T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

OLAY MÜDAHALESİ KAPSAMINDA WİNDOWS İŞLETİM SİSTEMİNE SAHİP CİHAZLARDAN TRİYAJ KAYITLARININ ELDE EDİLMESİ

Kaan YENİYOL

Yüksek Lisans Tezi

ADLİ BİLİŞİM MÜHENDİSLİĞİ ANABİLİM DALI

Adli Bilişim Mühendisliği Bilim Dalı

AĞUSTOS 2021

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Adli Bilişim Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

OLAY MÜDAHALESİ KAPSAMINDA WİNDOWS İŞLETİM SİSTEMİNE SAHİP CİHAZLARDAN TRİYAJ KAYITLARININ ELDE EDİLMESİ

Tez Yazarı
Kaan YENİYOL

Danışman
Doç. Dr. Fatih ERTAM

AĞUSTOS 2021
ELAZIĞ

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Adli Bilişim Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

Başlığı:	Olay Müdahalesi Kapsamında Windows İşletim Sistemine Sahip Cihazlardan Triyaj Kayıtlarının Elde Edilmesi
Yazarı:	Kaan YENİYOL
İlk Teslim Tarihi:	05.07.2021
Savunma Tarihi:	11.08.2021

TEZ ONAYI

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına göre hazırlanan bu tez aşağıda imzaları bulunan jüri üyeleri tarafından değerlendirilmiş ve akademik dinleyicilere açık yapılan savunma sonucunda OYBİRLİĞİ ile kabul edilmiştir.

		İmza	
Danışman:	Doç. Dr. Fatih ERTAM Fırat Üniversitesi, Teknoloji Fakültesi		Onayladım
Başkan:	Dr. Öğr. Üyesi Aytuğ BOYACI Milli Savunma Üniversitesi, Hava Harp Okulu		Onayladım
Üye:	Dr. Öğr. Üyesi Orhan YAMAN Fırat Üniversitesi, Teknoloji Fakültesi		Onayladım

Bu tez, Enstitü Yönetim Kurulunun ...../...../20..... tarihli toplantısında tescillenmiştir.

İmza

Doç. Dr. Kürşat Esat ALYAMAÇ
Enstitü Müdürü

BEYAN

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım "Olay Müdahalesi Kapsamında Windows İşletim Sistemine Sahip Cihazlardan Triyaj Kayıtlarının Elde Edilmesi " Başlıklı Yüksek Lisans Tezimin içindeki bütün bilgilerin doğru olduğunu, bilgilerin üretilmesi ve sunulmasında bilimsel etik kurallarına uygun davrandığımı, kullandığım bütün kaynakları atıf yaparak belirttiğimi, maddi ve manevi desteği olan tüm kurum/kuruluş ve kişileri belirttiğimi, burada sunduğum veri ve bilgileri unvan almak amacıyla daha önce hiçbir şekilde kullanmadığımı beyan ederim.

11.08.2021

Kaan YENİYOL

ÖNSÖZ

Bu tez çalışmasının tamamlanmasında yardımlarının esirgemeyen danışmanım Sayın Doç. Dr. Fatih ERTAM'a, Fırat Üniversitesi Adli Bilişim Mühendisliğinde görevli hocalarıma ve desteğini esirgemeyen aileme teşekkür ederim.

Kaan YENİYOL
ELAZIĞ, 2021

İÇİNDEKİLER TABLOSU

ÖZET

Olay Müdahalesi Kapsamında Windows İşletim Sistemine Sahip Cihazlardan Triyaj Kayıtlarının Elde Edilmesi

Kaan YENİYOL

Yüksek Lisans Tezi

FIRAT ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü

Adli Bilişim Mühendisliği Anabilim Dalı
Ağustos 2021, Sayfa: xiv + 57

Günümüzde, siber saldırganlar ele geçirdiği makineler üzerinde hızlı yayılım gösterebilmektedir. DFIR ekipleri, saldırının izlerini tespit etmek ve takip etmek için güvenlik ihlaline maruz kalan makinelere ait disklerin fiziksel veya mantıksal disk imajları almaktadırlar. Olay müdahale ve adli bilişim süreçlerinde vakaya ait dijital delillerin toplanması önem arz etmektedir. Herhangi bir vakada enfekte olmuş makinelerden disk imajı alıp analizini sağlamak uzun uğraşlar gerekmektedir. Adli bilişim uzmanları, saldırının takibi sürdürebilmesi için bazı makinelerden hızlı veriler toplayıp analiz etmelidir. Enfekte olmuş cihazlardan saldırının kaynağının ve yayılımın tespiti için Windows işletim sistemine sahip sistemlerden birkaç dosya sistem kaydı veya log dosyalarının toplanması ile sağlanmaktadır.

Adli bilişim uzmanının, vakanın hızlı analizi için canlı bir sistemden veya adli bir imaj içerisinden önemli işletim sistemi dosyalarını toplaması yeterli olacaktır. Bu tez çalışmasında, programların çalıştırılma, silinen veya bilinmeyen dosya, kullanıcı aktivite kayıtları ele alınmıştır. Windows işletim sistemlerine sahip local veya remote makineler üzerinde önemli kayıtların triyaj yöntemleri ile toplanmasından söz edilmiştir.

