir.

İşletim Sistemi	Windows 8.1 Pro (64 bit)
İşlemci	Intel® Core™ i7-4790 CPU@ 3.60 Ghz
Geçici Bellek	8.00 GB

Tablo 1. İnceleme bilgisayarının özellikleri

İşletim Sistemi	Windows 7 Professional Service Pack 1 (64 bit)
İşlemci	Intel® Core™ i7-4790 CPU@ 3.60 Ghz
Geçici Bellek	2.00 GB

Tablo 2. Deneme yapılan sanal bilgisayarların özellikleri

İşletim Sistemi	Windows 8.1 Pro (64 bit)
İşlemci	Intel® Core™ i7-4790 CPU@ 3.60 Ghz
Geçici Bellek	2.00 GB

Tablo 3. Test ve kontrol için kullanılan sanal bilgisayarın özellikleri

Araştırma konusunu test edebilmek için yapılan modelleme çalışmasında aşağıdaki sorular oluşturulmuştur.

1. Bir bilgisayarda bulut depolama uygulaması (Yandex.Disk) kurulduğunda hangi veriler oluşur?
2. Bir bilgisayardan bulut depolama uygulamasıyla depolama alanına dosya yüklendiğinde hangi veriler oluşur? (Dosyaların bu bilgisayardan yüklendiğine dair hangi delillere ulaşılabilir)
3. Bulut depolama uygulamasıyla dosyalar paylaşıma açıldığında bilgisayarda hangi veriler oluşur?
4. Bulut depolama alanından bilgisayara dosya indirildiğinde hangi veriler oluşur?

3.2. İncelenecek Örnek Bulut Servisi

Yandex Disk®

Yandex.Disk, Yandex firmasının kullanıcılarına dosya depolama hizmeti sağlayan bir servistir. Yandex Disk'te bulunan dosyalarla internete bağlı herhangi bir cihazdan erişilebilmektedir (57).

3.3. İncelemede Kullanılan Programlar

Vmware 10 : Vmware şirketinin bilgisayar işlevlerini sanallaştırma amacıyla ürettiği yazılımdır.

Encase 7.06 : Guidance Software şirketi tarafından üretilen adli bilişim yazılımının 7 numaralı versiyonlarından biridir.

Encase 6.19.1: Guidance Software şirketi tarafından üretilen adli bilişim yazılımının 6 numaralı versiyonlarından biridir. Encase 7.06 ile benzer özelliklere sahip olup kullanıcı arayüzü farklı olup, önümüzdeki dönemde şirket tarafından yeni sürümleri yayımlanmayacaktır.

HashCalc : Slavasoft şirketi tarafından üretilmiş, dosyaların çeşitli algoritma imzalarını hesaplamaya yardımcı bir programdır.

Dcode v4.02a : **www.digital-detective.co.uk** adresinden indirilebilen tarih zaman bilgilerini birbiri arasında çevirmeye yarayan programdır.

FTK Imager : Accessdata firmasının ürettiği bilgisayar aracılığıyla birebir kopya (imaj) alma programıdır.

3.4. İncelemede Kullanılan Yöntem

1. VMware sanallaştırma programı kullanılarak Windows 7 (64 bit) işletim sistemine sahip sanal bilgisayarlar oluşturulmuş ve işlemler bu bilgisayarlarda yapılmıştır Ayrıca yöntemi test edebilmek için bir adet Windows 8 (64 bit) işletim sistemine sahip sanal bilgisayar kullanılmıştır.

2. Oluşturulan ilk sanal bilgisayar kontrol numunesi olarak program kurulmadan muhafaza edilmiş, içeriğinde bulunan dosyaların algoritma imzaları hesaplanmış ve algoritma imzası veritabanı (hash set) oluşturulmuştur.

3. ***"Bilgisayarda bulut depolama uygulaması (Yandex Disk) kurulduğunda hangi veriler oluşur? (Bir bilgisayarda kullanılan bulut depolama uygulaması nasıl tespit edilir?)"*** [6] sorusunu cevaplamak için;

a. Uygulama sanal bilgisayara kurulmuş,

b. Sanal bilgisayar kapatılarak tüm dosyaların algoritma imzaları hesaplanmış ve bir önceki aşamada oluşturulan veritabanından farklı olanlar tespit edilmiş, bu dosyaların kurulumla birlikte oluşan dosyalar olduğu görülmüş,

c. Bilgisayarın kayıt defterinde (registry) meydana gelen değişiklikler tespit edilmiş, (uygulamalar kurulmadan önceki kayıt defteri ile kurulduktan sonraki durumları karşılaştırılmıştır.)

d. Uygulama kurulduğunda oluşan dosyalar analiz edilerek içeriğindeki veriler tespit edilmiştir.

4. ***"Bilgisayardan bulut depolama uygulamasıyla depolama alanına dosya yüklendiğinde hangi veriler oluşur? (Dosyaların bu bilgisayardan yüklendiği nasıl tespit edilebilir?)"*** [7] sorusunu cevaplamak için;

---

[6] Bir uygulama bilgisayarda kurulduğunda bilgisayarın işletim sistemine bağlı olarak klasör yapılarında değişiklik meydana gelir, uygulama kullanacağı kurulum dosyalarını işletim sisteminin bulunduğu klasörlere oluşturur, ayrıca bilgisayarın kayıt defterinde "registry" kayıt anahtarları oluşturur. Bu kurulum dosyalarına ulaşılması ve içeriklerinin analizi ile kayıt defterinin incelenmesi bize bir uygulamanın kullanıldığı ile ilgili bilgi verir.

[7] Dosyanın herhangi bir zamanda bilgisayarda bulunması veya bulunduğu ile ilgili verilere ulaşılması, uygulamanın kurulum dosyaları, log kayıtları içerisinde bu dosyalara ait bilgi bulunması bize fikir verecektir.

a. Yandex.Disk uygulaması kurulu olan bilgisayar kopyalanmış, işlemlere bu bilgisayar üzerinden devam edilmiş,

b. 10 adet örnek resim dosyası oluşturulmuş,

S.Nu	Dosya Adı	MD 5 Algoritma İmzası	Boyut	Önizleme
1	aslan.JPG	99b74d2b105f067a566ac9cd049af533	113.139	
2	baykuş.JPG	568c0010bc319ca9983e9dadba15a4f9	78.058	
3	kanarya.JPG	3fd9e7e7fe20dd6c2d02f0fc979edfbe	28.831	
4	kartal.JPG	d9bf4533b8f9288963cc22f090714bde	79.845	
5	koala.JPG	3c7678bd394138adff8a2906aa35b8cb	53.488	

S.Nu	Dosya Adı	MD 5 Algoritma İmzası	Boyut	Önizleme
6	kuleli.JPG	7602f802eaf05cd4bdde13e6a659c0d2	90.175	
7	kutup ayıları.JPG	db04dfa1d41750ca7c2f9944146b6b2d	60.948	
8	tilki.JPG	0e2f79aad8aa4c7ed302944182505709	65.203	
9	zebra.JPG	9bc505b801f2464ca60d82d8405f91e0	59.618	
10	zürafa.JPG	6a41ebe9f7bce88bdc00390157665040	78.756	

Tablo 4. Oluşturulan resim dosyaları ve algoritma imzaları

c. Dosyaların algoritma imzaları HashCalc programı ile hesaplanmış,

d. Bu dosyalar uygulama aracılığıyla bulut depolama alanına yüklenmiş,

e. Yüklenen dosyaların isimleri ve algoritma imzaları sanal bilgisayarlar üzerinde Encase 6.19.1 programı ile anahtar kelime olarak aratılmış,

f. Bir önceki aşamada uygulama kurulurken oluşan dosyalardaki değişiklikler dosyalar yüklendikten sonra tekrar kontrol edilerek farklılıklar tespit edilmiştir.

5. ***"Bulut depolama uygulamasıyla dosyalar paylaşıma açıldığında bilgisayarda hangi veriler oluşur?" (Bu bilgisayardan yüklenen dosyalar paylaşıma açılmış mıdır?)***[8] sorusunu cevaplamak için;

a. Bir önceki aşamada kullanılan sanal bilgisayarın kopyası alınmış ve aynı bilgisayar üzerindeki veriler korunarak bulut depolama alanına yüklenen dosyalar paylaşıma açılmış,

b. Uygulamanın kurulum dosyalarındaki değişiklikler incelenmiştir.

6. ***"Bulut depolama alanından bilgisayara dosya indirildiğinde hangi veriler oluşur?*** sorusunu cevaplamak için;

a. Uygulama yeni sanal bilgisayara kurulmuş,

b. (ibbali) olarak yeni bir hesap oluşturulmuş ve bu hesaba Tablo-4'te bulunanlardan farklı bir resim dosyası yüklenmiştir. (Topkapı_Sarayı.jpg)

c. (ibbali) hesabıyla paylaşıma açılan dosya (ynddeneme) hesabıyla oturum açılarak sanal bilgisayara indirilmiş,

d. Bilgisayar kapatılarak uygulamanın kurulum klasörleri incelenmiştir.

7. ***"Bulut depolama uygulaması bilgisayardan kaldırıldıktan sonra yüklenen, paylaşıma açılan veya indirilen dosyalar bilgisayardan silindiğinde bu veriler tespit edilebilir mi?***

a. Dosyaların bulut depolama alanına yüklendiği sanal bilgisayarın (4'üncü maddedeki bilgisayar) kopyası alınarak işlemlere bu bilgisayar üzerinden devam edilmiş,

b. Uygulama kaldırılmış,

c. Uygulamanın kurulum dosyaları ve diğer klasörler incelenmiştir.

[8] Dosyayı paylaşan kullanıcının bu bilgisayardan oturum açtığı ve paylaşım yaptığı dosyalarla ilgili bilgiler uygulamanın kurulum dosyalarında, log kayıtlarında bulunarak bağlantı kurulabilir.

8. ***İnceleme yöntemi farklı bir işletim sisteminde test edilirse benzer sonuçlara ulaşılabilir mi?***

a. Yandex.Disk uygulaması için oluşturulan Tablo 7'deki anahtar kelimeleri test edebilmek için incelemelerde kullanılan işletim sisteminden farklı (Windows 8) bir işletim sistemine sahip sanal bilgisayar kurulmuş,

b. Yandex.Disk uygulaması bu bilgisayara kurulmuş,

c. Tablo-4'teki dosyalar yüklenmiş ve paylaşıma açılmış,

d. Yandex.Disk uygulaması kaldırılarak, dosyalar silinmiş ve incelemeler yapılmıştır.

4. BULGULAR

4.1 Uygulama bilgisayara kurulduktan sonra tespit edilen veriler

Uygulama bilgisayarlara kurulduktan sonra tespit edilen veriler Tablo 5-6, Şekil 9-17'de görülmektedir.

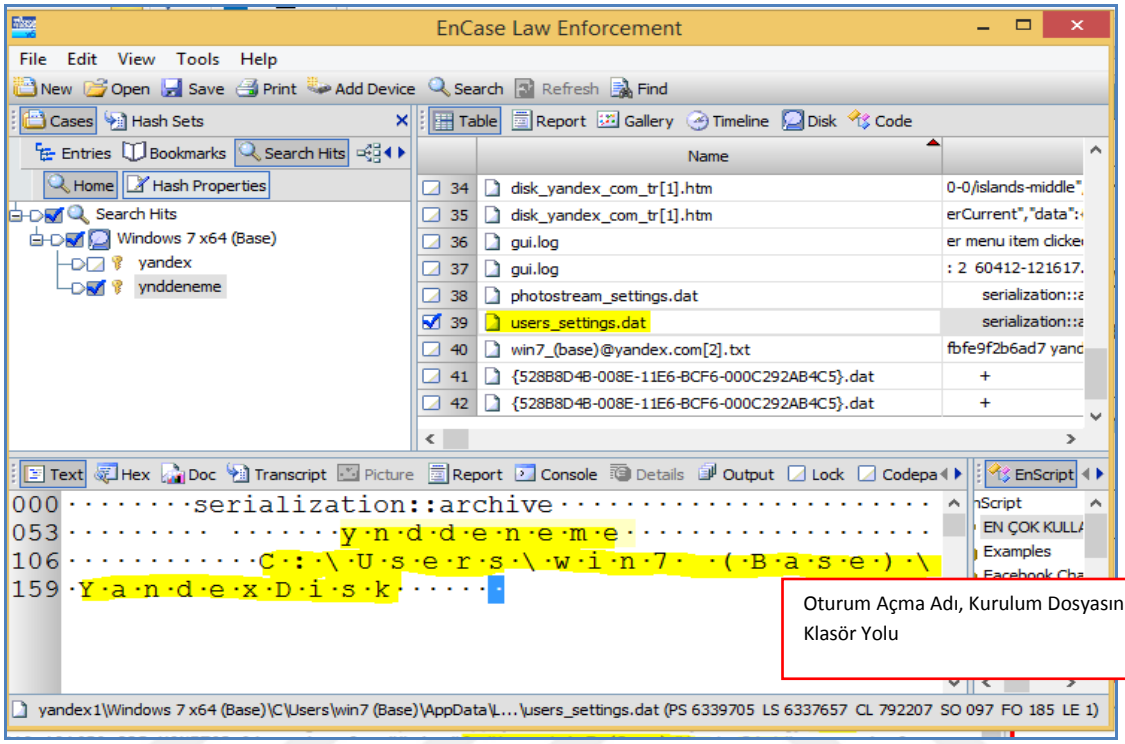
Oluşan Klasör	Eklenen Dosya
c:\Program Files\yandex\yandexDisk\bin\	yandexDiskOverlays-2398.dll
c:\Users\<Kullanıcı Adı>\AppData\Local\Temp\	yupdate-ping-yadisk.temp
c:\Users\<Kullanıcı Adı>\AppData\Local\yandex\yandex.Disk\	~Overlay_0.txt
c:\Users\<Kullanıcı Adı>\AppData\Local\yandex\yandex.Disk\	~Overlay_1.txt
c:\Users\<Kullanıcı Adı>\AppData\Local\yandex\yandex.Disk\	~Overlay_2.txt
c:\Users\<Kullanıcı Adı>\AppData\Local\yandex\yandex.Disk\	~Overlay_3.txt
c:\Users\<Kullanıcı Adı>\AppData\Local\yandex\yandex.Disk\	activity.dat
c:\Users\<Kullanıcı Adı>\AppData\Local\yandex\yandex.Disk\	config.xml
c:\Users\<Kullanıcı Adı>\AppData\Local\yandex\yandex.Disk\	events_cache_setup.dat
c:\Users\<Kullanıcı Adı>\AppData\Local\yandex\yandex.Disk\	main_menu_settings.dat
c:\Users\<Kullanıcı Adı>\AppData\Local\yandex\yandex.Disk\	menu_settings.dat
c:\Users\<Kullanıcı Adı>\AppData\Local\yandex\yandex.Disk\	notification_data.xml
c:\Users\<Kullanıcı Adı>\AppData\Local\yandex\yandex.Disk\	users_settings.dat
c:\Users\<Kullanıcı Adı>\AppData\Local\yandex\yandex.Disk\	yandexDiskInstaller.log
c:\Users\<Kullanıcı Adı>\AppData\Local\yandex\yandex.Disk\	yandexDiskSetup.log
c:\Users\<Kullanıcı Adı>\AppData\LocalLow\yandex\Updater\	yupdate-exec-statistic.log
c:\Users\<Kullanıcı Adı>\AppData\LocalLow\yandex\Updater\	yupdate-exec-yadisk.log
c:\Users\<Kullanıcı Adı>\AppData\LocalLow\yandex\Updater\yadisk\	appinfo.xml
c:\Users\<Kullanıcı Adı>\AppData\LocalLow\yandex\Updater\yadisk\	statistics.xml
c:\Users\<Kullanıcı Adı>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\yandex.Disk\	Ekran görüntüleri yandex.Disk'te.lnk
c:\Users\<Kullanıcı Adı>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\yandex.Disk\	yandex.Disk.lnk
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\	clids-yadisk.xml
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\	ui
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\yandexDisk\	dllyupdate.dll
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\yandexDisk\	downloader.exe
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\yandexDisk\	freetype6.dll
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\yandexDisk\	libcairo-2.dll
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\yandexDisk\	libexpat-1.dll
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\yandexDisk\	libfontconfig-1.dll
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\yandexDisk\	libpng14-14.dll
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\yandexDisk\	libpng14-14-x64.dll
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\yandexDisk\	license.rtf

Oluşan Klasör	Eklenen Dosya
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\yandexDisk\	yadisk_48x48.png
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\yandexDisk\	yandexDisk.exe
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\yandexDisk\	yandexDiskHooks.dll
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\yandexDisk\	yandexDiskInstaller-5052.exe
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\yandexDisk\	yandexDiskScreenshotEditor.exe
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\yandexDisk\	yandexDiskShellExt-4724.dll
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\yandexDisk\	yandexDiskStarter.exe
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\yandexDisk\	yupdate-exec.exe
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\yandexDisk\	zlib1.dll
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\yandexDisk\	zlib1-x64.dll
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\yandexDisk\wow64\	yandexDiskHooks.dll
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\yandexDisk\wow64\	yandexDiskShellExt-4724.dll
c:\Users\<Kullanıcı Adı>\AppData\Roaming\yandex\yandexDisk\wow64\	yandexDiskStarter.exe
c:\Users\<Kullanıcı Adı>\Desktop\	Ekran görüntüleri yandex.Disk'te.lnk
c:\Users\<Kullanıcı Adı>\Desktop\	yandex.Disk.lnk
c:\Users\<Kullanıcı Adı>\Links\	yandex.Disk.lnk
c:\Users\<Kullanıcı Adı>\yandexDisk\	desktop.ini
c:\Users\<Kullanıcı Adı>\yandexDisk\.sync\	core.log
c:\Users\<Kullanıcı Adı>\yandexDisk\.sync\	gui.log

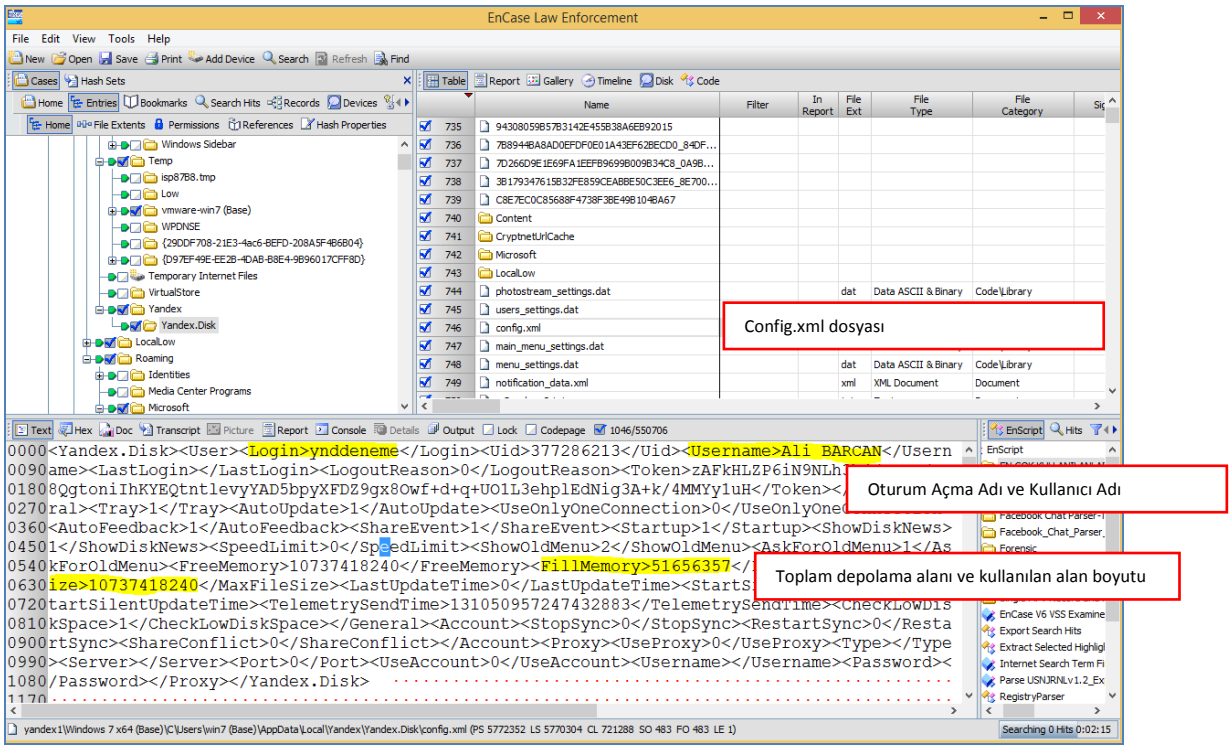
Tablo 5. Yandex.Disk kurulumu esnasında oluşan klasörler ve dosyalar