Bu tez çalışması kapsamında, Windows aktif dizini üzerinde yer alan cihazlara uzaktan bağlanarak cihazlar üzerinden dosya sistem ve uygulama kayıtlarının toplanmasını sağlayan ve Powershell betiğinde geliştirilen PS-TRIAGE isimli yazılım kodlanmıştır. PS-TRIAGE yazılımı ayrıca, makine üzerinden toplanan triyaj kayıtlarında ön analiz sağlayarak ve olay müdahale analistine çıktı olarak vermektedir.

Anahtar Kelimeler: Dijital Kanıt, Triyaj Kaydı, Olay Müdahalesi, Uygulama Kalıntıları, Dosya Sistem Kayıtları, DFIR

ABSTRACT

COLLECTION OF TRIAGE FROM MACHINES WITH WINDOWS OPERATING SYSTEM IN INCIDENT RESPONSE

Kaan YENİYOL

Master's Thesis

FIRAT UNIVERSITY
Graduate School of Natural and Applied Sciences

Department of Digital Forensic Engineering

August 2021, Pages: xiv + 57

Cyber threat actors can spread rapidly over the environment by using the machines that they compromised. DFIR teams acquire physical or logical disk images of the disks belong to compromised machines to detect and track the traces of the attackers. It is important to collect digital evidence of the incidents in incident response and digital forensic processes. In any case, it takes a long effort to acquire disk image from infected machines and analyze it. In some cases, Incident Response Analysts have to collect and analyze data from some machines as quick as possible in order to keep track of the attackers. Disk image acquiring processes can be achieved by collecting several file systems records or log files from devices with Windows operating systems to detect the root cause of the cyber-attack.

It will be sufficient for the Incident Response Analysts to collect important operating system files from a live system or a forensic disk image for quick analysis of the case. In this article, Evidence of Program Execution, Deleted File or File Knowledge, Account Usage records will be discussed within the scope of analysis process. In this paper studies about collecting important records on local or remote machines with Windows operating systems by triage methods will be explained.

As part of this thesis, a software called PS-TRIAGE, developed in the PowerShell script, was encoded that allows you to remotely connect to devices located in the Windows Active Directory and collect file system and application records via devices. PS-TRIAGE software also provides pre-analysis on machine-collected triage records and provides output to the incident response analyst.

Keywords: Digital Evidence, Forensic Triage, Incident Response, Application Log Record, File System Artifacts, DFIR

ŞEKİLLER LİSTESİ

Sayfa

TABLOLAR LİSTESİ

Sayfa

SİMGELER VE KISALTMALAR

Kısaltmalar

AD1	:	Access Data Format
DFIR	:	Digital Forensics and Incident Response
EDR	:	Endpoint Detection Responsev
EOE	:	Evidence Of Execution
ENV	:	Environment variables
IPS	:	Intrusion Prevention System
OS	:	Operating System
SANS	:	SANS Institute
SFTP	:	SSH File Transfer Protocol
SIEM	:	Security Information and Event Management
SOAR	:	Security Orchestration, Automation and Response
SSH	:	Secure Shell
WINRM	:	Windows Remote Management

1. GİRİŞ

Adli bilişim ve olay müdahalesi süreçlerinde, ilgili vakaya ait elektronik delillerin titizlikle toplanması ve saklanması oldukça önem arz etmektedir. Söz konusu elektronik delillerin bütünlüğünü koruyarak fiziksel veya mantıksal kopyasının alınıp analiz edilmesi gerekmektedir. Fiziksel ve mantıksal olmak üzere iki farklı imaj alma yöntemi bulunmaktadır. Tüm birimlerin inceleneceği veri depolama biriminde fiziksel, belirli bir bölümün/dosyanın inceleneceği veri depolama biriminde mantıksal imaj alma yöntemine başvurulmaktadır. Herhangi bir vakanın meydana geldiği ortamda yer alan elektronik delil sayısına göre elde edilen imajların sayısı ile imajların analiz süreleri değişkenlik gösterebilir.

Günümüzdeki siber saldırılarla karşı kaşıya kalan kurum veya kuruluşlara ait kurumsal ağında saldırganlar yanal hareket yöntemi ile yayılım gösterebilirler. Bu yanal hareket işlemleri ile kısa sürede birçok elektronik cihaz(Sunucu, Bilgisayar, Telefon) saldırganlar tarafından ele geçirilebilir. Adli bilişim uzmanı tarafından, söz konusu vakanın yaşandığı ortamda saldırının kaynağı ve yayılımın tespiti için ele geçirilen cihazlardan elektronik delil toplaması gerekebilir. Elektronik delil toplarken, ilgili sistemlerin çalışmasının devam ettirilmesine veya hizmet kesintisi sağlamamasına dikkat edilmesi gerekmektedir. Bu sebeple, adli bilişim uzmanı siber saldırılardan etkilenen sunucu veya bilgisayarlardan canlı olarak elektronik delil elde etmelidir. Elektronik delil toplanacak cihazların sabit sürücü boyutlarının fazla olması ilgili sistemin fiziksel veya mantıksal imajı alma süresi ile disk imajlarının analiz sürelerinin artmasını sağlamaktadır. Enfekte olan cihazlardan saldırının kaynağının ve yayılımın tespiti için Windows işletim sistemine sahip sistemlerden birkaç dosya sistem kaydı veya log dosyalarının toplanması ile sağlanabilir. Adli bilişim uzmanının, vakanın hızlı analizi için canlı bir sistemden veya adli bir imaj içerisinden önemli işletim sistemi dosyalarını toplaması yeterli olacaktır. Bu sayede fiziksel veya mantıksal disk görüntüsünü analiz etmek için saatler harcanmadan, ilgili vakanın çözülmesi sağlanabilir.