S.Nu.	Dosya Adı	Tespit Edilebilen Bilgiler
1	users_settings.dat	Oturum Açma Adı, Kurulum Dosyasının Klasör Yolu
2	config.xml	Oturum Açma Adı, Kullanıcı Adı, Toplam Depolama Alanı, Kullanılan Depolama Alanı Boyutu
3	core.log	Oturum Açma Adı, Toplam Depolama Alanı, İçeriğinde Bulunan Dosyalar ve Boyutları, İndirilen ve Yüklenen Dosyalar, Dosyaların İndirilme ve Yüklenme Zamanları, Kurulum Dosyalarının Klasör Yolu ve Bilgisayar Adı, Algoritma İmzası
4	gui.log	Oturum Açma Adı, Oturum Açıldığı Zaman, Oturum Açılan Bilgisayarla ilgili bilgiler
5	Cookie Dosyaları	Oturum Açma Adı

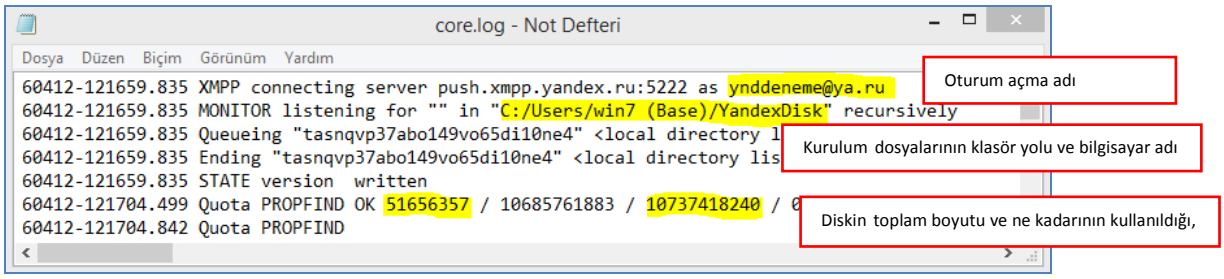
Tablo 6. Yandex.Disk kurulumu esnasında oluşan dosyalardan önemli görülenler ve içeriklerinde tespit edilen veriler



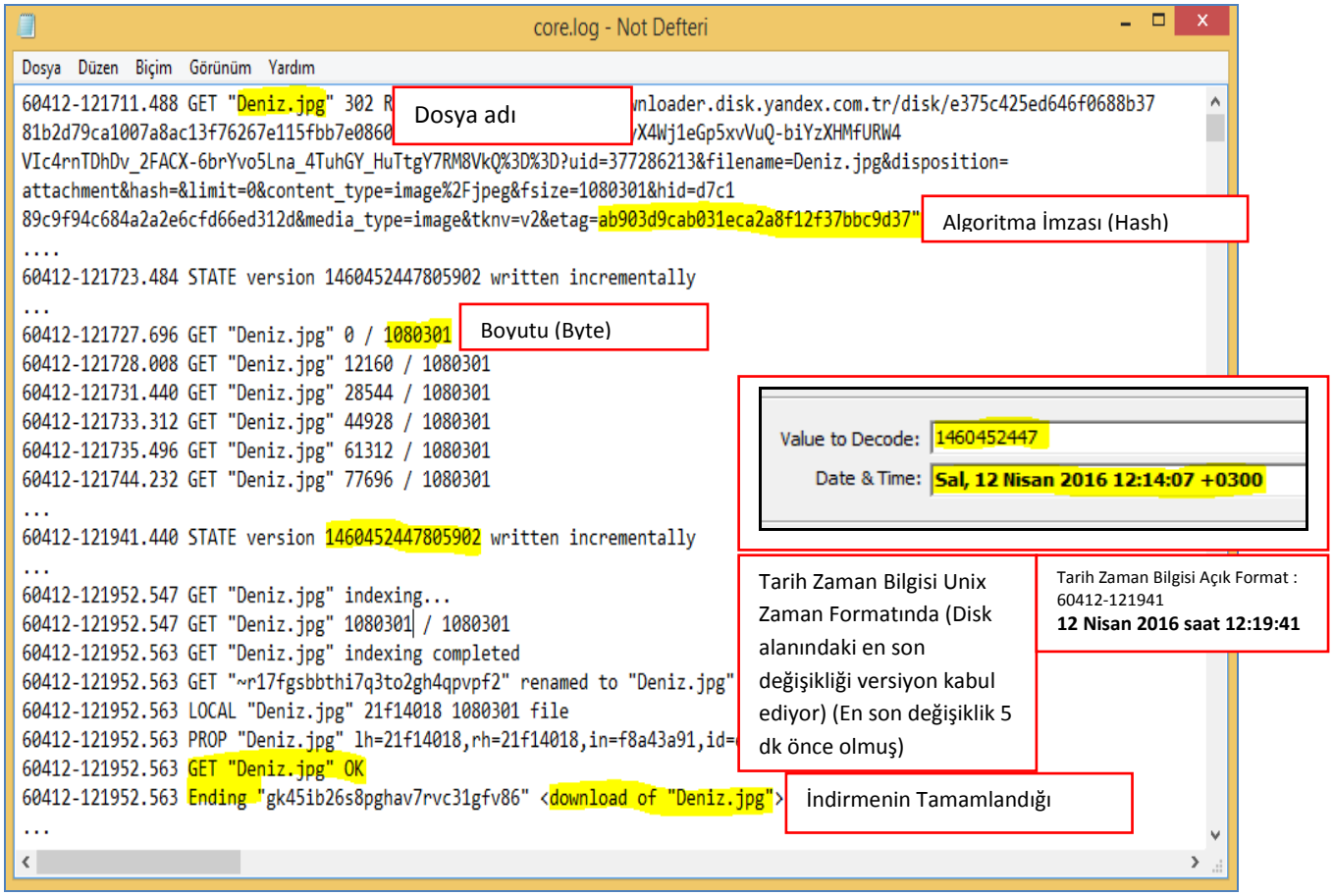
Şekil 9: users_settings.dat dosyasında tespit edilen veriler



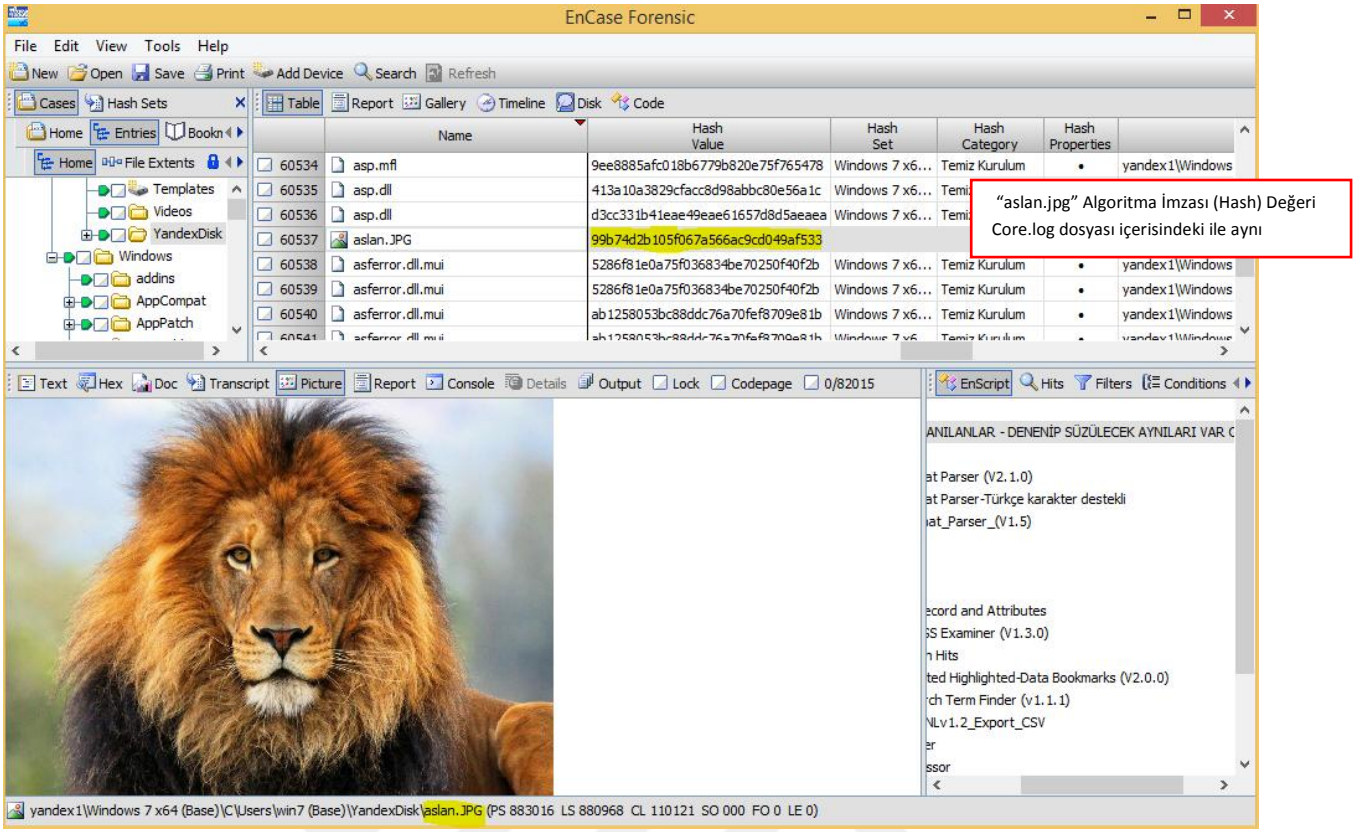
Şekil 10: Config.xml dosyasında tespit edilen veriler



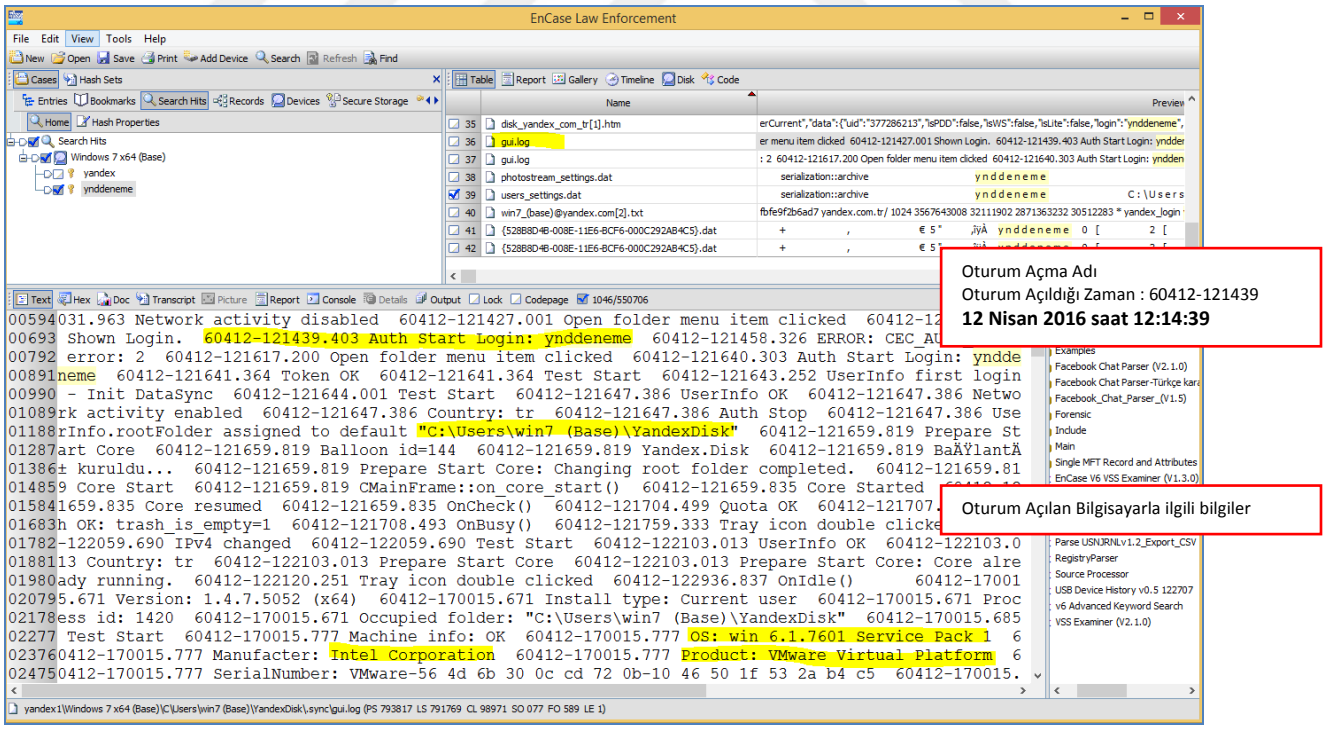
Şekil 11: Core.log dosyasında tespit edilen veriler (a)



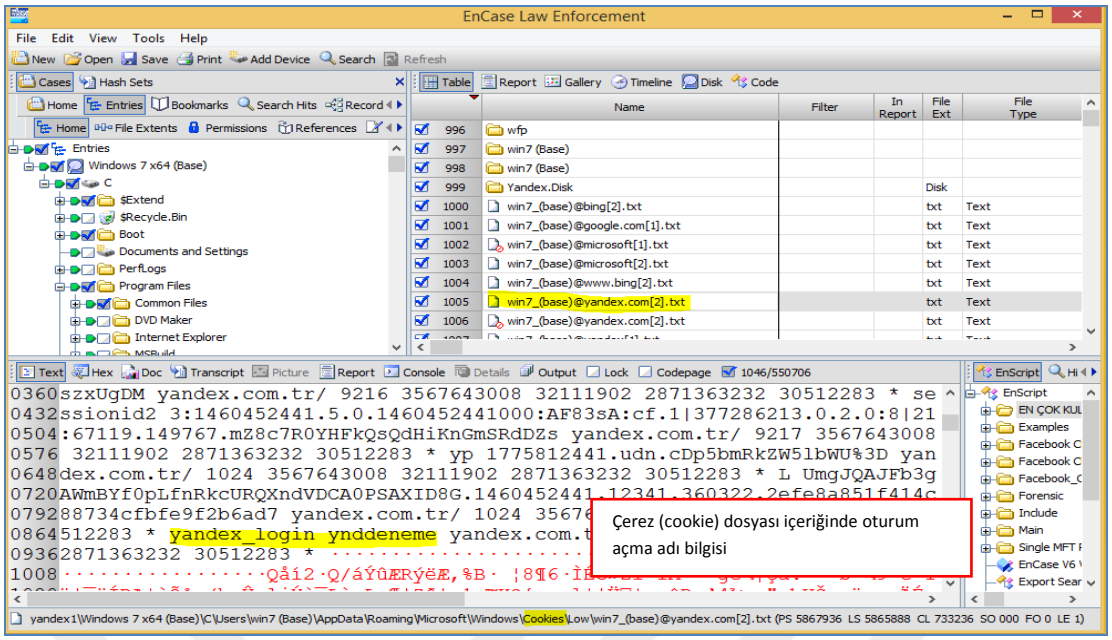
Şekil 12: Core.log dosyasında tespit edilen veriler (b)



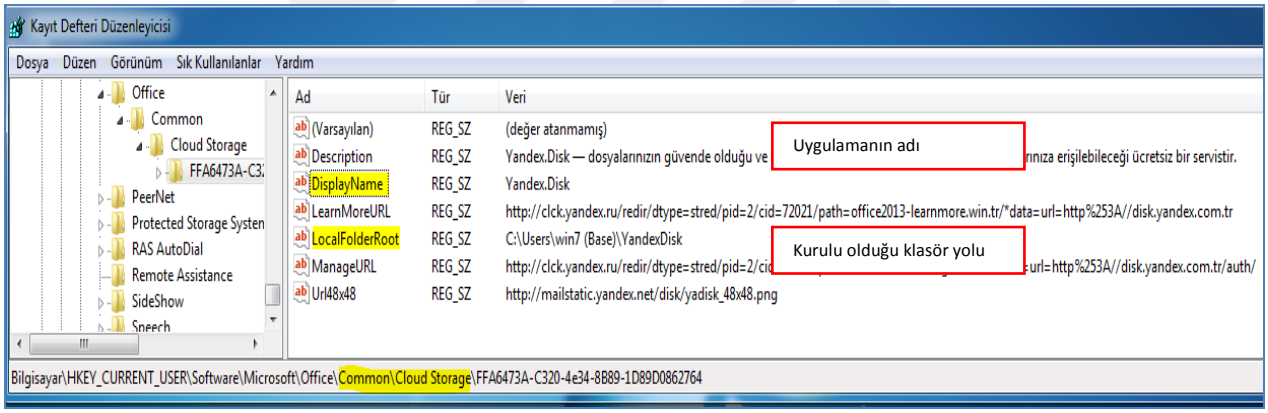
Şekil 13: core.log dosyasına kaydedilen dosyalara ait algoritma imzaları



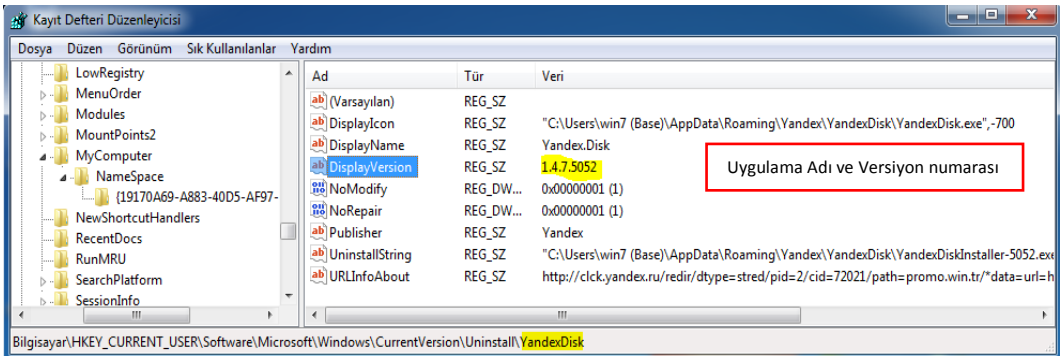
Şekil 14: gui.log dosyasının incelenmesi



Şekil 15: Çerez (cookie) dosyalarının incelenmesi

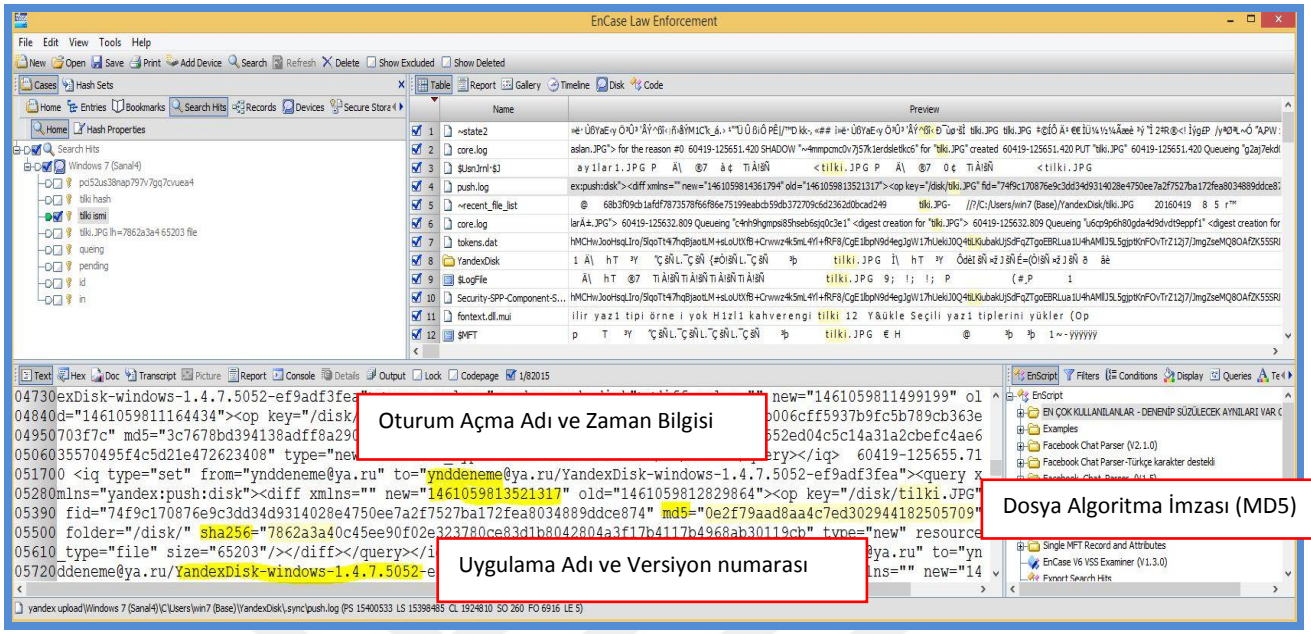


Şekil 16: Bilgisayar kayıt defterinin (registry) incelenmesi (a)

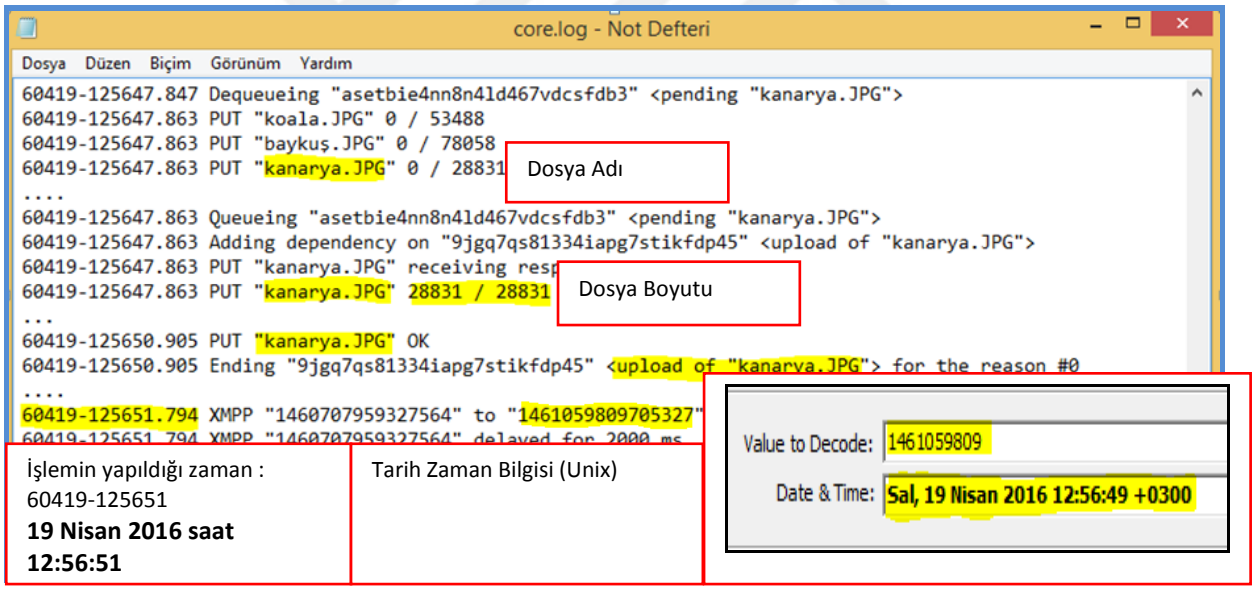


Şekil 17: Bilgisayar kayıt defterinin (registry) incelenmesi (b)

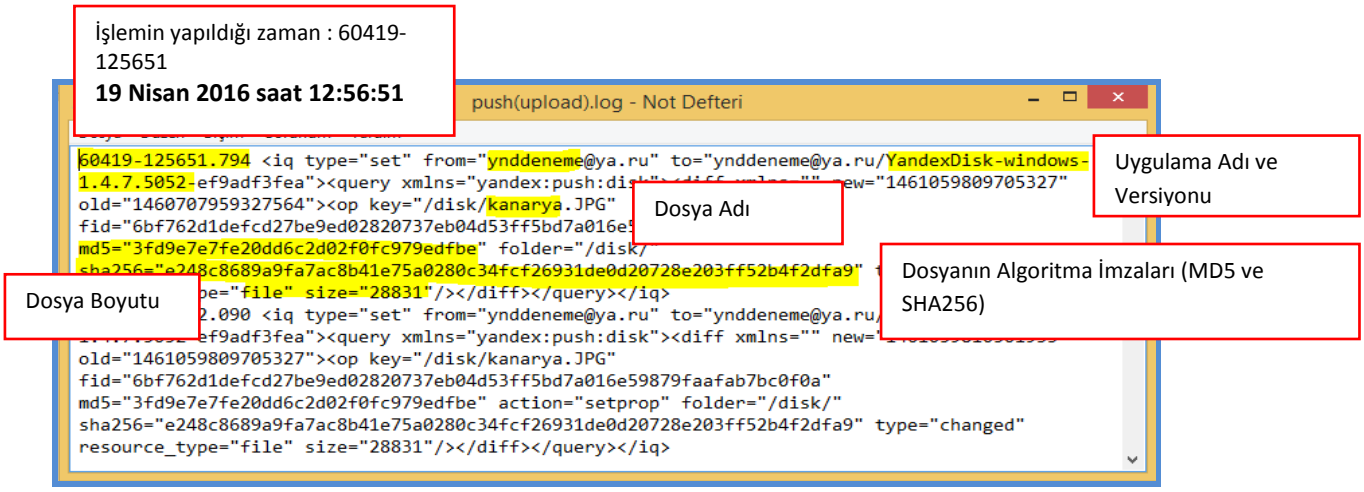
4.2 Uygulama aracılığıyla dosyalar yüklendikten sonra tespit edilen veriler



Şekil 18: Anahtar Kelime Sonuçları

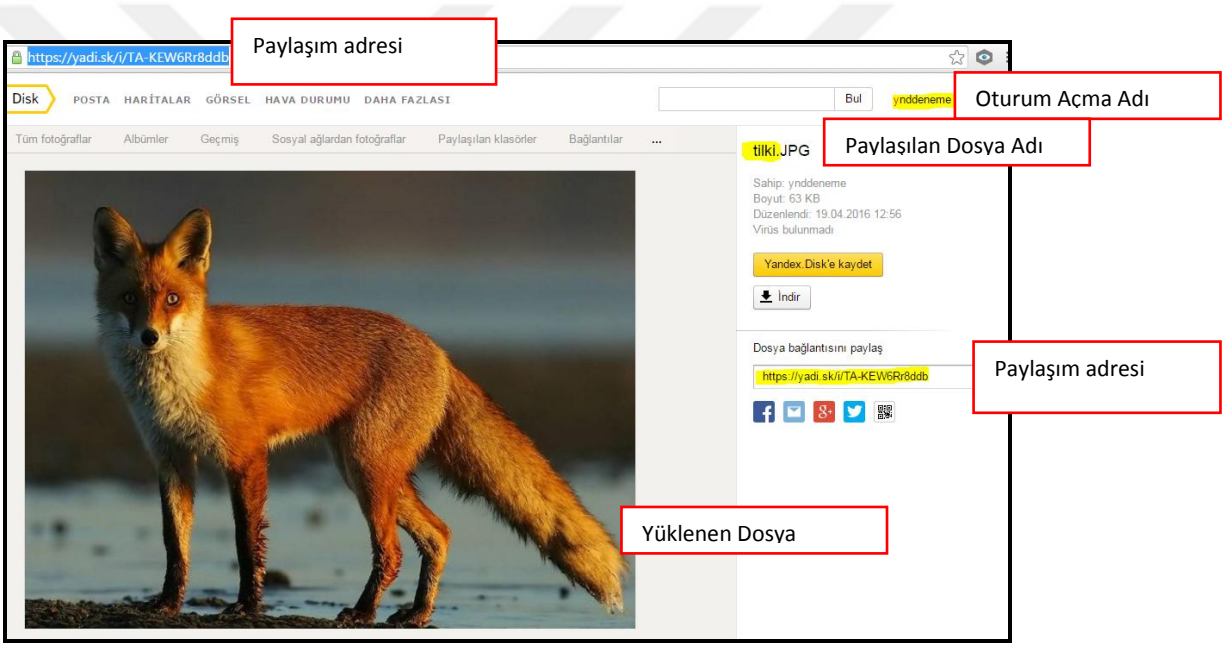


Şekil 19: core.log dosyasındaki değişiklikler

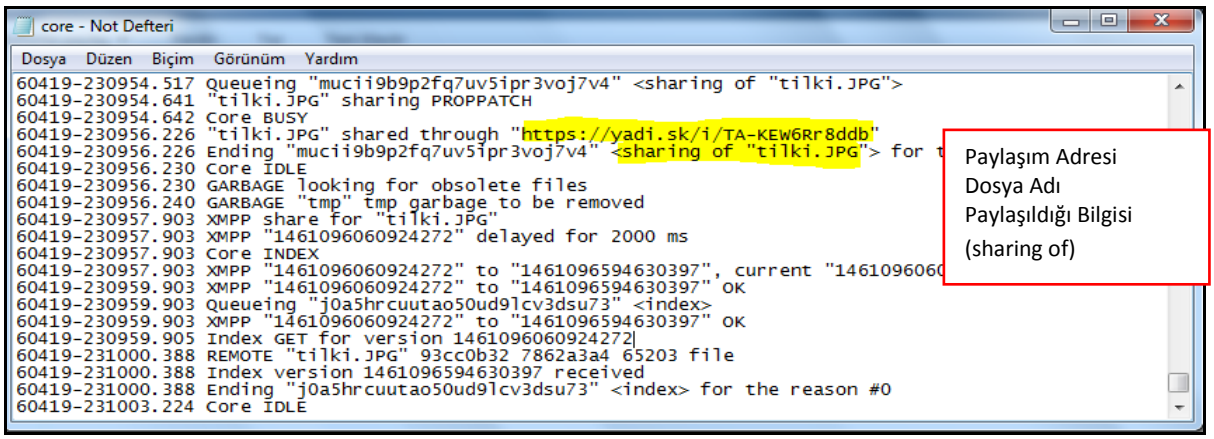


Şekil 20: push.log dosyasındaki değişiklikler

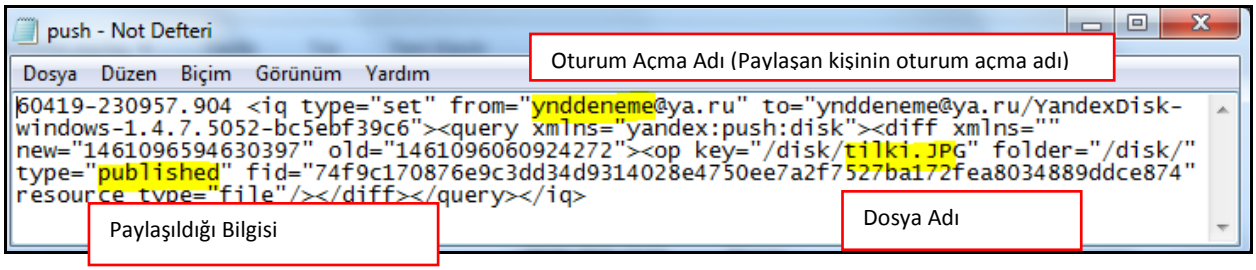
4.3 Dosyalar paylaşıma açıldıktan sonra tespit edilen veriler



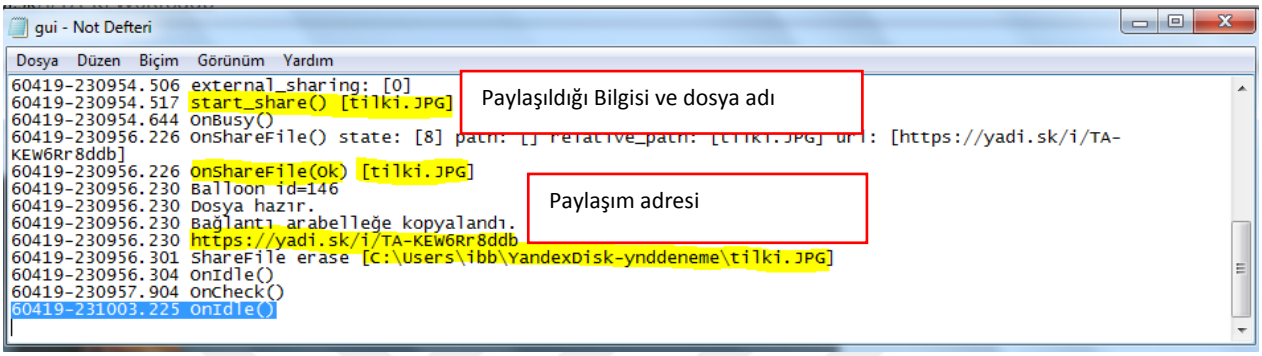
Şekil 21: Paylaşıma açılan dosya



Şekil 22: Core.log dosyası paylaşımdan sonra

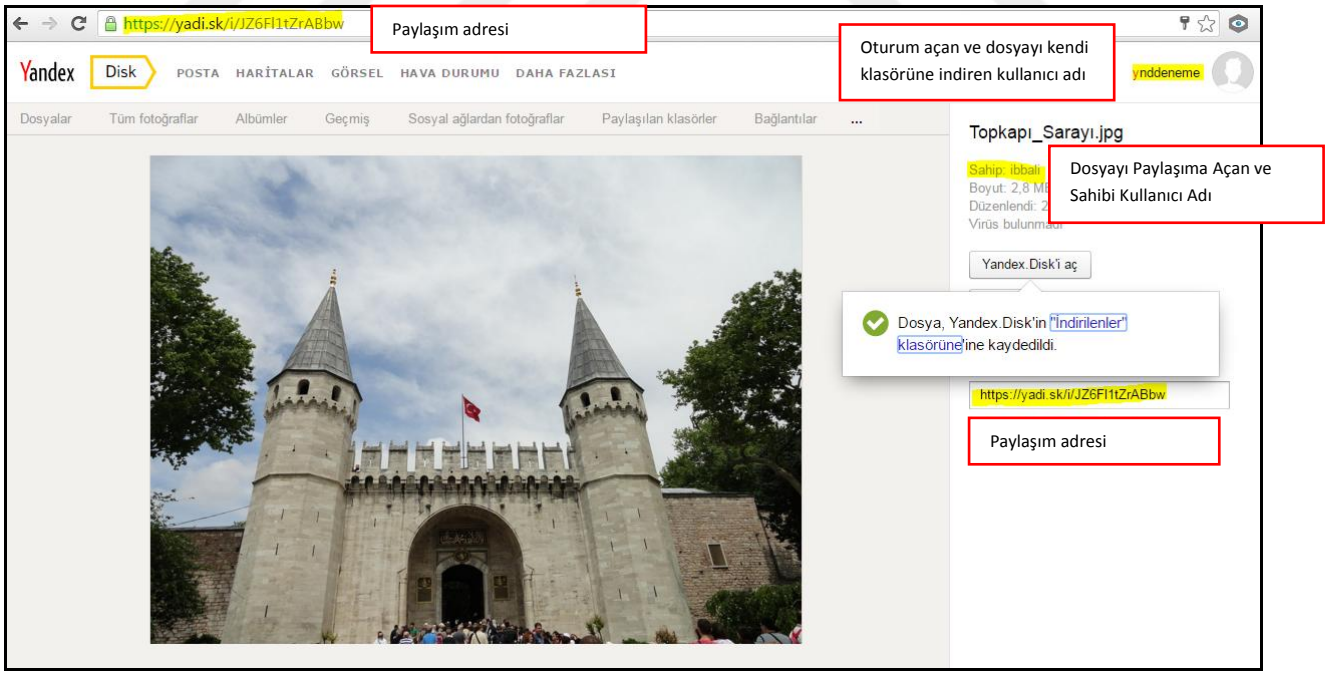


Şekil 23: push.log dosyası paylaşımdan sonra

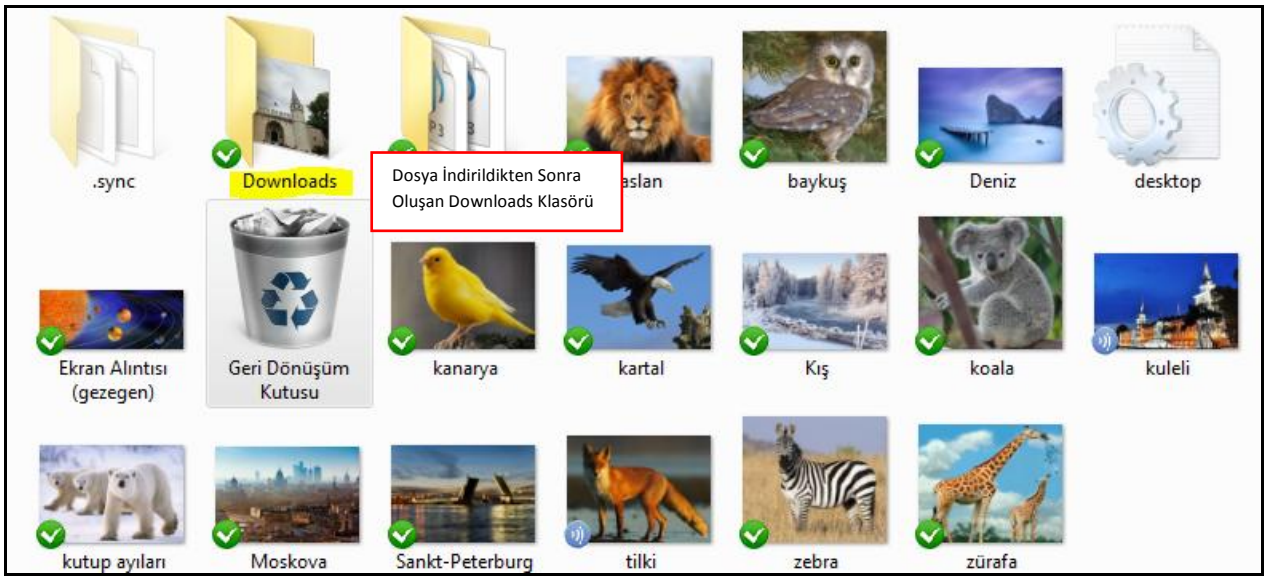


Şekil 24: gui.log dosyası paylaşımdan sonra

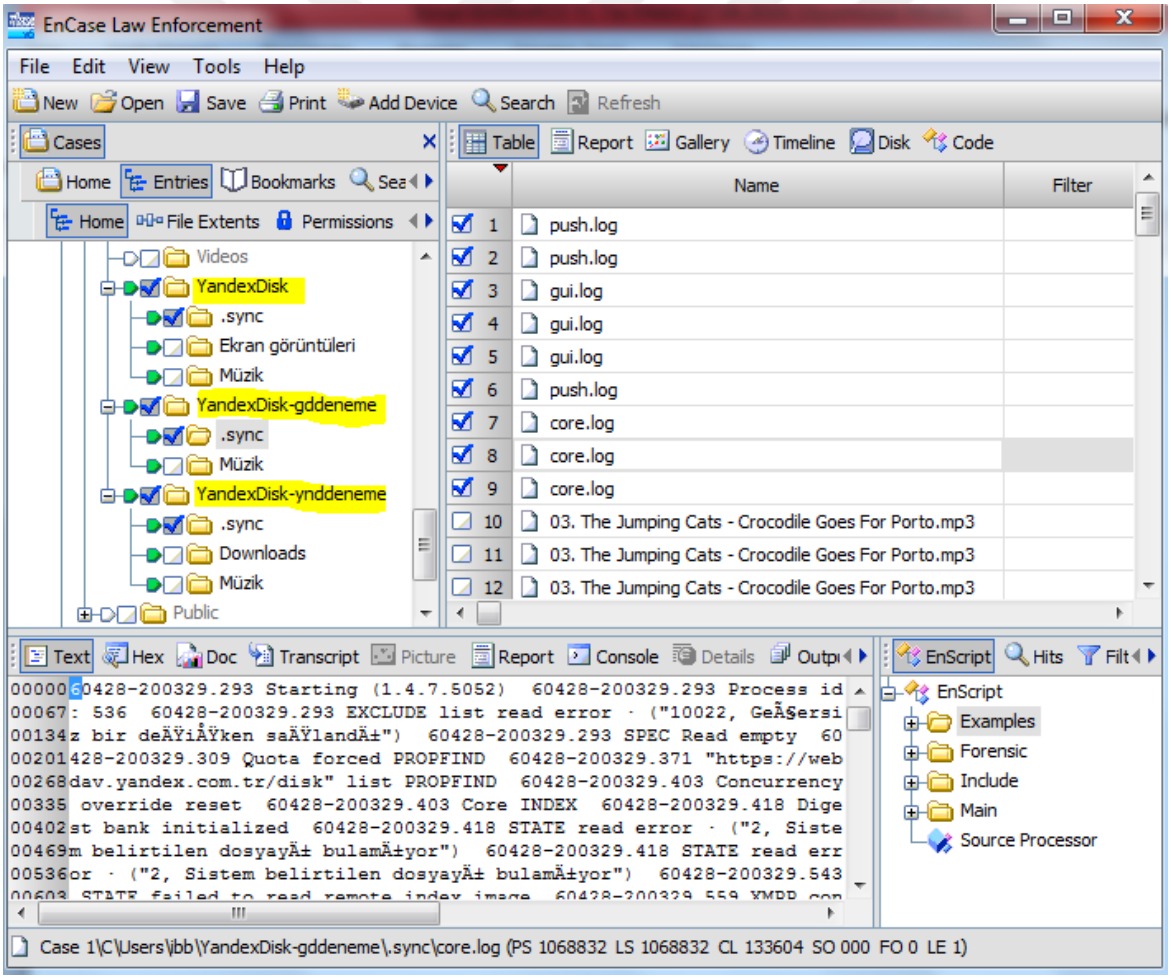
4.4 Dosya indirilmesi ile ilgili tespit edilen veriler