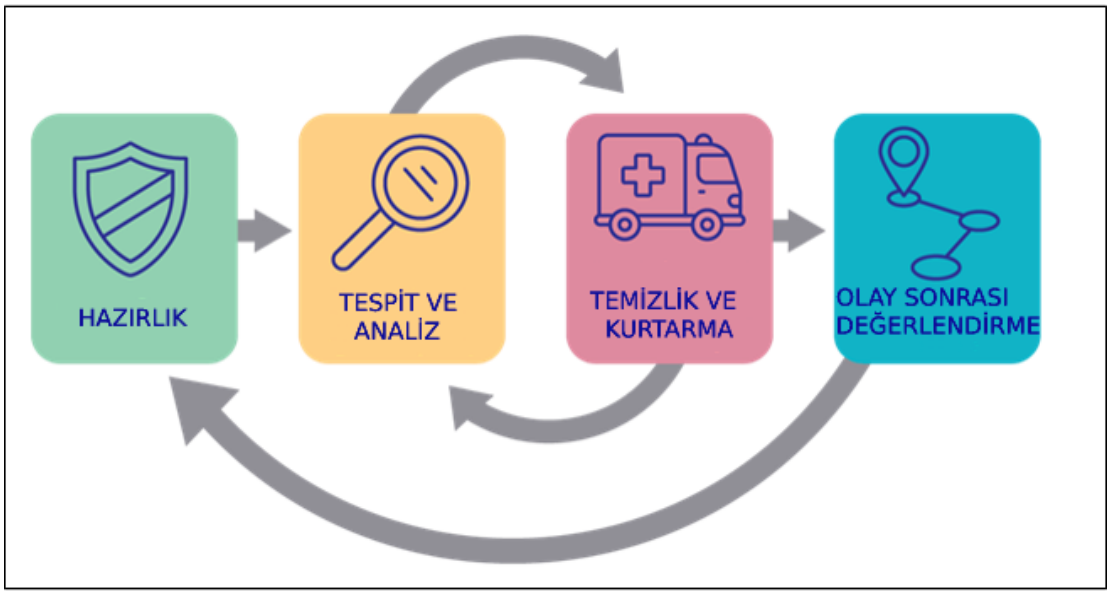
Olay müdahalesinde, bir ortamda siber saldırılardan etkilenen 100 adet sunucu olduğunu varsayalım söz konusu sunuculara ait fiziksel veya mantıksal disk imajlarının elde edilmesi yönteminin haricinde triyaj veri toplanması yeterli olacaktır. Toplanan kayıtlar ile vakanın analiz süresinin ve analizcinin iş yükünü azaltılacaktır. Bu makale Windows işletim sistemine sahip cihazlardan dosya sistem kaydının ve log dosyalarının elde edilmesi yöntemlerinden ve ilgili vakanın ana nedeninin tespiti için analiz edilmesi gereken kayıtlarından detaylı olarak bahsedilmiştir.

2. OLAY MÜDAHALE VE DÖNGÜSÜ

Olay müdahalesi, siber güvenlik olayına metodoloji olarak müdahale etme planıdır. Olay müdahalesi ve döngüsü, siber saldırı durumunda aktiveyi hızla kontrol altına almak, zararı en aza indirmek ve olaydan deneyimler elde edilerek yeni önlemlerin alınması için adımlar atılmasıdır. Olay müdahalesi, şüpheli bir siber saldırı ihlaline hazırlanmak, tespit etmek, kontrol altına almak ve ortadan kaldırmak için bir kuruluş tarafından benimsenen sistematik yaklaşımdır. Bir olay müdahale planında, siber saldırılara düzenli ve etkili bir yanıt verilmesinin yanı sıra kuruluşun verilerini, itibarını ve gelirini korumaya da yardımcı olmaktadır.