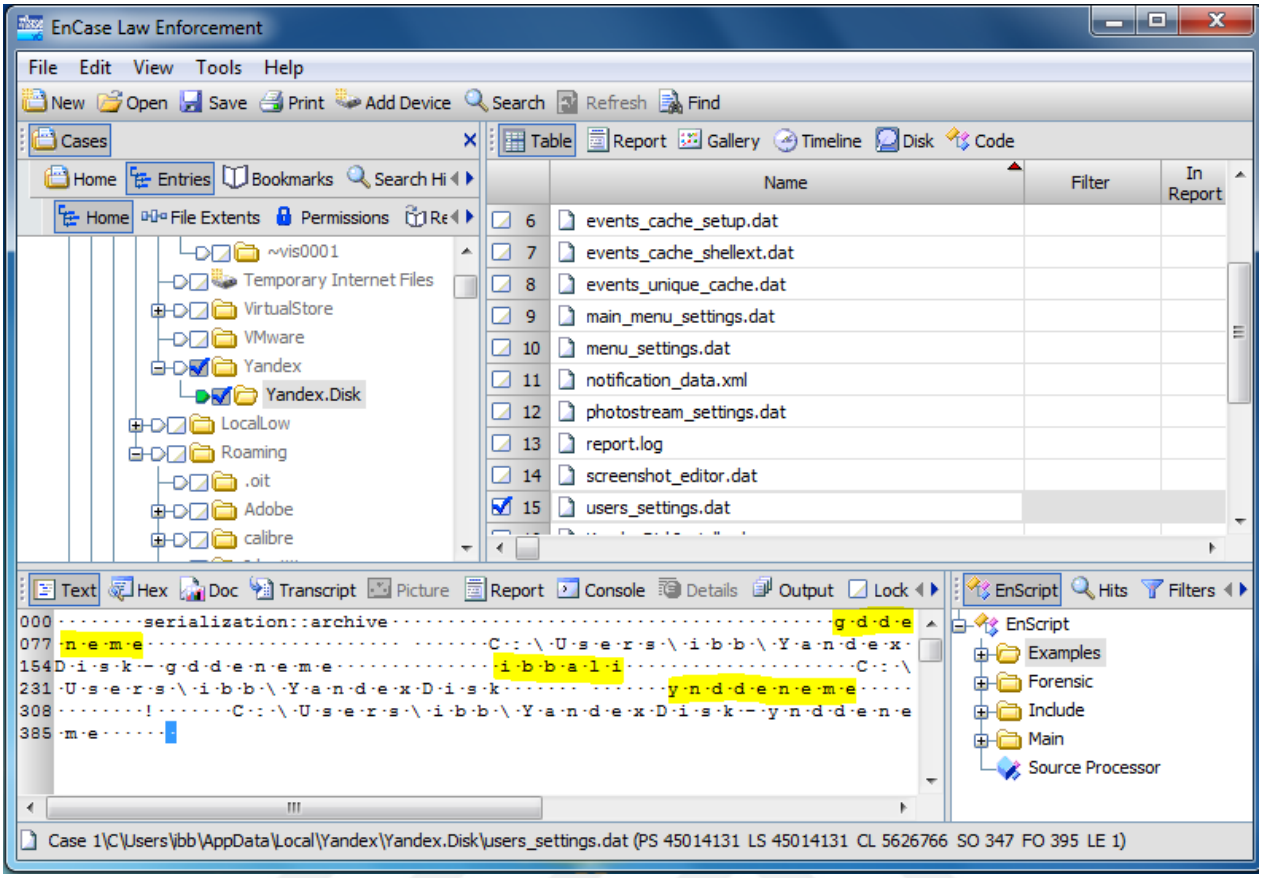
Şekil 25: İndirilen dosyanın internet tarayıcı üzerindeki görüntüsü



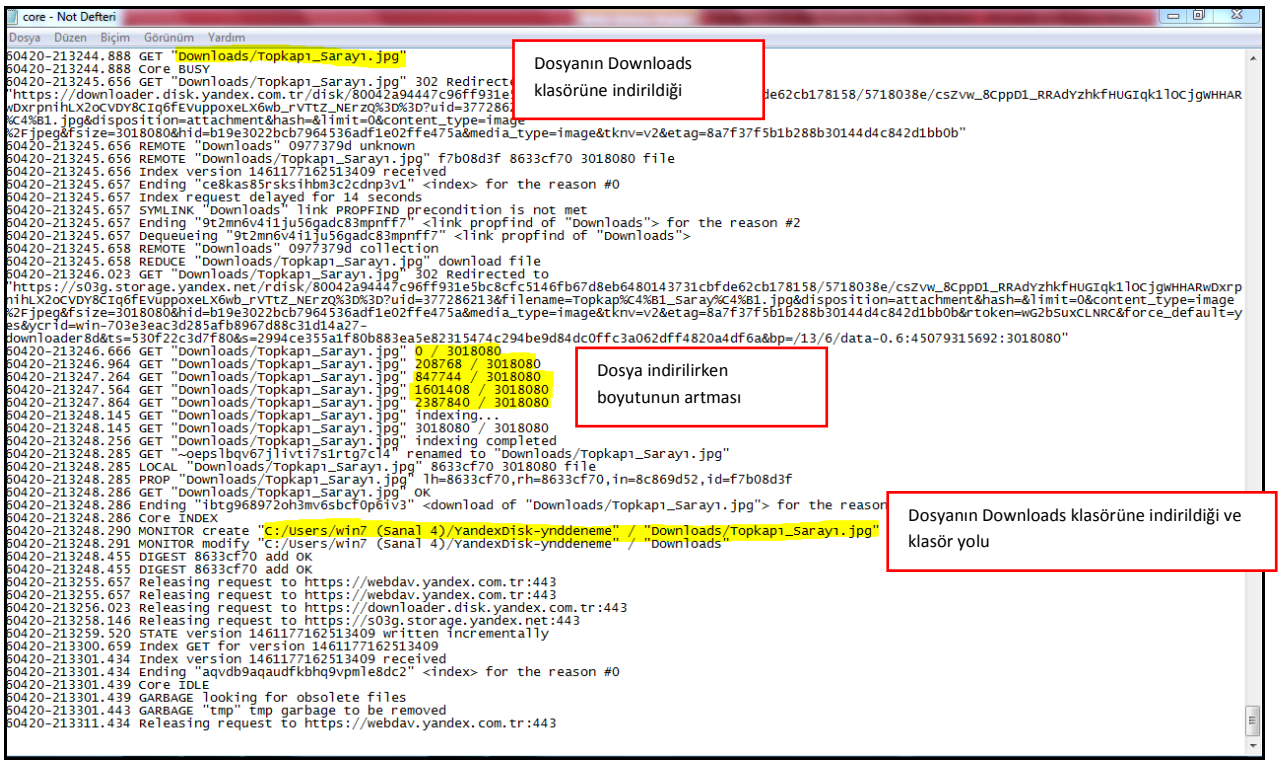
Şekil 26: Yeni oluşan "Downloads" klasörü



Şekil 27: Bilgisayarda birden fazla oturum açıldığında klasör yapısı



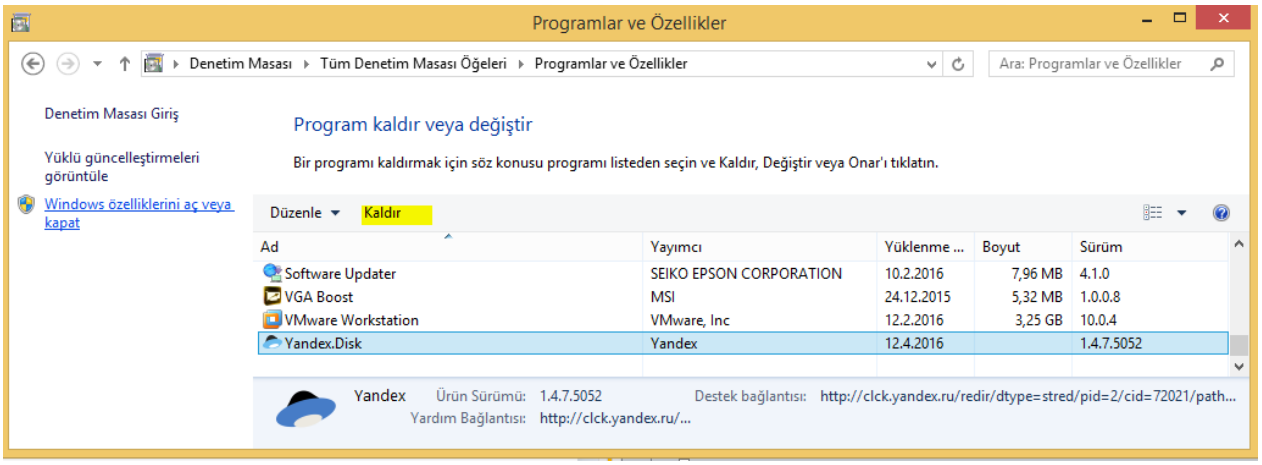
Şekil 28: Bilgisayarda birden fazla oturum açıldığında users_settings.dat



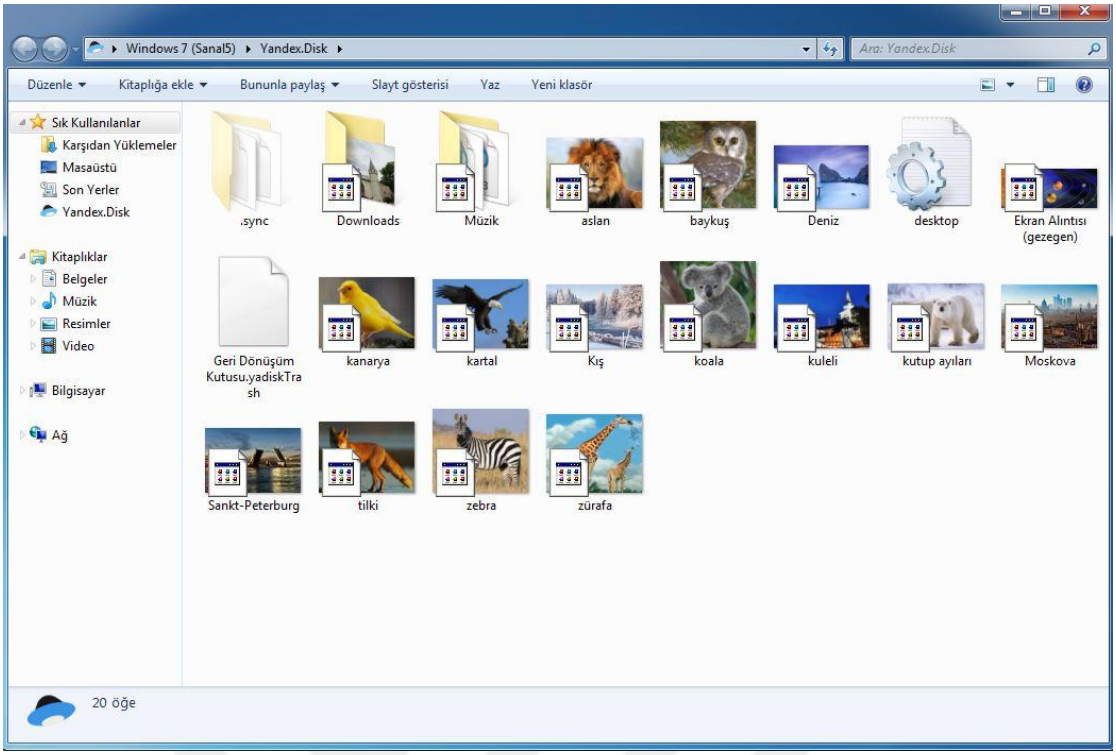
Şekil 29: Dosya indirildiğinde core.log dosyasındaki değişiklikler

Şekil 30: Dosya indirildiğinde push.log dosyasındaki değişiklikler

4.5 Uygulama kaldırıldığında tespit edilen veriler



Şekil 31: Yandex.Disk uygulamasının kaldırılması



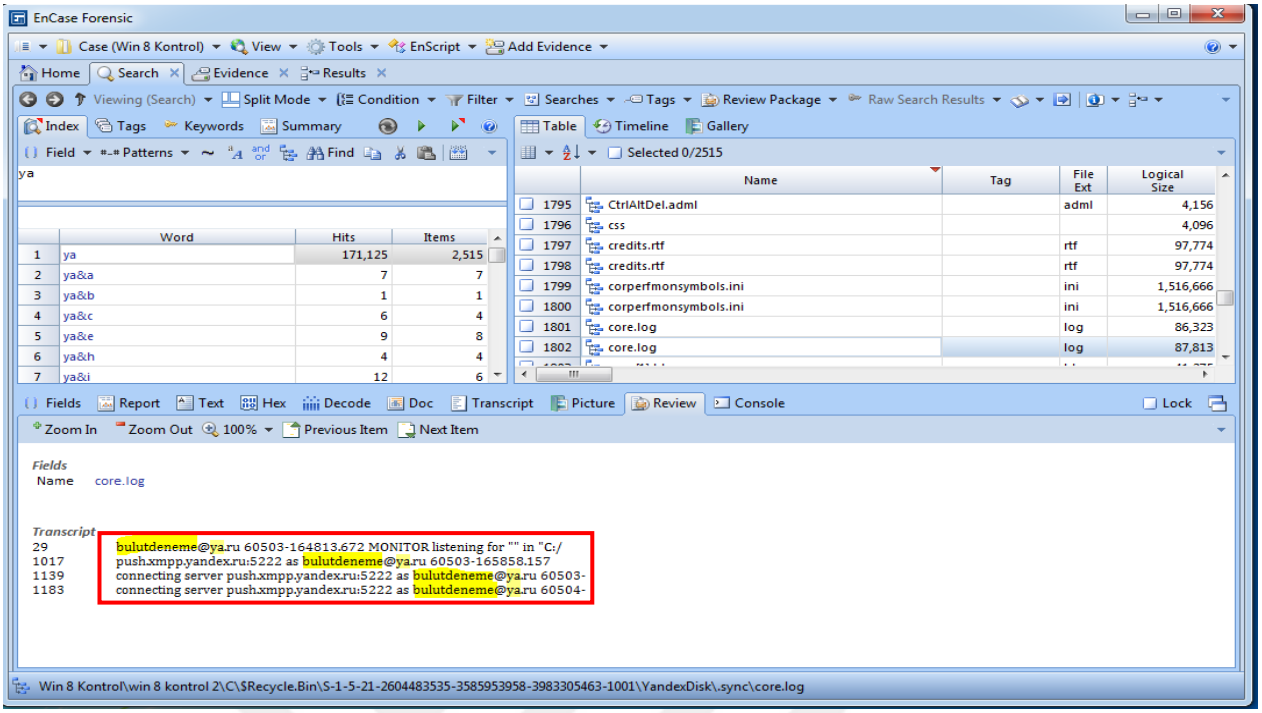
Şekil 32: Uygulama kaldırıldıktan sonraki tespitler Yandex.Disk klasörü

Tespit Edilecek Veri	Bulunabilecek Dosya	Aranacak Anahtar Kelimeler
Oturum Açma Adı	Core.log dosyası içeriğinde	Oturumaçmaadı**@ya.ru**
	Config.xml dosyası içerisinde	**<LastLogin>** Oturumaçmaadı **</LastLogin>**
	Çerez (Cookies dosyasında)	**yandex_login** Oturumaçmaadı
Oturum Açma Zamanı ile ilgili yapılacak değerlendirme	Gui.log içerisinde	**60412-121439 Auth Start Login :** Oturum Açma Adı Oturum Açma Adı Oturum Açıldığı Zaman : 60412-121439 **12 Nisan 2016 saat 12:14:39** **(Oturum açıldığı zaman)**
	Core.log	**60412-121659.819 Starting (1.4.7.5052)** **(Programın çalıştığı zaman bilgisi)**

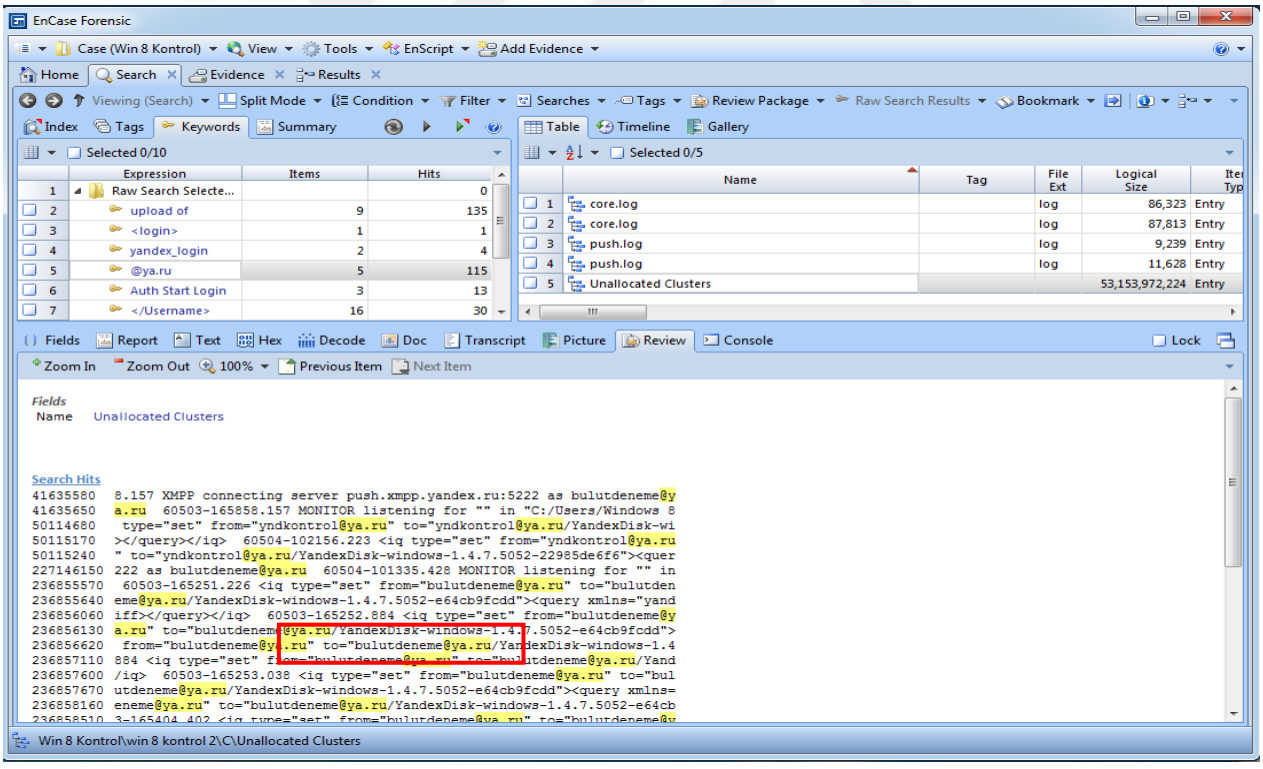
Tespit Edilecek Veri	Bulunabilecek Dosya	Aranacak Anahtar Kelimeler
	içerisinde	
Kullanıcı Adı	Config.xml dosyası içerisinde	**<Username>**Kullanıcı Adı**</Username>**
Yüklenen Dosya adı	Push.log dosyası içerisinde	**<upload of "**dosya adı**"**
Yüklenen/paylaşılan dosyaların algoritma imzaları	Push.log dosyası içerisinde	**sha256="**e440f858f9dd46f5f1310ce4099b6e61cb0f44b6d71c105d53ae617c4bd68621 **md5="**280bda61768fdc3d7e079e6e107badd2
Dosyaların paylaşıma açılıp açılmadığı	Push.log dosyası içerisinde	**type="**published
	Gui.log içerisinde	**OnShareFile(**