Günümüzde adli bilişim süreçlerinde, kurumsal bir olay müdahale prosedürleri giderek daha fazla kullanılmaktadır. Hazırlık kapsamında, bir kuruluşun olay müdahale sürecini hızlandırmak için bir siber saldırının öncesinde alabileceği prosedürler olarak tanımlanır. Olay müdahalesinde zaman kısıtlıdır ve dijital kanıtların hızlı bir şekilde toplanmasını ve analiz edilmesini gerekmektedir. Örneğin, potansiyel bir güvenlik ihlaline müdahale edilirken, adli bilişim açısından sağlam kanıtların edinilmesi, saldırgan tehdidinin hızla kesintiye uğraması veya etkisiz hale getirilmesi, ortaya çıkan ekonomik ve itibar kaybın en aza indirilmesi ile dengelenmelidir [1]. Olay müdahalesinde amaç güvenlik çözümleri tarafından yakalanamayan ve önlenemeyen siber saldırıların detaylı şekilde tespitini gerçekleştirmek ve bu saldırılara olabildiğince zamanında etkili olarak müdahale etmektir.

Siber saldırılara karşı, sağlam bir olay müdahale döngüsü; hazırlık, tespit etme ve analiz, temizlik ve kurtarma, saldırı sonrası alınacak önlemler olarak üzere dört aşamadan oluşmaktadır. NIST tarafından belirlenen olay müdahalesi süreçlerine ait hazırlık, tespit ve analiz, temizlik ve kurtarma, olay sonrası değerlendirme aşamalarının döngüsü Şekil 2.1'de yer almaktadır [2].



Şekil 2.1. Olay Müdahale Döngüsü

2.1. Hazırlık Aşaması

Olay müdahalesinde hazırlık aşaması, müdahale süreçlerinin temellerini oluşturmaktadır. Siber saldırıdan etkilenen kuruluşun kurumsal ağ ortamının tanınması, tehditlerin belirlenip 7/24 izlenmesi, kurum için olayın risklerinin belirlenmesi gerekmektedir. Siber saldırıya somut adımlarla kronolojik olarak nasıl ilerlenmesi gerektiği, müdahale adımlarının akış şemalarının çizilmesi ve kontrol listelerinin eklenmesi ile olay müdahale sürecinin iyi yönetilmesini sağlamaktadır. Olayları uygun bir şekilde sınıflandırmak için kritik, yüksek, orta veya düşük önem dereceleri belirlenmelidir. Bu şekilde tüm olaylara aynı odaklanmayı, kaynakların tahsisini ve fazla müdahale ekiplerinin yer alması gerektirmez. Olay müdahale planları, operasyonel ekipler tarafından diğer işlevlere ve paydaşlara bilgilerin neyin, ne zaman ve nasıl iletilmesi gerektiğini açıkça ortaya koymalıdır. Bir siber saldırı sırasında, tüm paydaşlar(Adli bilişim uzmanları, olay müdahale ekipleri, domain ortam sorumluları, firewall güvenlik çözümü yöneticileri vs.) rollerinin ve sorumluluklarının farkında olmalıdır. Resmi roller ve sorumluluklar, olay müdahale planının bir bölümünde açıkça belirtilmelidir.

Hazırlık aşamasında, analizcilerin her zaman erişebildiği ve uygulamasının yapıldığı senaryo adımları(Playbook) geliştirilmelidir. Bu senaryolarda, en yaygın siber saldırı olayları veya sistemlerinize doğrudan etki edecek riskleri belirtebilirsiniz. Söz konusu risklere müdahale edilmesi durumda operasyonel olarak rehberlik edecek ve eyleme geçirilebilir durumda olan senaryo adımları oluşturulmalıdır.

2.2. Tespit Aşaması

Kurumsal ağ ortamındaki kötü niyetli aktivelerin tespiti için güvenlik kontrollerinin sağlanması bütünüdür. Ağ üzerindeki aktivelerin takibi için IDS ve IPS alarmların takibi, kural yazımı ve alarmları oluşturulabilir. Uç noktaların izlenmesi ve ajanların kurumları yapılması ile makineler üzerinde, hesap çalma, yayılım, zafiyetlerin sömürülmesi gibi kötücül aktivitelerin tespiti sağlanmalıdır. Siber istihbarat servislerinin aktif olarak kullanılması, dark web, hack forumları gibi sitelerde, çalınan kurumsal bilgilerin izlenmesi, tespit edilmesi ve ihlal bildiriminin yapılması sağlayabilmektedir. Bu tür bir izlemede, olayı potansiyel olarak kamuoyuna açıklanmadan önce tespit ederek için son bir müdahale görevi gerektirebilir. İyi eğitimli ekiplerin, doğru olay müdahale planlarına uyum sağlaması, ekiplerin kötü niyetli aktiviteyi tespit ettiğinde, uygun bir şekilde öncelik tanıyabilmesi ve daha geniş organizasyonları nasıl uyaracaklarını bilmesi gerekmektedir. Aktivelerin izlenmesinde görevli olan ekiplerin, herhangi bir siber saldırı olayının tespitinde panik olmamalı, uygun önlemler alınmalıdır [3].

2.3. Temizlik ve Kurtarma

Siber saldırı sonucunda oluşan kötücül aktivite izlerinin kurumsal ağ üzerinde temizlenmesi, yok edilmesi ve saldırının tekrar yaşanmaması için önlemlerin alınması sağlanmalıdır.

2.4. Olay Sonrasının Değerlendirilmesi

Kurtarma aşaması ile olayı geride bırakıp, kuruluşun itibarı ve ekonomik kayıplarını önlemek için gelecekte benzer siber saldırı olaylarla mücadele hazırlıklı olunması gerekmektedir. Siber saldırının kök nedeninin anlaşılması, iyileştirmelerin uygulanması ve geri bildirimlerin sağlanması gibi döngüden oluşmaktadır [4]. Her olaydan deneyim edilmesi ve bazı olay müdahale dokümanlarının güncellenmesi sağlanmalıdır. Ek olarak, SOAR, EDR, IPS, IDS gibi sistemlerde uygun alarmların oluşturulması ve sistemlerin yetkin bir ekip ile izlenmesi sağlanmalıdır.

3. ARTIFACT KAYITLARI

Siber saldırıdan etkilenen sistemlerde, olay müdahalesi oldukça hızlı olmalı ve doğru kanıt olabilecek kayıtların toplanması sağlanmalıdır. Microsoft Windows, dünyada en yaygın kullanılan işletim sistemidir. Bu nedenle, olay müdahale analistlerinin Windows'ta artifacts kayıtlarının nasıl oluşturulduğunu, söz konusu kayıtlar üzerinden, bir kullanıcının aktivitelerini izlemek veya siber saldırının izlerinin tespit edilmesi için nasıl kullanılabileceğini anlamaları beklenmektedir. Bahse konu artifacts kayıtları, silinmiş veriler, geri yükleme noktaları, metadata verileri, geri dönüşüm kutusu gibi yapıları içermektedir [5].

Windows sistemler üzerinde gerçekleşebilecek herhangi bir siber saldırı veya adli bilişim vakalarında kanıt olarak analiz edilmesi gereken dosyalar artifacts olarak adlandırılmaktadır. Windows işletim sistemlerine sahip makineler üzerinde gerçekleşebilecek herhangi bir olay müdahalesinde siber saldırının izlerinin tespiti için toplanan çeşitli uygulama kalıntıları, dosya sistem kayıtları ve olay günlüğü kayıtları analizi yapılabilmektedir. Söz konusu artifacts kayıtları ile bir sistemin fiziksel veya mantıksal imajını almadan kötücül bir siber saldırı aktivitesinin analizi sağlanabilmektedir.

3.1. Uygulama Kayıtları

Windows işletim sistemlerine sahip makineler üzerinde kurulu olan uygulamalara ait veri tabanları ve log dosyaları gibi artifacts kayıtları yer almaktadır. Söz konusu kayıtlar, genellikle uygulamanın kurulu olduğu dizin içerisinde ve geçici dizinler altında yer almaktadır. Olay müdahalesi veya adli bilişim süreçlerinde uygulama kayıtlarında analizi yapılarak, son kullanıcının gerçekleştirdiği aktiviteler veya uygulamanın kötü amaçlı olarak kullanıp kullanılmadığını tespiti sağlanabilmektedir.

3.1.1. Uzak Masaüstü Yazılım Kayıtları

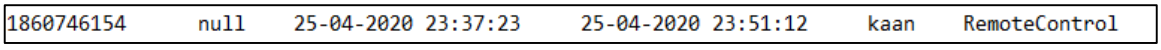
Uzak masaüstü yazılımları ile uzakta bulunan herhangi bir bilgisayar veya sunucuya bağlanarak kontrolü sağlanmaktadır. Bazı kurum veya kuruluşlarda bur tür yazılımların kullanıma izin verilse de, bazı kurumlar bu tür yazılımların bilgi güvenliği politikalarına aykırı olduğu değerlendirip, son kullanıcılar tarafından kullanımı yasaklamıştır. Saldırganların bazı uzak masaüstü yazılımlarını kullanarak hedef makinelere erişim sağladığı ve zararlı aktivitelerde bulunarak kurumsal ağ üzerinde yayılım gösterdikleri bilinmektedir [6].

Uzak masaüstü yazılımlarını kullanılarak, bilgisayarlara uzaktan bağlanarak erişim sağlanması yararlıdır, ancak söz konusu yazılımları kullanan siber saldırganlar, fiziksel cihazlara (makinelere) uygun olmayan bir şekilde erişim sağlayabilmektedir. Kötü niyetli kişiler, yetkisiz veya yasadışı bir şekilde diğer kişilerin sistemine erişebilirler. Bu, bir kuruluşun ticari faaliyetleriyle ilgili önemli bilgilerin veya kurumsal verilerin çalınmasına yol açabilmektedir. Bu nedenle, sistemde geride kalan verilerden kanıt çıkarmak için uzak masaüstü yazılımlarının artifacts kayıtlarının doğru bir şekilde analizi gerekmektedir. Bu verilerin analizi sonrasında, olay müdahale ve adli bilişim uzmanları, saldırganın sisteme gerçekten erişip erişmediğini ve erişim süresi gibi bilgilerin tespiti sağlayabilmektedir.