Tablo 7. Yandex.Disk uygulamasının incelenmesinde kullanılabilecek anahtar kelimeler

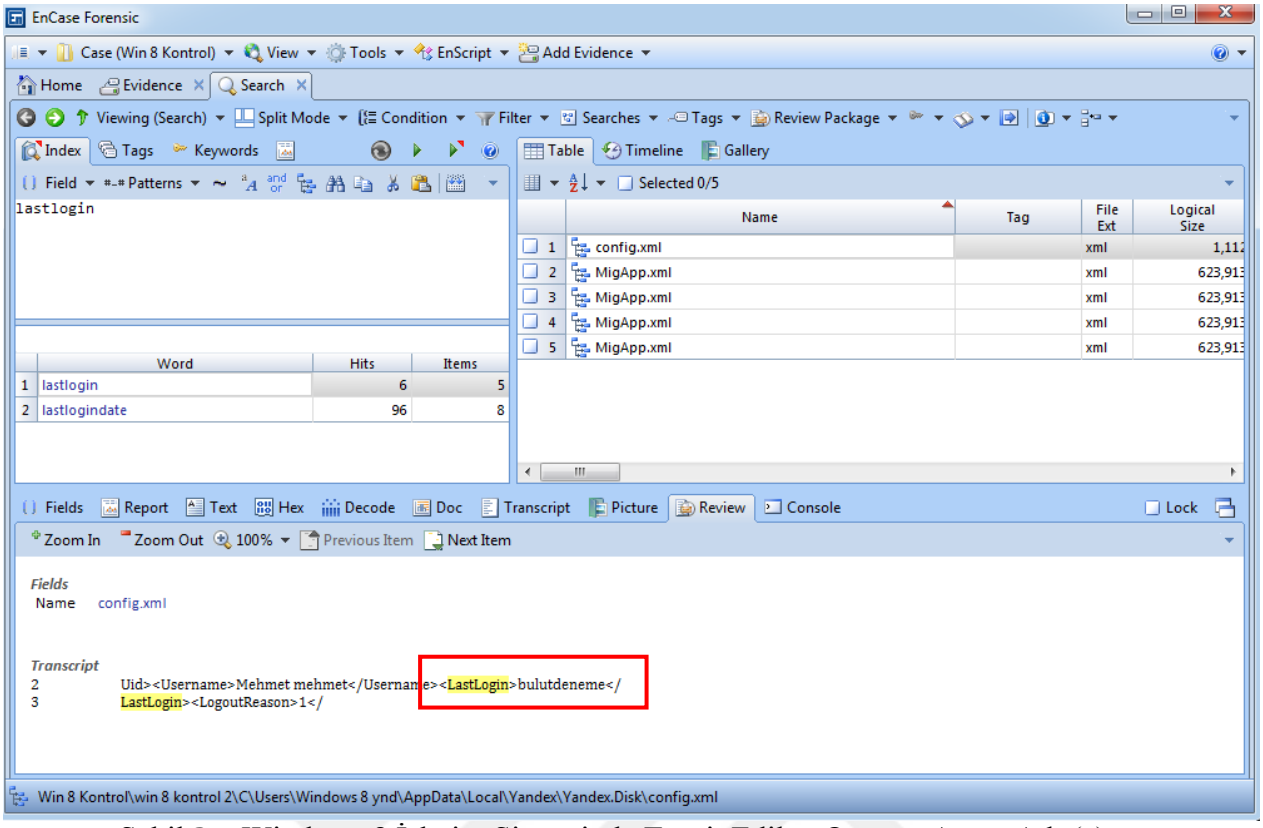
4.6 Yöntemin farklı bir işletim sisteminde test edilmesi sonucu tespit edilen veriler



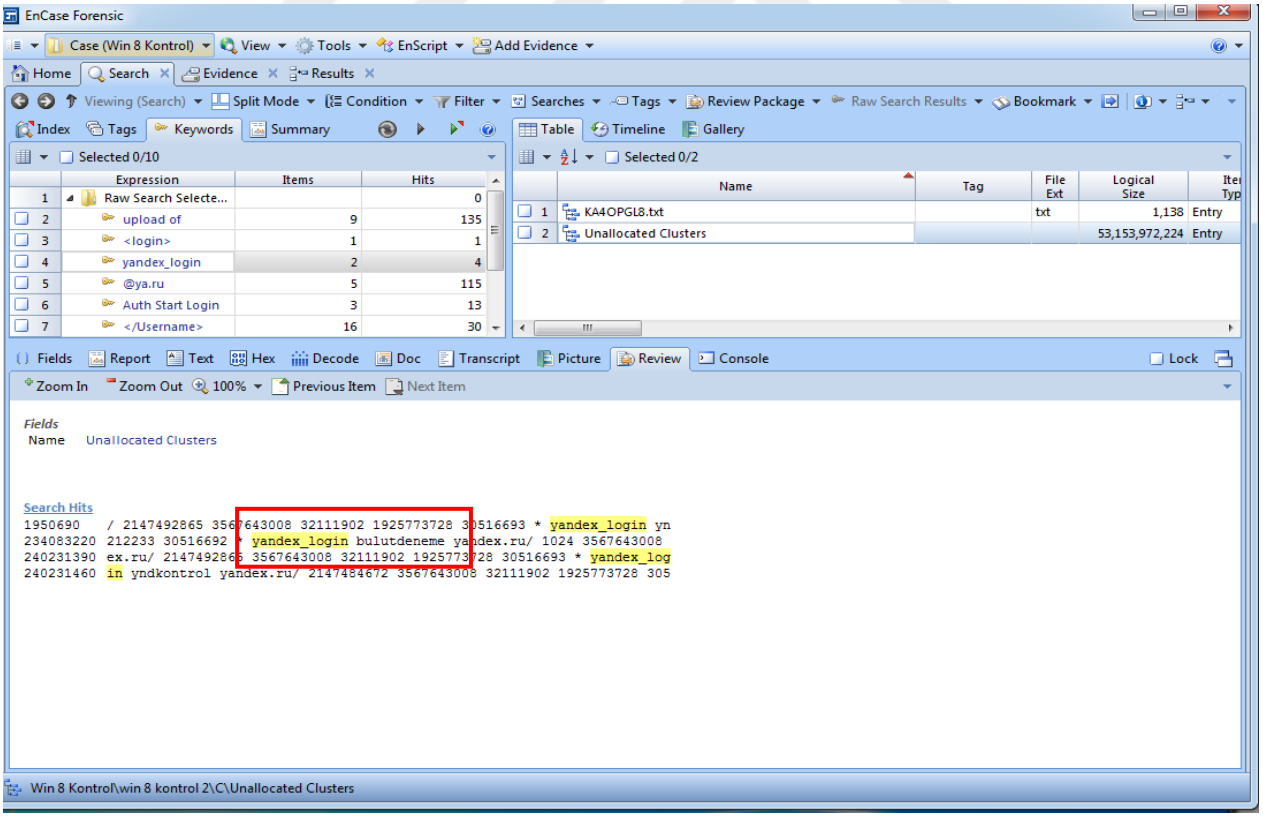
Şekil 33: Windows 8 İşletim Sisteminde Tespit Edilen Oturum Açma Adı (a)



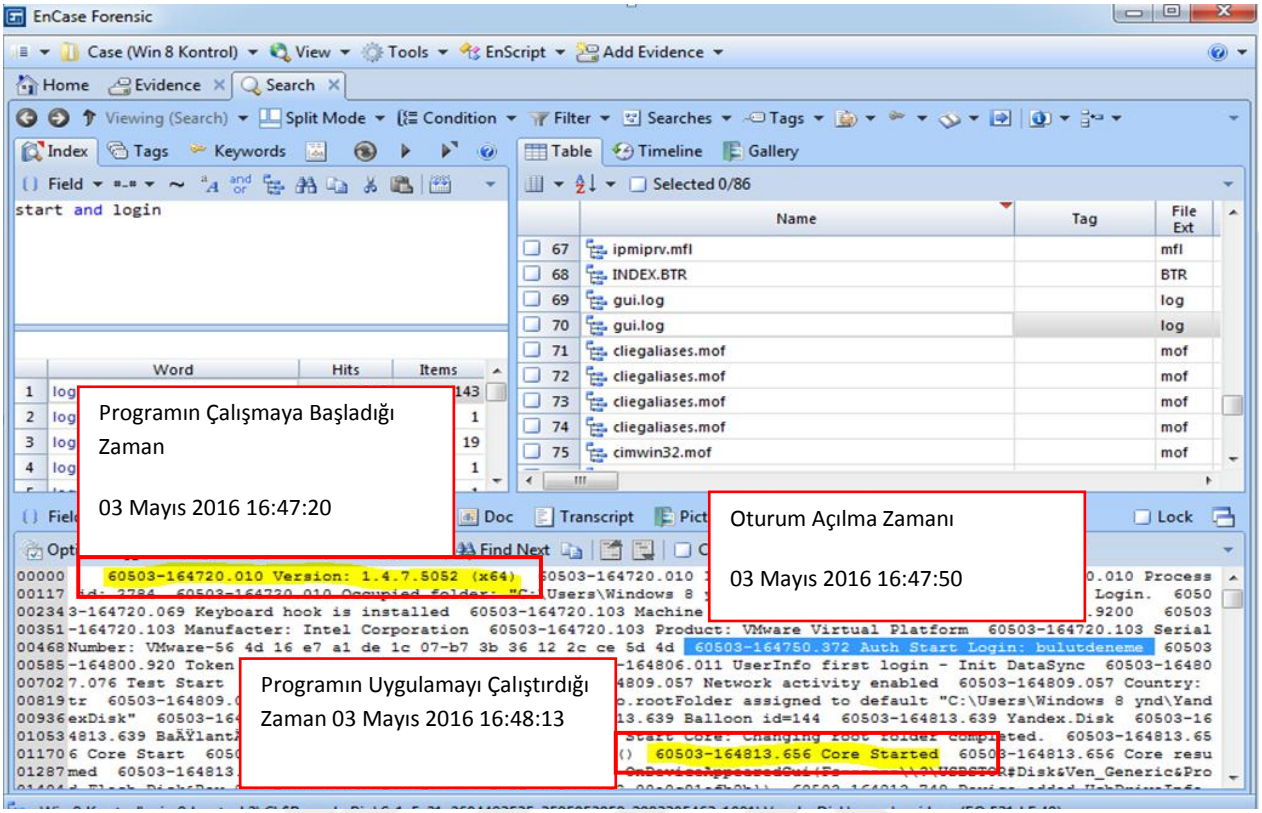
Şekil 34: Windows 8 İşletim Sisteminde Tespit Edilen Oturum Açma Adı (b)



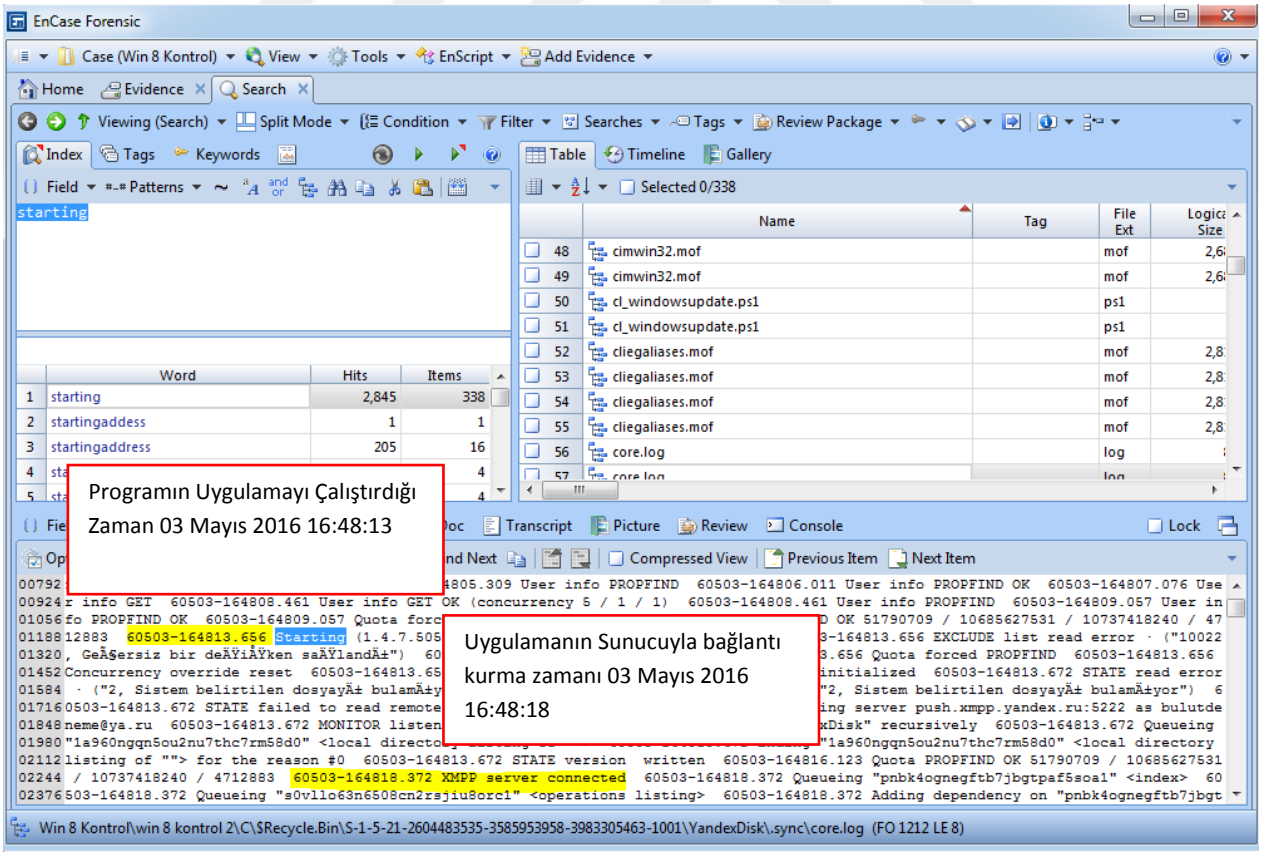
Şekil 35: Windows 8 İşletim Sisteminde Tespit Edilen Oturum Açma Adı (c)



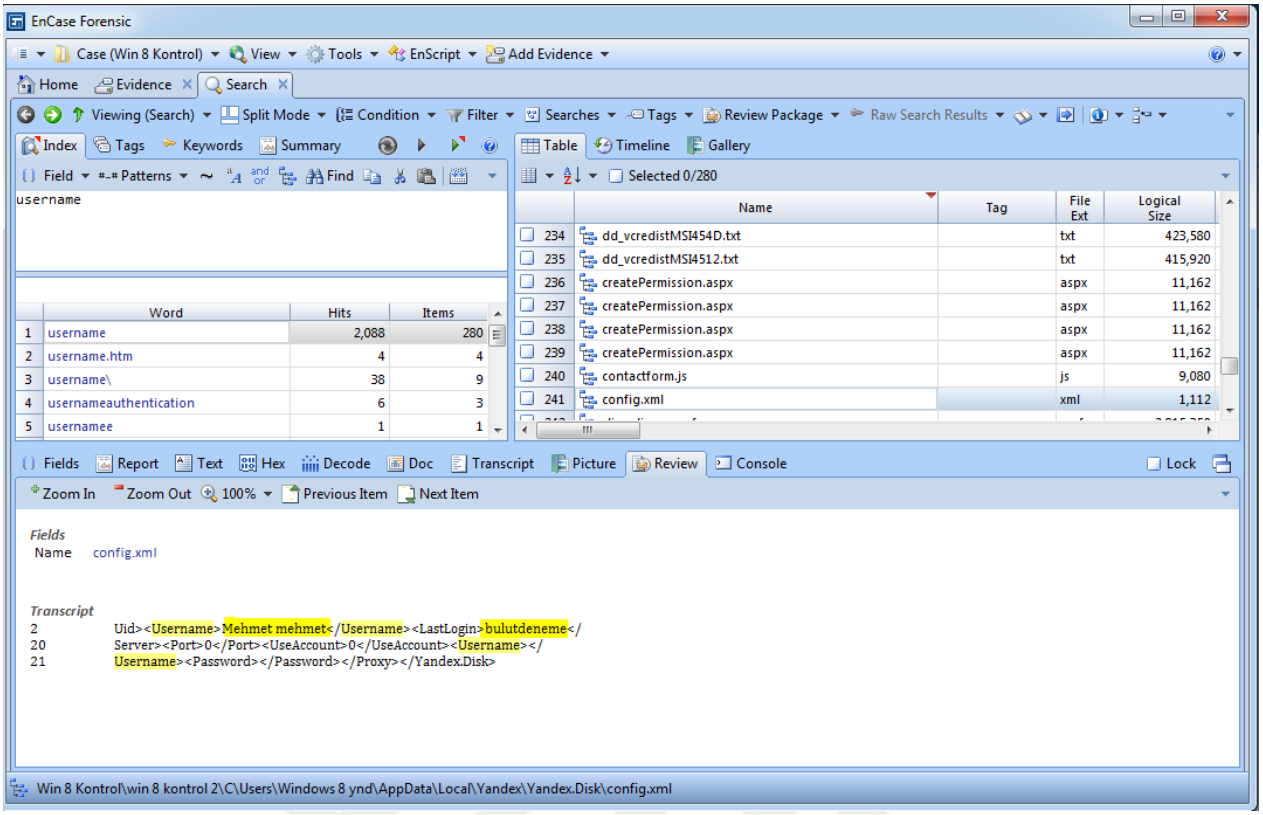
Şekil 36: Windows 8 İşletim Sisteminde Tespit Edilen Oturum Açma Adı (d)



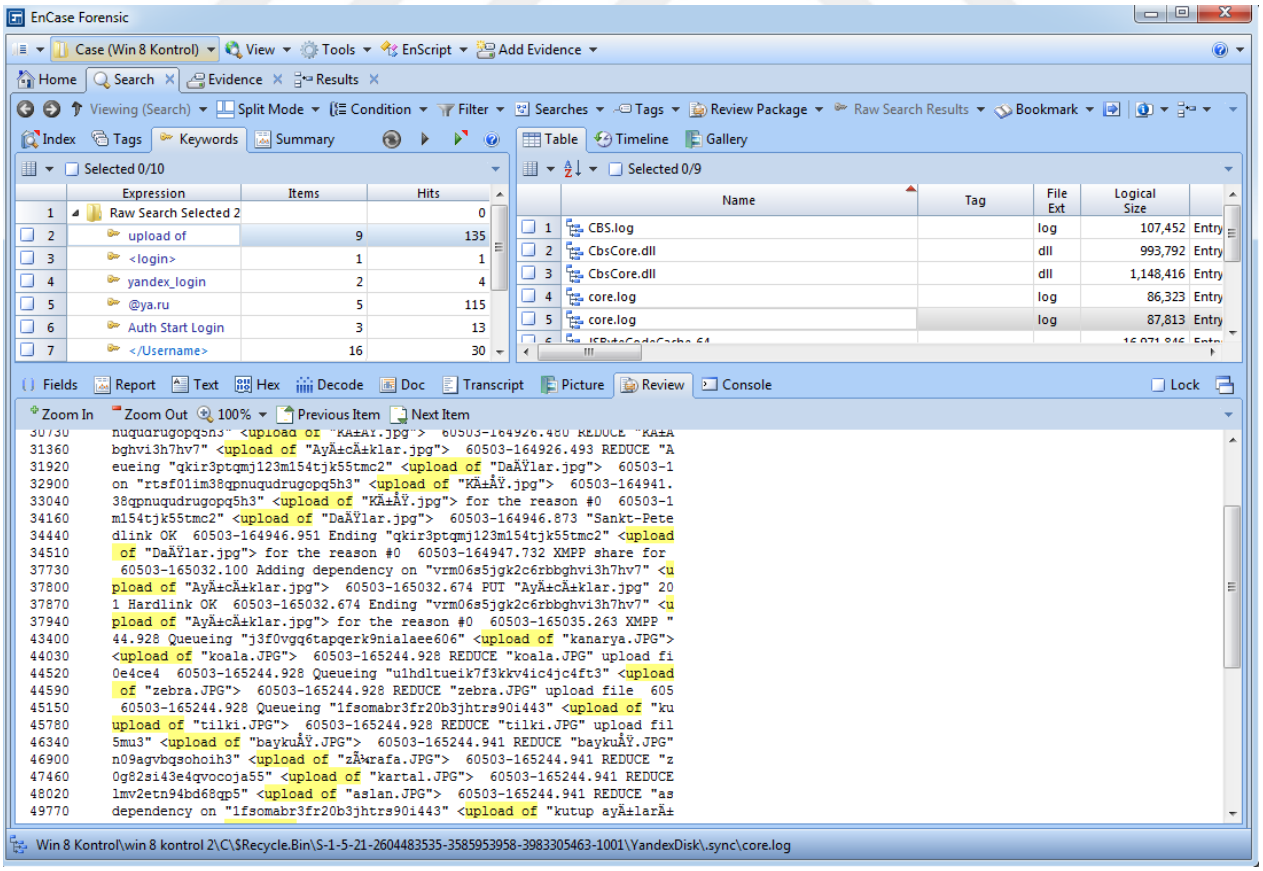
Şekil 37: Windows 8 İşletim Sisteminde Tespit Edilen Oturum Açma Zamanı (a)



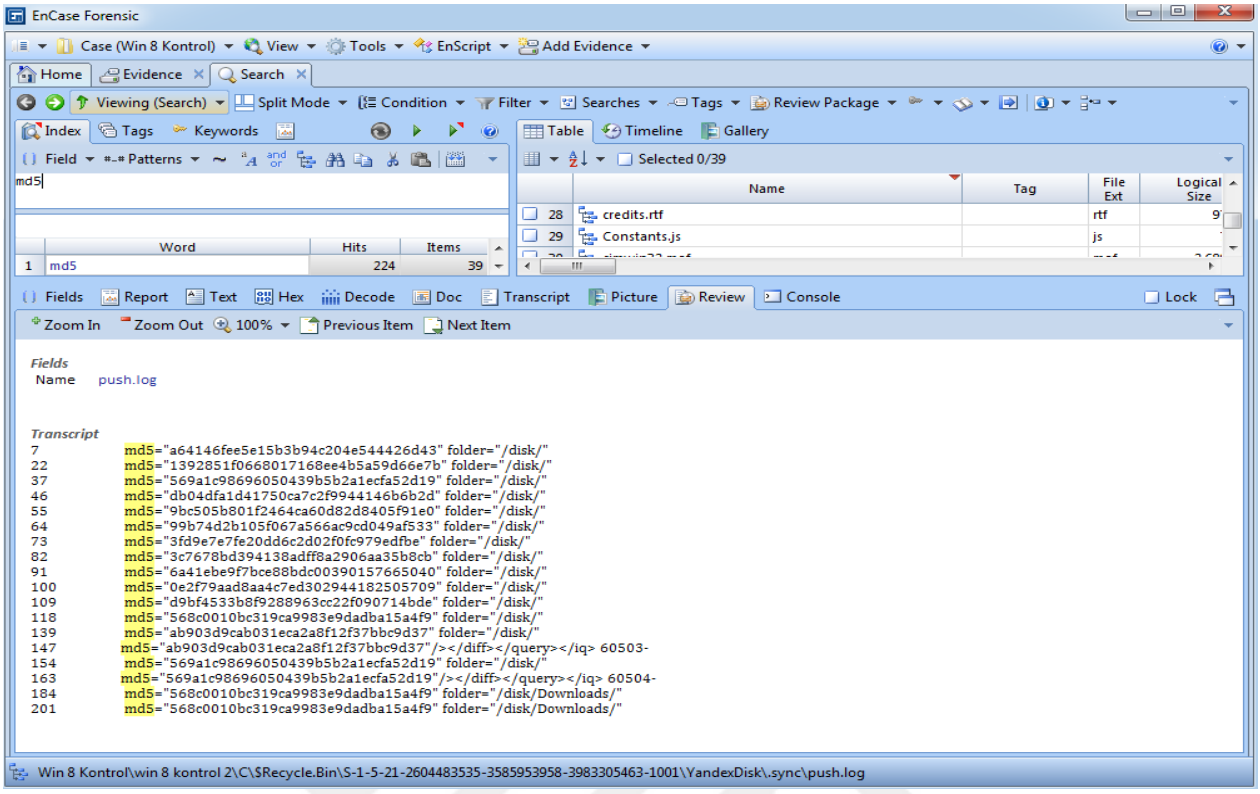
Şekil 38: Windows 8 İşletim Sisteminde Tespit Edilen Oturum Açma Zamanı (b)



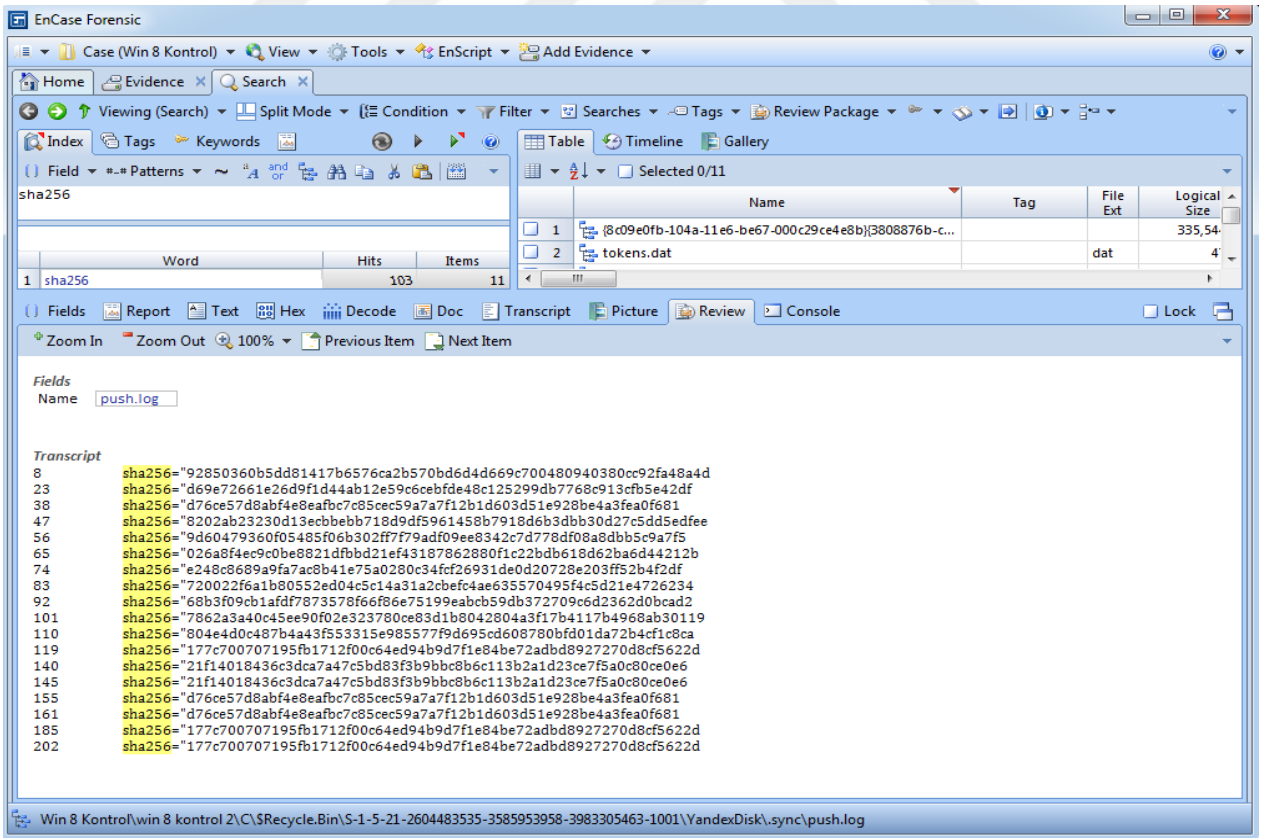
Şekil 39: Windows 8 İşletim Sisteminde Tespit Edilen Kullanıcı Adı



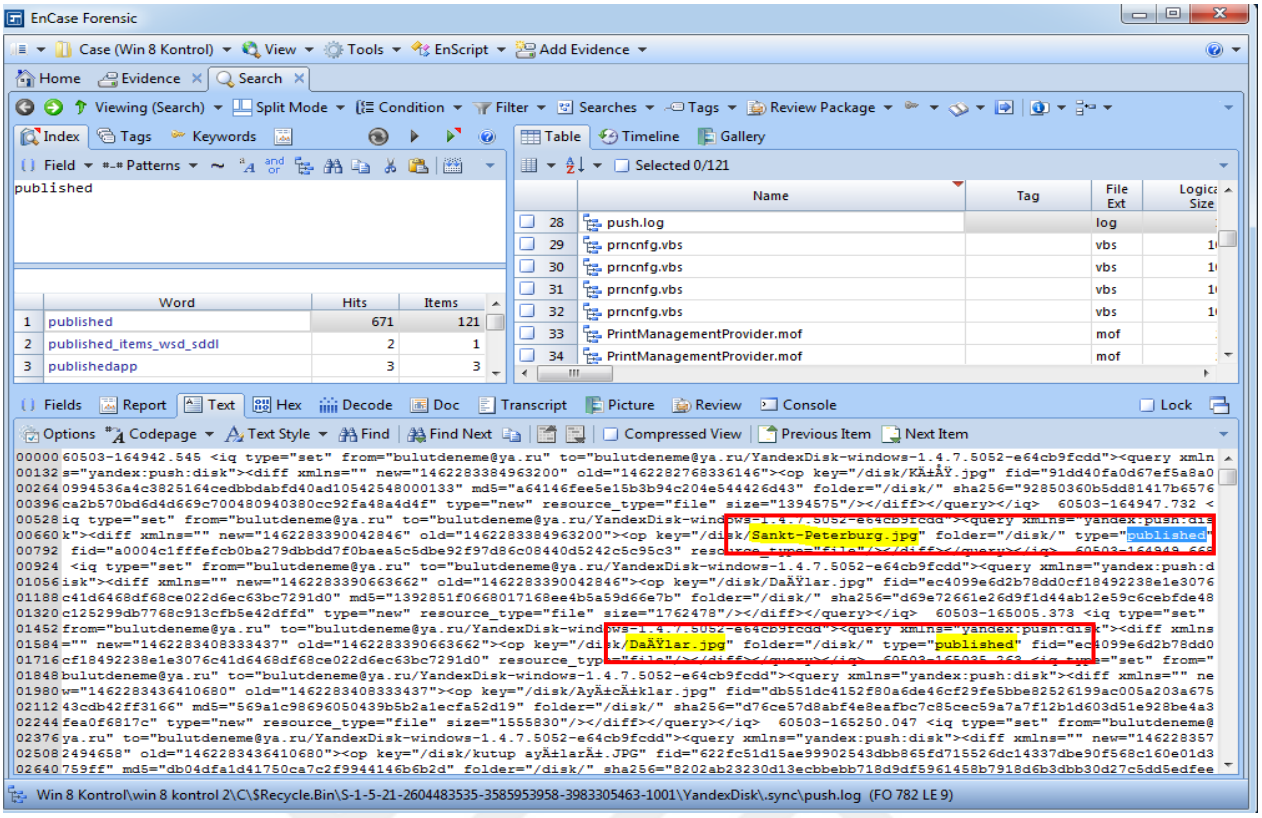
Şekil 40: Windows 8 İşletim Sisteminde Tespit Edilen Yüklenen Dosya İsimleri



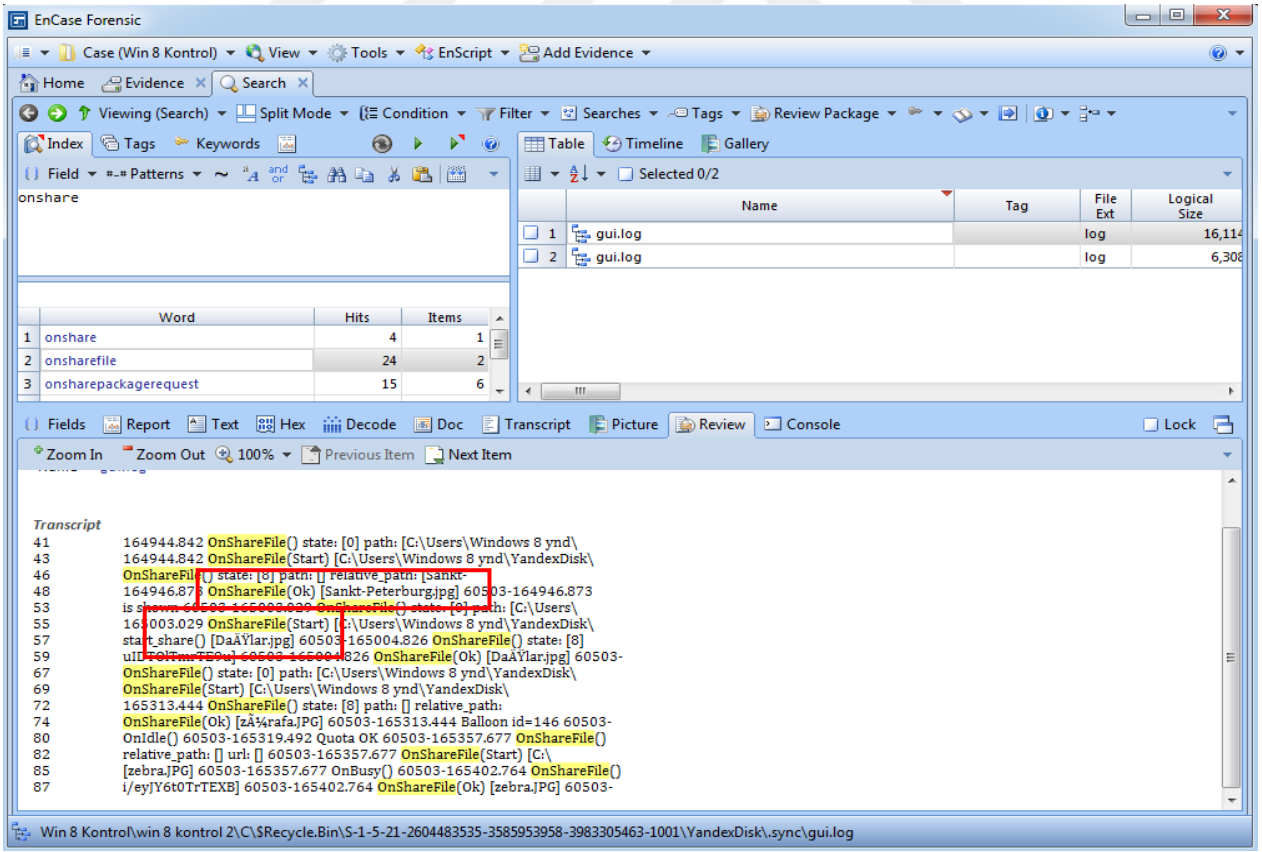
Şekil 41: Yüklenen Dosyaların MD5 Algoritma İmzaları (a)



Şekil 42: Yüklenen Dosyaların SHA256 Algoritma İmzaları (b)



Şekil 43: Paylaşıma Açılan Dosyalar (a)



Şekil 44: Paylaşıma Açılan Dosyalar (b)

Tespit Edilecek Veri	Aranacak Anahtar Kelimeler	Tespit Edilen Veri
Oturum Açma Adı	bulutdeneme**@ya.ru**	Şekil 33. Şekil 34.
	<LastLogin> Oturumaçmaadı **</LastLogin>**	Şekil 35.
	yandex_login bulutdeneme	Şekil 36.
Oturum Açma Zamanı ile ilgili değerlendirme	**60503-164750 Auth Start Login :** bulutdeneme Oturum Açma Adı :bulutdeneme Oturum Açıldığı Zaman : **03 Mayıs 2016 saat 16:47:50**	Şekil 37.
	60503-164813.656 Starting (1.4.7.5052)	Şekil 38.
Kullanıcı Adı	**<Username>**Mehmet mehmet**</Username>**	Şekil 39.
Yüklenen Dosya adı	**<upload of "**kanarya.JPG**"** **<upload of "**tilki.JPG**"** **<upload of "**kartal.JPG**"** **<upload of "**aslan.JPG**"**	Şekil 40.
Yüklenen/paylaşılan dosyaların algoritma imzaları	**sha256="**e440f858f9dd46f5f1310ce4099b6e61cb0f44b6d71c105d53ae617c4bd68621 **md5="**db04dfa1d41750ca7c2f9944146b6b2d	Şekil 41. Şekil 42.
Dosyaların paylaşıma açılıp açılmadığı	Sankt_Petersburg.JPG **type="**published Dağlar.jpg **type="**published	Şekil 43.
	OnShareFile(Ok) [Sankt_Petersburg.JPG] **OnShareFile(**Ok) [Dağlar.jpg]	Şekil 44.

Tablo 8. Encase 7.06 programı ile yapılan test sonucu tespit edilen veriler

5. TARTIŞMA VE SONUÇ

Bulut bilişim bilgisayarlara ait kaynakların internet üzerinden kullanımına dayalı bir bilişim modeli olması sebebiyle, klasik adli bilişim yazılımları ve donanımları ile bulut bilişimde delil toplamanın bazı teknik ve hukuki sorunları bulunmaktadır.

Bulut bilişim uygulamalarında adli bilişim boyutuyla delil elde edilebilecek iki nokta bulunmaktadır. Biri servis sağlayıcıya ait bulut depolama alanı olarak hizmet veren uzaktaki sunucu bilgisayarlar (yedekleme sunucuları dahil) diğeri ise yerel kullanıcı bilgisayarıdır.