Teamviewer Kayıtları

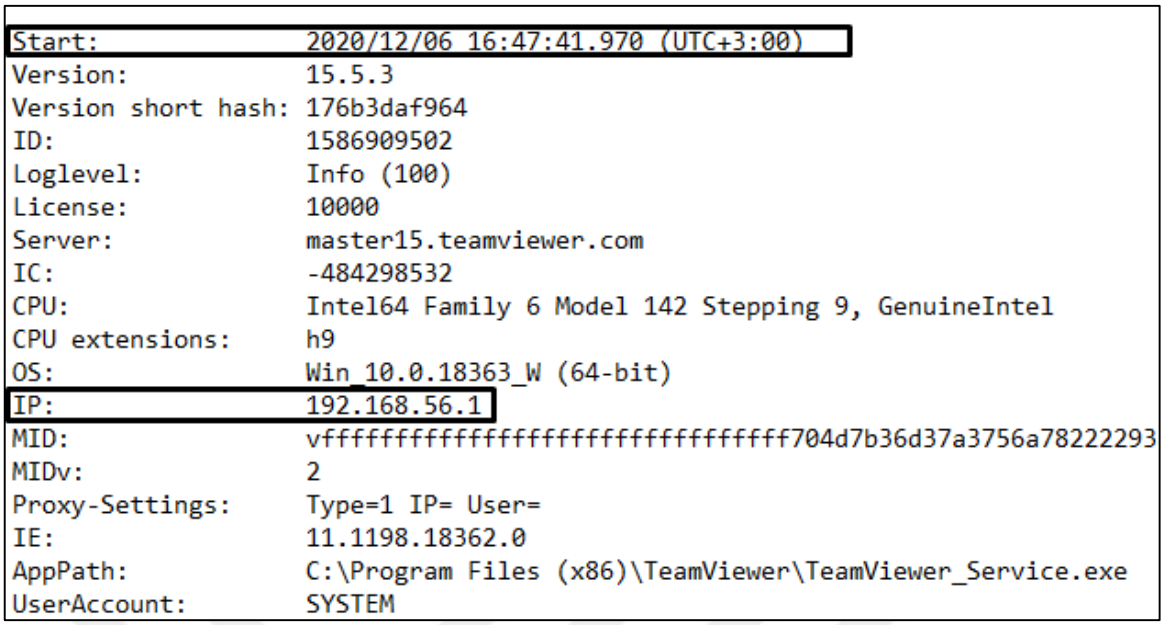
Teamviewer uzaktan bağlantı aracının, artifacts kayıtları "**C:\Program Files (x86)\TeamViewer"** veya "**C:\Users\[Account]\AppData\Roaming\TeamViewer**" dizinlerinde almaktadır.

Şekil 3.1'de "**Connections_incoming.txt**" isimli log dosyasında yer alan, uzak masaüstü yazılımı ile bilgisayar üzerinde açılan oturuma ait kayıt yer almaktadır.



Şekil 3.1. Teamviewer ile oturum açan kullanıcı bilgisi

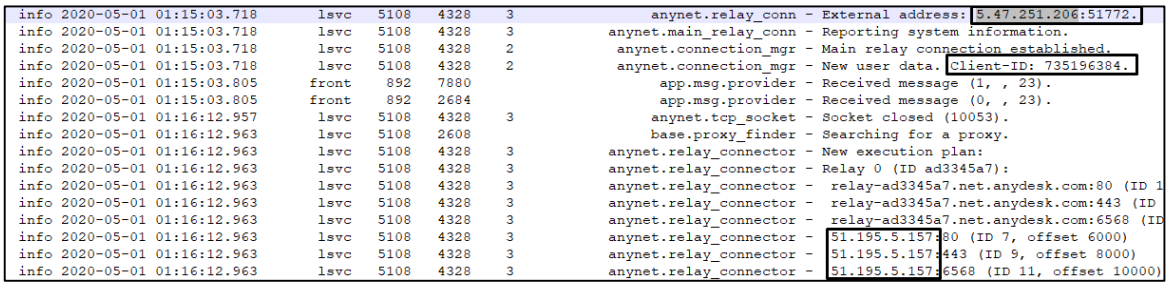
"**TeamViewerX_Logfile.log**" isimli log dosyasında ise Teamviewer'ın her bir etkinliğini zaman damgaları, uzak sistem IP'si, Teamviewer Kimliği vb. bilgileri içermektedir. Bu günlük dosyası, tüm gelen ve giden bağlantıların tam geçmişidir [7]. Teamviewer uygulaması ile açılan oturumlara ait detaylı log kaydı Şekil 3.2'de beyan edilmiştir.



Şekil 3.2. Teamviewer ile açılan oturuma ait detaylı kayıt

Anydesk Kayıtları

Anydesk uzaktan bağlantı aracının, artifacts kayıtları **"%programdata%\AnyDesk**" veya **"%appdata%\AnyDesk**" dizinlerinde almaktadır. "**ad.trace**" veya "**ad_svc.trace**" isimli log dosyalarında uzak masaüstü erişimlerine ait detaylı bilgi yer almaktadır. Anydesk yazılımına ait örnek log kaydı Şekil 3.3'de yer almaktadır.