Ülkemizde bilgisayarlardan delil elde etmek amacıyla arama, kopyalama ve el koyma işlemi 5271 sayılı Ceza Muhakemesi Kanununun 134'üncü maddesi kapsamında yapılmaktadır. Ayrıca Adli ve Önleme Aramaları Yönetmeliği'nin 17'nci maddeside arama ve el koymanın nasıl yapılacağına dair ayrıntılı açıklamalarda bulunmuştur (36). Bu kararla el konulan şüpheliye ait bilgisayarın dışında bulut depolama alanından iki şekilde delil elde edilebilir ya servis sağlayıcıdan istenilen veriler talep edilebilir, ya da bu alana uzaktan erişerek (kullanıcı şifresiyle erişim sağlayıp uzaktan birebir kopyalama ya da şifreyle oturum açarak delilleri tespit vb.) delilleri kendimiz toplayabiliriz. Kendi hukuk sistemimiz dahilindeki bir mahkemeden alınacak arama kararı ülkemiz yargı sınırları dışındaki bir bulut depolama alanına (sunucu bilgisayara) erişime yetki vermemektedir. Bu konuda mevcut mevzuat çerçevesinde istinabe yoluyla ilgili ülkenin adli birimlerinden yardım alınmaktadır[9]. Ayrıca Avrupa Konseyi Siber Suç Sözleşmesi taraf olan devletler nezdinde uluslararası işbirliğini kolaylaştırmış olmasına rağmen ülkeler suç tanımları konusunda uzlaşı sağlamadıklarından ülkemizde suç olan bir eylem başka bir ülkede suç sayılmayabilmektedir[10]. Servis sağlayıcılar da müşterileri hakkında işbirliğine sıcak bakmamaktadırlar ve istenilen verileri sağlayabilecek yeterli alt yapı ve uzman personele sahip olmamaları soruşturmaların yürütülmesinde sıkıntılara yol açmaktadır.

Yasal süreçlerin dışında bulut bilişim sistemlerinden delil elde etme konusunda bir takım teknik zorluklarda bulunmaktadır. Klasik adli bilişimde delil elde edilecek bilişim sistemine

[9] http://www.uhdigm.adalet.gov.tr/adli_yardimlasma/adli_isbirligi_ceza/cz_istinabe_9_internet_ortaminda_islenen_suclar.html [Erişim Tarihi: 20.04.2016]

[10] Türkiye tarafından 2010 yılında imzalanan Avrupa Konseyi Siber Suç Sözleşmesi 22 Nisan 2014 tarihli ve 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Uygun Bulunduğuna Dair Kanun ile onaylanmış ve 02 Mayıs 2014 tarihinde yürürlüğe girmiştir. [Erişim Adresi: https://www.tbmm.gov.tr/develop/owa/kanunlar_gd.durumu?kanun_no=6533] [Erişim Tarihi:20.04.2016]

genellikle fiziksel olarak el konulmuştur. Bu sistemden delil elde etmek amacıyla bu amaçla geliştirilmiş delile zarar vermeyen, değişikliğe uğramasını engelleyen donanım ve yazılımlar kullanılmaktadır. Bulut sistemlerden delil elde edilmesinde ise delillere zarar verilmediğini kanıtlayan genel kabul görmüş ve test edilmiş yazılım ve donanımlar bulunmamaktadır.

Klasik adli bilişimde geliştirilen yöntemler sayesinde elektronik deliller mahkemelerde son dönemde kabul görmeye başlamıştır ve bu delillerin bilimsel olarak doğruluğu tekrarlanabilen deneylerle kanıtlanabilmektedir. Halihazırda bulut depolama alanından delil elde etmeye yönelik birebir kopya alma amacıyla uzaktaki bir sunucuya erişim sağlandığında bu alandaki verilerin değişmediğini, bütünlüğünün bozulmadığını, başka bir kullanıcının alanına müdahale edilmediğini kesin olarak saptamak mümkün görünmemektedir (27).

Bulut Bilişim ile ilgili ülkemizde yapılan çalışmalara bakıldığında adli bilişim boyutuyla bulut sistemlerinden delil elde edilmesine yönelik uygulama içeren bir çalışmaya rastlanılmamıştır. Yapılan literatür çalışmasında Oktay tarafından bulut sistemlere yönelik siber saldırı konusunda bir tez çalışması yapıldığı (25), Sevli ve Küçüksille'nin (58) çalışmalarında bulut ortamında adli bilişimle ilgili karşılaşılan sorunlar ve uygulanabilecek yöntemleri belirttikleri görülmüştür (58).

Yurtdışında yapılan çalışmalara bakıldığında Chung ve ark. (55) tarafından 4 farklı servis sağlayıcıya ait bulut bilişim depolama uygulamalarının (*Amazons3, Google Docs, Dropbox ve Evernote*), Hale (59) tarafından Amazon şirketine ait Amazon Bulut Depolama uygulamasının, Quick ve Choo (60),(61) tarafından Dropbox uygulamasıyla Microsoft Skydrive uygulamalarının incelendiği görülmüştür. Uyguladığımız inceleme yöntemine benzer olarak internet geçmişi, log kayıtları, klasör yapıları incelenmiş ve kullanıcı adları, yüklenen ve paylaşılan dosyalar ve bunların algoritma imzalarının tespit edilebildiği görülmüştür. Ancak bu çalışmalardan bazılarında bilgisayar üzerinde tespit edilebilecek olan kullanıcı şifresiyle oturum açılarak bulut depolama alanından delil toplanması önerildiğinden daha önce ifade edilen hukuki sorunlar nedeniyle çalışmamızda bu yöntemler uygulanmamıştır. Ayrıca bu çalışmalarda delil içerebilecek dosyaların neler olduğu ortaya konulmuş ancak dosyaların silinmiş olduğu durumlarda içerdikleri verilere silinmiş alanlardan ulaşabilmek için kullanılabilecek anahtar kelimelere yer verilmemiştir. Tablo 7'de örnek olarak kullandığımız Yandex.Disk uygulamasının delil içerebilecek dosyaları (oturum açma adı, içerdiği dosyalar, dosyaların yükleme ve paylaşıma açılma bilgileri vb.) ile bu dosyalara

ait içeriklere bilgisayarın silinmiş alanlarından da ulaşabilmek için kullanılabilecek anahtar kelimeler verilmiş olup bu sayede Yandex.Disk uygulaması kullanan bir bilgisayarda yapılacak adli incelemede aranılan verilere hızlı ve kolay bir yöntemle ulaşılabileceği değerlendirilmektedir.

Bu çalışmada internet üzerinde veri depolama hizmeti veren bulut bilişim depolama uygulamalarını kullanan bilgisayarlarda suç konusu bir soruşturma üzerine yapılan incelemelerde hangi verilerin tespit edilebileceği araştırılmıştır. Bulut bilişim depolama alanında bulunan ve suç unsuru taşıyan bir içerik ile soruşturma kapsamında el konulan bir bilgisayar arasında bağlantı kurabilmek için oluşturulan soruların cevaplarına ulaşmak için için yapılan incelemelerde;

Örnek olarak seçtiğimiz Yandex.Disk uygulaması kurulduktan sonra bilgisayardaki klasör yapısı incelenmiş ve Tablo 5'teki dosyaların yandex uygulamasıyla ilişkili olduğu değerlendirilmiş bu klasörler ve dosyalar üzerinde yapılan incelemede (bulgu 4.1),

- **C:\Users\<Kullanıcı Adı>\YandexDisk**
- **C:\Users\<Kullanıcı Adı>\AppData\Local\Yandex\YandexDisk**

klasörleri altında Yandex.Disk uygulamasına ait kurulum dosyalarının oluştuğu görülmüş;

Ayrıca uygulama kurulmadan önceki ve sonraki bilgisayarlarda tüm dosyaların algoritma imzaları karşılaştırıldığında 1045 dosyada değişiklik görülmüş bunlardan Yandex.Disk kullanımıyla ilgili veri ihtiva ettiği değerlendirilen Tablo 6'daki dosyalar incelenmiştir.

- **"users_settings.dat"** dosyasında Oturum Açma Adı, Kurulum Dosyasının Klasör Yolu (Şekil 9)
- **"config.xml"** dosyasında Oturum Açma Adı, ilk giriş yapan Kullanıcı Adı, Toplam Depolama Alanı, Kullanılan Depolama Alanı Boyutu (Şekil 10)
- **"core.log"** dosyasında Oturum Açma Adı, Kurulum dosyalarının klasör yolu ve bilgisayar adı, Diskin toplam boyutu ve ne kadarının kullanıldığı, İçeriğinde Bulunan Dosyaların Adları ve Boyutları, İndirilen ve Yüklenen Dosyaların Adları, Dosyaların İndirilme ve Yüklenme Zamanları, Algoritma İmzaları (Şekil 11,12,13)
- **"gui.log"** Oturum Açma Adı, Oturum Açıldığı Zaman, Oturum Açılan Bilgisayarla ilgili bilgiler (Şekil 14)
- **"Cookie Dosyaları"** Oturum Açma Adı (Şekil 15) tespit edilebilmiştir.

Birden fazla kullanıcının oturum açtığı bilgisayarda sadece ilk giriş yapan kullanıcının kullanıcı ismi tespit edilebilmiştir. (config.xml dosyası içerisinde sadece ilk giriş yapan kullanıcıya ait kullanıcı adı bilgisi tutulmaktadır.)

Bilgisayarların uygulama kurulmadan önceki ve sonraki kayıt defterlerinde yapılan analiz ve karşılaştırma neticesinde Yandex.Disk'in uygulama adı, kurulan klasör yolu ve versiyon numarası tespit edilebildiği görülmüştür (Şekil 16-17).

Tablo 4'te yüklenen dosyalar eşitlendikten sonra dosyaların isimleri ve algoritma imzaları sanal bilgisayarlar üzerinde Encase 6.19.1 programı ile anahtar kelime olarak aratılmış 12 adet dosyada bulunduğu görülmüş (Şekil 18) *"$LogFile, $MFT, $UsnJrnl·$J"* gibi sistem dosyalarının yanında (bulgu 4.2);

- **core.log** dosyası
- **push.log** dosyası ve
- **YandexDisk** klasör indeksinin içeriğinde tespit edilmiştir.

Bir önceki aşamada uygulama kurulurken oluşan dosyalardaki değişiklikler dosyalar bulut depolama alanına yüklendikten sonra tekrar kontrol edildiğinde,

- **"gui.log"** dosyasında işlem yapılan sürelerde uygulamanın kendi işleyişiyle ilgili işlevlerin kaydedildiği ve bunlarla ilgili zaman bilgisinin bulunduğu yüklenen dosyalarla ilgili bir bilgi bulunmadığı,
- **"core.log"** dosyasında yüklenen dosyaların adı ve boyutu, yüklenme zamanı bilgilerinin oluştuğu, Yandex.Diskin en son durumunun Unix zaman formatında versiyon olarak kaydedildiği (Şekil 19),
- **"push.log"** dosyası ilk kurulum esnasında boş olarak tespit edilmiş iken, dosyalar yüklendikten sonra içeriğinde işlemlerin yapılma zamanı (dosya yükleme) bilgisi, içeriğinde bulunan dosyaların adı, boyutu (byte olarak) ve algoritma imzaları (MD5 ve SHA256), oturum açma adı (ynddeneme), yandex uygulamasının versiyon numarası oluştuğu görülmüştür (Şekil 18,20).

Tarih zaman bilgilerinden açık formatta yazılan zaman bilgisi, bilgisayarın tarih zaman bilgisini kaydettiği görülmüş ve kullanıcı tarafından bilgisayarın tarih zamanı değiştirildiğinde değiştiği tespit edilmiştir. Versiyon olarak kullanılan zaman bilgisi ise bilgisayarın tarih zamanı değiştirildiğinde değişmemektedir.

Dosyalar paylaşıma açılırken hem Yandex.Disk uygulaması hem de internet tarayıcı kullanılabilmektedir. Paylaşımda olan bir dosya ise ancak internet tarayıcı üzerinden bilgisayara indirilebilmekte ya da Yandex.Disk alanına kaydedilebilmektedir (bulgu 4.3).

Örnek olarak "Tilki.jpg" dosyası paylaşıma açıldıktan sonra paylaşım adresi "https://yadi.sk/i/TA-KEW6Rr8ddb" olarak görülmüştür. Bu paylaşım adresi dosyayı paylaşımdan kaldırıp tekrar paylaşıma açtığımızda değişmektedir. Bu adresle dosyanın ilişkisi paylaşımda olduğu sürece devam etmektedir. (Şekil 21)

Bu paylaşım adresini herhangi bir internet tarayıcının adres satırına girdiğimiz takdirde bu dosyaya ulaşabilmektedir. Bunun için Yandex.Disk'te bir oturum açmak gerekmemektedir. Eğer paylaşıma açan kullanıcının haricinde üçüncü bir kişinin açtığı bir oturumda veya oturum açılmadan bu adrese ulaşıldığında bu dosyayı paylaşan kişinin kullanıcı adı (Sahip:ibbali) şeklinde Şekil 21'deki gibi görülmektedir.

Kurulum dosyalarında yapılan incelemede;

- **Core.log** dosyasında "https://yadi.sk/i/TA-KEW6Rr8ddb" paylaşım adresi ve paylaşılan dosyanın adı paylaşıma açıldığını belirten bir kelime (<sharing of "tilki.JPG") (Şekil 22),
- **Push.log** dosyasında "tilki.JPG" dosyasının paylaşıldığı (published) bilgisi (Şekil 23)
- **Gui.log** dosyasında paylaşılan dosya adı "tilki.JPG", dosyanın paylaşıldığı bilgisi (start_share) ve "https://yadi.sk/i/TA-KEW6Rr8ddb" paylaşım adresi tespit edilmiştir. (Şekil 24)

Yandex.Disk üzerinde bulunan bir dosya indirilirken kullanılan internet tarayıcının ekran görüntüsü Şekil 25'te görülmektedir. Ekran görüntüsünde dosya adı ve boyutu, paylaşım adresi ve sahibi bilgileri görülmektedir (bulgu 4.4).

Dosya indirildiği zaman **C:\Users\<Kullanıcı Adı>\YandexDisk** klasör yolu altında **Downloads** isimli bir klasör oluştuğu bu klasörün ilk kurulumda oluşmadığı ilk defa dosya indirildiğinde otomatik olarak oluştuğu görülmüştür (Şekil 26). Yapılan incelemelerde dosyayı paylaşan kişinin dışında bir kullanıcı bu dosyayı bilgisayarına indirdiğinde, bu kişinin bir Yandex.Disk uygulaması mevcutsa ve oturumu açıksa **C:\Users\<Kullanıcı Adı>\YandexDisk\Downloads** klasörü altına kaydedilmekte, Yandex.Disk uygulaması yoksa veya oturumu açık değilse bilgisayarında bulunan ve internetten indirilen diğer tüm dosyaların ön tanımlı olarak kaydedildiği **C:\Users\<Kullanıcı Adı>\Downloads** klasörünün altına kaydedilmektedir.

Farklı bir hesapla oturum açıldığı takdirde bilgisayarda yeni bir "YandexDisk" klasörü oluştuğu ve diğer hesaptan ayrılması amacıyla sistem dosyaları olan gui.log, core.log ve push.log **C:\Users\<Kullanıcı Adı>\YandexDisk-ynddeneme\.sync** klasörü altında yeni oturumla ilgili bilgileri saklamak için oluştuğu görülmüştür (Şekil 27). Ayrıca users_settings.dat dosyasında kullanılan tüm oturum açma adlarının kaydedildiği tespit edilmiştir (Şekil 28).

- **Core.log** dosyasında dosyanın indirildiği bilgisi (GET "Downloads/Topkapı_Sarayı.jpg"), dosyanın indirilirken boyutunun sıfırdan başlayıp artarak gerçek boyutuna (toplam boyutuna) geldiği, indirildiği klasör yolu (Şekil 29) görülmüştür. Bir dosya indirilirken core.log dosyasında (GET) isimli bir girdi kullanıldığı görülmüştür.
- **Push.log** dosyasında dosyanın indirildiği klasör, dosyanın algoritma imzası (MD5 ile SHA256) ve boyutu (size="3018030) tespit edilmiştir (Şekil 30).

Yandex.Disk uygulaması önce kendi kurulum dosyası aracılığıyla kaldırılmaya çalışılmış, ancak kurulumu kaldırmaya yönelik (uninstall) bir işlem gerçekleştirilememiştir. Daha sonra Windows işletim sisteminin **Denetim Masası\Tüm Denetim Masası Öğeleri\Programlar ve Özellikler** sekmesi altından Yandex.Disk uygulaması seçilerek kaldırılmıştır (Şekil 31). Kaldırma işlemi sonrasında yapılan incelemede **C:\Users\<Kullanıcı Adı>\YandexDisk\.sync** içerisinden kurulum dosyaları ile yüklenen, paylaşılan veya indirilen dosyaların silinmediği görülmüştür (Şekil 32)(bulgu 4.5).

Kullanıcı tarafından dosyaların yüklendikten sonra silinebileceği değerlendirilerek bu dosyalarda tarafımızdan silinmiştir. Silinen verilere ulaşmak için Tablo 7'de belirtilen anahtar kelimeler oluşturulmuştur.

Yandex.Disk uygulaması için oluşturulan bu anahtar kelimelerin kullanılabilirliğini test edebilmek için incelemelerde kullanılan işletim sisteminden farklı bir işletim sisteminde (Windows 8) uygulamanın kurulması, dosyaların yüklenmesi ve paylaşıma açılması işlemleri tekrarlanmış daha sonra uygulama kaldırılarak, dosyalar silinmiştir (bulgu 4.6).

Oluşturulan anahtar kelimeler Encase 7.06 programıyla bilgisayarda aratılmış ve bilgisayarda kurulu olan Yandex.Disk uygulamasının oturum açma adı, kullanıcı adı, paylaşıma açılan dosyalarla ile ilgili bilgiler tespit edilebilmiş olup (Tablo 8) inceleme sonuçlarımızla tutarlı olduğu görülmüştür (Şekil 33,44).

Bilişim sistemleri yenilenen ve dinamik bir yapıya sahip olmaları sebebiyle yeni uygulamalar, hizmetler ve servisler sürekli geliştirilmektedir. Yeni hizmete giren ve adli bilişim uzmanlarının ilk defa karşılaştığı bir bulut depolama uygulamasından da delil elde edebilecek sistematik bir inceleme yöntemi şu aşamalardan oluşabilir.

Öncelikle suç konusu dosya internet üzerinde (paylaşıma açılmış bir dosya olabilir) tespit edilmelidir.

İnceleme öncesinde yapılacak testlerde doğru uygulama kullanılması için bu dosyanın paylaşıldığı uygulamanın (hizmet servis sağlayıcının) hangisi olduğu sorusu cevaplanmalıdır.

Şüpheliye ait bilgisayarda bu uygulamanın kurulup kurulmadığı araştırılmalıdır.

Bu uygulamanın çalışma prensipleri ve hangi bilgileri elde edebileceğimizle ilgili bulgular bölümünde yapılan çalışmaya benzer şekilde sanal bilgisayarlarda denemeler yapılmalıdır.

Bu denemelerde oturum açma adları, paylaşılan ve yüklenen dosyaların isimleri, algoritma imzaları, uygulama ile yapılan faaliyetlerin neler olduğu (yükleme, indirme, paylaşıma açma vb.) ve yapılan faaliyetlerin işlem zamanı tespit edilmeye çalışılmalıdır.

Oturum açma zamanı ve işlemlerin yapıldığı zaman bilgileri belirlenirken birden fazla dosyada zaman bilgileri kontrol edilmelidir. Ayrıca bilgisayarın açılışında uygulamanın otomatik açılması, kullanıcının bilgisayar taih zamanını değiştirmiş olabileceği de gözönüne alınmalıdır.

Yapılan denemelerde elde edilen sonuçlara göre şüphelinin bilgisayarında delil elde edilebilecek (oturum açma adları, dosya isimleri vb.) dosyaları, bu dosyaların içeriğinde yapılan işlemlerle ilgili kayıtları bulmaya yönelik anahtar kelimeler oluşturulmalıdır. Aradığımız delili (oturum açma adı, yüklenen dosyalar vb.) farklı dosyalardan da tespit edebilmeye yönelik olarak mümkünse her biri için birden fazla anahtar kelime üretilmelidir.

Geriye dönük olarak elde edilen bu verilerden örnek depolama uygulaması olarak kullandığımız "Yandex.disk"le ilgili bir dosya incelendiğinde yukarıdaki verileri elde edebilmek ve şüphelinin yaptığı işlemleri tespiti için Tablo 7'deki anahtar kelimeler kullanılabilir.

Son olarak bilişim teknolojileri dinamik bir yapıya sahip olup çok geniş uygulama alanları mevcuttur. Adli bilişim uzmanlarının yaptıkları incelemeler kullanılan sistemin çeşidine (bilgisayar, cep telefonu vb.), bu sistemlerin sahip oldukları işletim sistemlerine (Windows[11], Linux[12], IOS[13], Android[14] vb.), dosyalama sistemlerine (NTFS[15], FAT[16] vb.), kullandıkları diskin çeşidine (SSD[17], HDD[18] vb.) göre değişmektedir. Bu sistemlerin her birinin verileri saklama, kayıt tutma özellikleri farklı olduğundan yapılan testlerin el konulan cihazın özelliklerine benzer sistemler üzerinde yapılması daha sağlıklı sonuçlar verecektir.

Ayrıca yapılan çalışmalarda tespit edilen hususlardan bazıları bilişim teknolojilerinin sürekli yenilenmesi nedeniyle değişikliğe uğrayabilecektir. Örneğin kullandığımız uygulamalara yeni bir yazılım güncellemesi geldiğinde bu anahtar kelimelerin bazılarında değişiklik olabilecektir. Ya da farklı işletim sistemlerinin veya sabit disklerin verileri saklama

[11] Windows: Microsoft Firmasının İşletim Sistemi
[12] Linux : Açık Kaynak İşletim Sistemi
[13] IOS : Apple Firmasının Mobil İşletim Sistemi
[14] Android : Açık Kaynak Mobil İşletim Sistemi
[15] New Technology File System NTFS : Yeni Nesil Dosyalama Sistemi
[16] File Allocation Table-FAT : Dosya Tahsis Tablosu Sistemi
[17] Solid State Disc-SSD : Katı Hal Disk
[18] Hard Disc Drive-HDD : Sabit Disk (Türkçe karşılığı olarak uygulamada genellikle sabit disk kullanılmaktadır.)

özelliklerinden dolayı silinen bazı verilerin tespit edilememesi durumuyla karşılaşılabilecektir. Bu sebeple bilgisayarların diğer alanlarında bulunabilecek verilerde adli bilişim uzmanlarına yol gösterecektir.

Bahsedilen yasal ve teknik zorluklara rağmen el konulan bir bilgisayarda bu uygulamalarla ilgili çok çeşitli verilere ulaşılabilmekte ve bulut depolama alanıyla bu bilgisayar bağlantısını ortaya koyabilecek şekilde ilişkilendirilebilmektedir. Yeni yöntem, yazılım ve donanımlar geliştirilene kadar geçen sürede klasik adli bilişim yöntemleri, bulut bilişim depolama uygulamalarını kullanan bilgisayarların incelenmesinde kullanılmaya devam edilecektir. Bu sebeple adli bilişim uzmanlarına yol göstermesi açısından bu yöntemlerin daha çok uygulamayla test edilmesi ve bu yöntemlerin de sistematik hale getirilmesi gerekmektedir.

Olay yerinden elde edilen suç konusu bir bilgisayarla bulut depolama alanının bağlantısını tespit edebilmek için çeşitli yöntemler kullanılabilir. Bunlardan bir tanesi de suç konusu içeriğin bulunduğu bulut depolama alanına el koyduğumuz bilgisayardan oturum açılıp açılmadığı, dosyaların bu bilgisayardan yüklenip yüklenmediği ve paylaşılıp paylaşılmadığının tespit edilmesidir. Bu tespitler neticesinde soruşturma/kovuşturma makamları suç eylemi ile suç aleti ve fail arasındaki bağlantıyı kurabilecektir.

Bu çalışmanın adli bilişimin en yeni konularından biri olan ve analiz yöntemleri geliştirilmeye devam eden bulut bilişim ile ilgili inceleme yapan/yapacak adli bilişim uzmanlarına, soruşturma ve kovuşturma makamlarına yardımcı olacağı değerlendirilmektedir.

6. KAYNAKLAR

(1) Yıldız, Ö. R., (2009) Bilişim dünyasının yeni modeli: Bulut Bilişim (Cloud Computing) ve Denetim, *Sayıştay Dergisi 74-75*

(2) Avşar, Z., Öngören, G., (2010), *Bilişim Hukuku*, Türkiye Bankalar Birliği Yayınları No:270 (Pasifik Ofset), İstanbul.

(3) Kılıç, M.S., (2012) İşletim Sistemlerinin Adli Bilişim Açısından İncelenmesi, Yüksek Lisans Tezi, Polis Akademisi Güvenlik Bilimleri Enstitüsü, Ankara.

(4) Mahmutoğlu, F.S., (2013) Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi, *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası Cilt:71 Sayı:1, s.856-889*, İstanbul.

(5) Berber, L.K., (2004) *Adli Bilişim (Computer Forensics)*, Yetkin Yayınları, İstanbul.

(6) Ceylan, R., Şirikçi, A.S, (2011) *"Bilişim Teknolojileri İncelemeleri-Veri İncelemeleri"*, Ed. Cihangiroğlu, B., Adli Bilimler Cilt 2**,** Jandarma Kriminal Daire Başkanlığı Yayınları, Ankara, 152-174.

(7) Pichan, A., Lazarescu, M., Soh, S.T., (2015) Cloud Forensics: Technical Challenges, Solutions and Comparative Analysis, *Digital Investigation Vol.13 pp.38-57* Doi: http://dx.doi.org/10.1016/j.diin.2015.03.002

(8) Erdoğan, Y., (2010), Bilişim Sistemine Girme ve Kalma Suçu, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Cilt: 12 Özel S., s.1363-1433.*

(9) Köksal, A., (2010), *Adı Bilgisayar Olsun*, Cumhuriyet Yayınları, Ankara

(10) Türk Dil Kurumu, (2016), [Erişim Adresi: www.tdk.gov.tr] [Erişim Tarihi:10.03.2016]

(11) Akarslan, H. (2012), *Bilişim Suçları*, Seçkin Yayıncılık, Ankara.

(12) Karagülmez, A., (2014), *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, Seçkin Yayıncılık, Ankara

(13) Karakehya, H., (2009), Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu, *Türkiye Barolar Birliği Dergisi, Sayı 81 s.187-211.*

(14) Dülger, M.V., (2012), *Bilişim Suçları ve İnternet İletişim Hukuku*, Seçkin Yayıncılık, Ankara.

(15) The Enigma of Alan Turing [Erişim Adresi: https://www.cia.gov/news-information/featured-story-archive/2015-featured-story-archive/the-enigma-of-alan-turing.html] [Erişim Tarihi:26.04.2016]

(16) Bıçakçı, S., (2013) *21. Yüzyılda Siber Güvenlik*, İstanbul Bilgi Üniversitesi Yayınları, İstanbul.

(17) Reilly, D., Wren, C., Berry, T., (2011) Cloud Computing: Pros and Cons for Computer Forensic Investigations, *International Journal Multimedia and Image Processing (IJMIP), Volume 1, Issue 1, March 2011*. p.26-34.

(18) Huth, A., Cebula, J., (2011) The Basics of Cloud Computing, Carnegie Mellon University. [Erişim Adresi: https://www.us-cert.gov/sites/default/files/publications/USCERT-Cloud ComputingHuthCebula.pdf] [Erişim Tarihi :28.04.2016]

(19) Mell,P., Grance,T., (2011). The NIST Definition of Cloud Computing, National Institute of Standards and Technology, Information Technology Laboratory. [Erişim Adresi :http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf] [Erişim Tarihi:20.04.2016] Doi: http://dx.doi.org/10.6028/NIST.SP.800-145

(20) Benson,P., (2013a) The Cloud Defined, Part 1 of 8: On-Demand Self Service, [Erişim Adresi:http://www.pbenson.net/2013/04/the-cloud-defined-part-1-of-8-on-demand-self-service/] [Erişim Tarihi: 10.04.2016]

(21) Benson,P., (2013b) The Cloud Defined, Part 2 of 8: Broad Network Access,

[Erişim Adresi: http://www.pbenson.net/2013/05/the-cloud-defined-part-2-of-8-broad-network-access/] [Erişim Tarihi: 10.04.2016]

(22) Benson,P., (2013c) The Cloud Defined, Part 3 of 8: Resource Pooling, [Erişim Adresi : http://www.pbenson.net/2013/05/the-cloud-defined-part-2-of-8/] [Erişim Tarihi: 10.04.2016]

(23) Benson,P., (2013d) The Cloud Defined, Part 4 of 8: Rapid Elasticity [Erişim Adresi :http://www.pbenson.net/2013/05/the-cloud-defined-part-4-of-8-rapid-elasticity/] [Erişim Tarihi: 10.04.2016]

(24) Benson,P., (2013e) The Cloud Defined, Part 5 of 8: Measured Service [Erişim Adresi :http://www.pbenson.net/2013/05/the-cloud-defined-part-5-of-8-measured-service] [Erişim Tarihi: 10.04.2016]

(25) Oktay, U., (2013) Bulut Bilişimde Vekil Ağ Saldırı Tespit Sistemi, Yüksek Lisans Tezi, Hava Harp Okulu Havacılık ve Uzay Teknolojileri Enstitüsü, İstanbul.

(26) Yüksel, H., (2012) Bulut Bilişim Mimari Yapısı, *Bulut Bilişim El Kitabı s.7-9* [Erişim Adresi : http://www.cozumpark.com/files/folders/308132/ download.aspx] [Erişim Tarihi: 20.04.2016]

(27) Henkoğlu, T., Külcü, Ö., (2013) Bilgi Erişim Platformu Olarak Bulut Bilişim: Riskler ve Hukuksal Koşullar Üzerine Bir İnceleme, *Bilgi Dünyası Dergisi Cilt:14 Sayı:1 s. 62-86*, e-ISSN:2148-354x.

(28) Martini, B., Choo., K.K.R., (2013) Cloud storage forensics: ownCloud as a case study, *Digital Investigation, 10 (2013) 287–299*, Elsevier Ltd., Doi: http://dx.doi.org/10.1016/j.diin.2013.08.005

(29) Ruan K., Carthy, J., Kechadi, T., Crosbie, M. (2011), Cloud Forensics, *Advances in Digital Forensics VII, Springer, pp35-46*

(30) Şanlı, O., (2011), Bulut Bilişim, *13'üncü Akademik Bilişim Konferansı*, Malatya [Erişim Adresi:http://ab.org.tr/ab11/bildiri/34.pdf] [Erişim Tarihi :06.04.2016]

(31) Özmestik, F.Ü., (2015) Bilişim Sistemleri Üzerine Arama ve El Koyma Tedbirine İlişkin Mevzuat ve Uygulamada Yaşanan Sorunlar, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.

(32) Casey, E., (2011) Digital Forensics, *In : Digital Evidence and Computer Crime: Forensic Science Computer and Internet,* Elsevier Inc., p:7-32

(33) Özen, M., Özocak, G., (2015) Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M.134), Ankara Barosu Dergisi [Erişim Adresi : http://www.ankarabarosu.org.tr/siteler/ankarabarosu/tekmakale/2015-1/01.pdf] [Erişim Tarihi: 20.04.2016]

(34) Bilgen, T., (2010), Türk Ceza Kanununda Banka veya Kredi Kartlarının Kötüye Kullanılması, Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Kamu Hukuku Programı, İzmir.

(35) Shinder, D.L., (2002), *Scene of The Cybercrime: Computer Forensics Handbook*, Syngress Publishing, Inc., Rockland (Massachusetts-USA).

(36) Aktaş, K., (2014), "Karşılaştırmalı Hukukta Elektronik Deliller", Adli Bilişim ve Elektronik Deliller, Ed. Çakır, H., Kılıç, M.S., Seçkin Yayıncılık, Ankara.

(37) Avrupa Siber Suçlar Sözleşmesi, (2001) [Erişim Adresi: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf] [Erişim Tarihi 18.03.2016]

(38) Aytekin, A., Kılıç, M.S., Çakır, H., (2014) Karşılaştırmalı Hukuk Açısından Siber Suçlar, Güncel Tehdit: Siber Suçlar, Ed. Çakır, H., Kılıç, M.S., Seçkin Yayıncılık, Ankara.

(39) Gültekin, Ö., (2011) Olay Yeri İncelemesinde Karşılaşılan Sorunlar ve Çözüm Önerileri, *Türkiye Adalet Akademisi Dergisi, Cilt:2 Sayı:4 s.473-508.*

(40) Yükseloğlu, E.H., Özcan, Ş.Ş., Ceylan, B., (2008) Olay Yeri İncelemesi ve Türkiye'deki Uygulamalar, *Polis Bilimleri Dergisi Cilt:10 (1), s.61-80.*

(41) Brown, C.L.T., (2010) Computer Forensics and Evidence Dynamics, *in Computer Evidence, Collection and Preservation,* Course Technology pp.1-69.

(42) Mukasey, M.B., Sedwick,J.L., Hagy,D.W., (2008) Electronic Crime Scene Investigation: A Guide for First Responders, Second Ed., National Institute of Justice, Washington. [Erişim Adresi : https://www.ncjrs.gov/pdffiles1/nij/219941.pdf] [Erişim Tarihi:02.04.2016]

(43) Özdilek, A.O., (2006) Uygulamadan Örnek Olaylarla Bilişim Suçları ve Hukuku, Vedat Kitapçılık, İstanbul

(44) Sarsıkoğlu, Ş., (2015), Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı, *Türkiye Adalet Akademisi Dergisi*, *Sayı:22* s.427-454.

(45) Say, K., (2006), Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi, Yüksek Lisans Tezi, Ankara Üniversitesi, Sağlık Bilimleri Enstitüsü, Ankara.

(46) John, J.L., (2012) Digital Forensics and Preservation, *Digital Preservation Coalition,* Great Britain. Doi: http://dx.doi.org/10.7207/twr12-03 pp.10

(47) Kara, U., Yükseloğlu, E.H., (2015) *Hukukçular ve Genetikçiler için Temel Adli Genetik*, Nobel Tıp Kitabevi, İstanbul.

(48) Hayes, D.R., (2015) A Practical Guide to Computer Forensics Investigations, Pearson Education, USA [Erişim Adresi:http://ptgmedia.pearsoncmg.com/images/9780789741158/samplepages/9780789741158.pdf] [Erişim Tarihi: 02.04.2016]

(49) ENFSI (2010), Policy on Standards and Accreditation, [Erişim Adresi : http://www.enfsi.eu/sites/default/files/documents/bylaws/policy_on_standards_for_accreditation.pdf] [Erişim Tarihi : 20.04.2016]

(50) www.jandarma.tsk.tr/basin/not/BN2008subat22.doc [Erişim Tarihi: 05.05.2016]

(51) TÜRKAK (2016), [Erişim Adresi: https://secure.turkak.org.tr/kapsam/search] [Erişim Tarihi:10.04.2016]

(52) Şirikçi, A.S., (2012), Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi, *Bilişim Teknolojileri Dergisi*, 5 (3), s.29-34

(53) Yetim, S. (2008) Dijital Kanıt Araştırma Yöntemleri, *İstanbul Barosu Dergisi, Cilt:82 Sayı:3 s.1201-1221.*

(54) NIST Cloud Computing Forensic Science Working Group Information Technology Laboratory (2014) "*NIST Cloud Computing Forensic Science Challenges"* U.S. Department of Commerce [Erişim Adresi:http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf] [Erişim Tarihi: 04.04.2016]

(55) Chung, H., Park, J., Lee, S., Kang, C., (2012) Digital Forensic Investigation of Cloud Storage Services, *Digital Investigation, Vol.9 81–95, 2012* Elsevier Ltd.
Doi: http://dx.doi.org/10.1016/j.diin.2012.05.015

(56) Grispos, G., Storer, T., Glisson, W.B., (2012). Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics, *International Journal of Digital Crime and Forensics, Volume 4, Issue 2, pp. 28-48*

(57) YANDEX, (2016) Sorular ve Yanıtlar-Disk-YandexDisk [Erişim Adresi:https://www.yandex.com.tr/support] [ErişimTarihi:06.04.2016]

(58) Sevli, O., Küçüksille, E.U., (2013) Bulut Ortamında Adli Bilişim, *6'ncı Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı,* Ankara.

(59) Hale, J.S., (2013) Amazon Cloud Drive Forensic Analysis, *Digital Investigation*, Elsevier Ltd. pp.259-265 Doi: http://dx.doi.org/10.1016/j.diin.2013.04.006

(60) Ouick, D., Choo, K.K.R., (2013a) Digital droplets: Microsoft SkyDrive forensic data remnants, *Future Generation Computer Systems, Volume 29, pp.1378-1394* Doi: http://dx.doi.org/10.1016/j.future.2013.02.001

(61) Ouick, D., Choo, K.K.R., (2013b) Dropbox analysis: Data remnants on user mahcines, *Digital Investigation,* Elsevier Ltd. pp.3-18 Doi:http://dx.doi.org/10.1016/j.diin.2013.02.003

ÖZGEÇMİŞ

Bireysel Bilgiler

Adı	**:** İsmail
Soyadı	**:** BARBAROS
Doğum yeri ve tarihi	**:** Bakırköy – 08.10.1981
Uyruğu	**:** Türkiye Cumhuriyeti
Medeni durumu	**:** Evli
İletişim adresi	**:** İstanbul Jandarma Kriminal Laboratuvar Amirliği Maslak/İstanbul
İş Telefon	**:** 0212 285 26 52
E-posta	**:** ismailbrbrs@gmail.com

Eğitim Durumu

1999-2003	Kara Harp Okulu /ANKARA (İşletme Ana Bilim Dalı Sistem Mühendisliği Bölümü)
1995- 1999	Maltepe Askeri Lisesi / İZMİR
1993-1995	Ömer Bedrettin Uşaklı Ortaokulu / UŞAK
1992-1993	Nişanca Ortaokulu / İSTANBUL
1991-1992	Vatan İlkokulu / İSTANBUL
1987-1991	Ebusuud İlkokulu / İSTANBUL

Yabancı Dili : İngilizce

Yabancı Dil Puan ve Türü : YDS –88.75 (Kasım 2014)

Mesleki Deneyim

2014-Halen	İstanbul J.Krim.Lab.A.liği Kimyasal ve Moleküler Biyolojik İncelemeler Şube Müdürü
2013-2014	J.Krim.D.Bşk.lığı Pl.Koor.Ş.Md.lüğü Proje Subayı
2013	J.Krim.D.Bşk.lığı Bilş.Teknj.İnc.Ş.Md.lüğü Veri ve Donanım İnc.Uzm.
2010-2013	J.Krim.D.Bşk.lığı Bilş.Teknj.İnc.Ş.Md.lüğü Veri ve Donanım İnc.Uzm.Yrd.
2003-2010	Jandarma Teşkilatının çeşitli birliklerinde takım ve bölük komutanlıkları.

Katıldığı Kurslar ve Bilimsel Etkinlikler

2014 Taktik Sivil Asker İşbirliği Kursu (*NATO Barış İçin Ortaklık Eğitim Merkezi*)

2013 Macintosh İşletim Sistemleri, Hard Diskler, Cep Telefonlarından Veri Toplama Atölye Çalışması (*AB Eşleştirme Projesi*)

2013 Encase Internet Examination (*Guidance Software*)

2013 Encase Computer Forensic 2 (*Guidance Software*)

2013 Encase Computer Forensic 1 (*Guidance Software*)

2012 İnternet Soruşturmaları (*AB Eşleştirme Projesi*)

2012 Veri Madenciliği ve Analizi Eğitimi (*AB Eşleştirme Projesi*)

2012 Beyaz Şapkalı Hacker Eğitimi (CEH v7) (*Meslek içi Eğitim*)

2012 Linux/Unix Sistem Yönetimine Giriş Eğitimi (*Meslek içi Eğitim*)

2012 Trafik Kazaları Adli İncelemeleri Eğitimi (*AB Eşleştirme Projesi*)

2012 Olay Yeri İnceleme için En İyi Uygulama Kılavuzu Yazma Atölye Çalışması (*AB Eşleştirme Projesi*)

2010 Veri ve Donanım İnceleme Uzmanlığı Laboratuvar Uzmanlık Eğitimi (*Meslek içi Eğitim-2 yıl süreyle*)

2006 Barışı Destekleme Harekatında Operasyonel Lisan Kursu (*NATO Barış İçin Ortaklık Eğitim Merkezi*)