Şekil 3.3. Anydesk Log Kaydı

3.2. Windows İşletim Sisteminde Yer Alan Artifact Kayıtları

Windows işletim sistemi (OS) siber dünyada önemli bir rol oynamaktadır. Windows işletim sistemlerinden biri olan NTFS, önemli verileri depolayan ve yöneten Windows işletim sistemi altındaki ortak dosya sistemidir. NTFS dosya sisteminin verilerini analiz edilmesi, olay müdahale süreçlerinde büyük önem taşımaktadır. Örneğin, veriler silinirse Windows işletim sistemi altında doğrudan gözlemleyemeyiz, ancak bazı önemli aktivite kanıtları NTFS dosya yapısında yer almaktadır [8]. Güvenilir bir veri kaynağı ve adli bilişim için güçlü bir kanıt verilerini tutmaktadır. Windows işletim sistemi üzerinde gerçekleştirilen herhangi bir işlem, olay veya aktivite dosya

sistem kayıtları üzerinde kayıt edilmektedir. Dosya sistem kayıtlarının analizi sonucunda, bir vakaya yönelik kayıtlar tespit edilebilir, aktivitenin zaman çizelgesi çıkartılabilmektedir.

Genellikle, bir sistemdeki tüm olaylar dosya sistemi içinde aşağıdaki örnek kayıtlar gibi bir iz bırakacaktır.

- Bir dosyadaki değişiklik (tarih, saat, son erişim)
- Bir dosyanın oluşturulması veya silinmesi
- Alan kullanımında artış / azalma
- Kullanıcı oluşturulması ve silinmesi,
- İşlem olaylarının günlüğü
- Çalıştırılan yazılımlar ve kurulu olan programlar
- Takılan USB bellek kayıtları
- Uzak masaüstü erişim kayıtları
- Ortak alana erişim kayıtları

3.2.1. Dosya sistem kayıtları

MFT, NTFS dosya sisteminin temelini oluşturmaktadır. Sistemde bulunan tüm dosya ve dizinler hakkında bilgi içerir bundan dolayı her bir dosya MFT tablosunda en az bir girdi bulundurmaktadır. Her bir girdi 1KB boyutunda olmasının yanı sıra yalnız ilk 42 baytın tanımlanmış bir amacı vardır. Geri kalan bölüm özellikleri içermektedir. Buna örnek olarak bir attribute, sadece dosyanın ismini depolamak için kullanılabilir [9]. Arka planda, Windows NTFS dosya sistemi, işletim sistemin çöktükten sonra bilinen dosyaların kurtarılmasını sağlamak için kullanılan bir işlem mimarisine sahiptir. Windows, sisteminin beklenmedik şekilde kapanmasına neden olan kritik hatalardan sonra veri tutarlılığını sürdürmeyi sağlamaktadır. NTFS özellikle aşağıdaki dosya işlemlerini günlüğe kaydeder:

- Dosyanın oluşturulma tarihi
- Dosyanın silinme tarihi
- Dosyanın adı
- Dosyanın boyutunu
- Bir dosyayı yeniden adlandırma
- Bir dosyaya değiştirilme tarihi

Windows NTFS, $LogFile dosyasında bir dizi dosya değişikliğini kaydeden bir günlük kaydı tekniği kullanır. İşlem dizisi tamamlandıktan sonra, işletim sistemi değişiklikleri taahhüt eder ve işlem yapılır. Bu şekilde, bir işlem diske kaydedilmeden önce sistemin çökmesi durumunda, sistem $LogFile'daki değişiklik sırasını okuyabilir ve ardından sistemdeki dosyaları okunabilir haline getirilebilmektedir.

Olay müdahale analiz süreçlerinde, $LogFile'ı analiz edilmesi sonucunda, yapılan geçmiş işlemlerin kronolojik bir listesini elde edilebilir. $LogFile sabit boyuttadır, bu nedenle boyutu dolduğunda ve eski verilerin üzerine yeni işlemlerle yazılır. Bir sistemde yapılan dosya değişikliklerinin sıklığına bağlı olarak geçmiş işlemlerin sayısı değişecektir. $LogFile'ın boyutu bir birim için tipik olarak 64 MB'dir, ancak ihtiyaca göre yeniden boyutlandırılabilir. Standart varsayılan boyut ve normal kullanım kullanıldığında, $LogFile'da kaydedilen birkaç saatlik etkinlik beklenebilir. Bu zaman aralığı oldukça özneldir ve dosya sistemi değişikliklerinin sıklığına bağlı olarak değişmektedir.

Journal dosyası ise ($J), dosya ve dizinlerde, metadata değişikliği, dosya oluşturulma ve silinme gibi her değişiklik yapıldığında güncellenmektedir.

MFT, $J ve $logfile isimli dosya sistem kayıtlarında, zararlı bir aktivitede oluşan dosyaların, isimleri, oluşturulma zamanı ve aktivite zamanı gibi önemli kayıtlar yer alabilmektedir [10].

MFT dosya sistem kaydında, dosyalar MAC(b) zamanına göre kayıt edilir. MAC(b) zamanları aşağıdaki gibidir.

- M (Modified) Değiştirilme
- A (Access) Erişme
- C (Change) MFT değiştirilme tarihi
- B (Birth) Oluşturulma tarihi

Dosya sistem kayıtlarının yer alan konum bilgisi Tablo 3.1'de sunulmuştur.

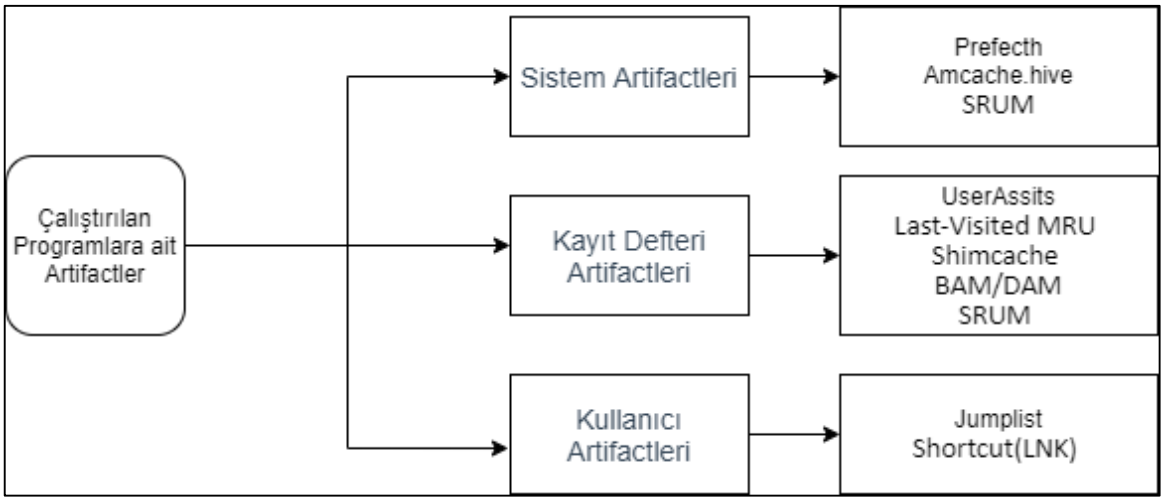
Tablo 3.1. Dosya sistem kayıtları

Artifacts	Konum
Dosya sistem kayıtları	C:$Extend$Usnjrnl:$J C:$MFT C:$LogFile

3.2.2. Programların Çalıştırılma Kayıtları

Windows tabanlı bilgisayarlarda, belirli programların veya uygulamaların ne zaman çalıştırıldığı, ne sıklıkta kullanıldığını, bunlara kimin eriştiğini tespiti ve vakaları ilerletmek için zaman çizelgeleri oluştururken her analizci programların çalıştırılma kayıtlarını analiz etmektedir.

Genel olarak programların çalıştırılma kayıtları, sistem artifactleri, kayıt defteri artifactleri, kullanıcı artifactleri olarak 3 başlık altında toplanabilir. Windows dosya sistemi üzerinde yer alan çalıştırılabilir dosyalara ait kayıtların tutulduğu kalıntılar Şekil 3.4'de yer almaktadır.



Şekil 3.4. Programların Çalıştırılmasına İlişkin Tutulan Kayıtların Sınıflandırılması

UserAssist

UserAssist, bir Windows makinesinde yürütülen programların tablosunu, çalışma sayısı ve son yürütme tarihi ve saati ile birlikte görüntüler.

Shimcache

Windows Shimcache, çalıştırılan programlarla uyumluluk sorunlarını izlemek için Microsoft tarafından Windows XP'den başlayarak oluşturulmuştur. Önbellek, işletim sistemine bağlı olarak çeşitli dosya meta verilerini depolamaktadır. Aşağıdaki maddelerde, bazı meta verilerine yer verilmiştir [11].

- Dosyanın Tam Yolu
- Dosya boyutu
- $ Standard_Information (SI) Son Değiştirilme zamanı
- Shimcache Son Güncelleme zamanı
- İşlem Yürütme İşareti

Amcache.hve

Amcache.hve, ilk olarak Windows 7 işletim sisteminde, programların son çalıştırılma tarihlerinin tuttuğu dosyadır. Aynı zamanda ilgili dosya daha önceden RecentFileCache.bcf (XP sistemlerde bulunmaktadır.) olarak yer almaktadır. Amcache.hve dosyası, Windows sisteminin farklı sürümleri arasında herhangi bir programın uyumluluğunu denetlemek için kullanılan Windows uygulama deneyimi ve uyumluluk özelliğinin aktif edilmesi sonucunda oluşturulmaktadır [12]. Programların sistemden silinmesinden veya kaldırılmasından sonra bile, Amcache.hve dosyasındaki kayıtlar silinmemektedir Amcache.hve bilgilerinin, programların silinmesinin zaman damgasını tahmin etmek için kullanılabilmektedir. Amcache.hve, Windows NT kayıt defteri (REGF) biçimine benzer hiyerarşik yapıyı izler [13]. Windows 7 ve sonrası

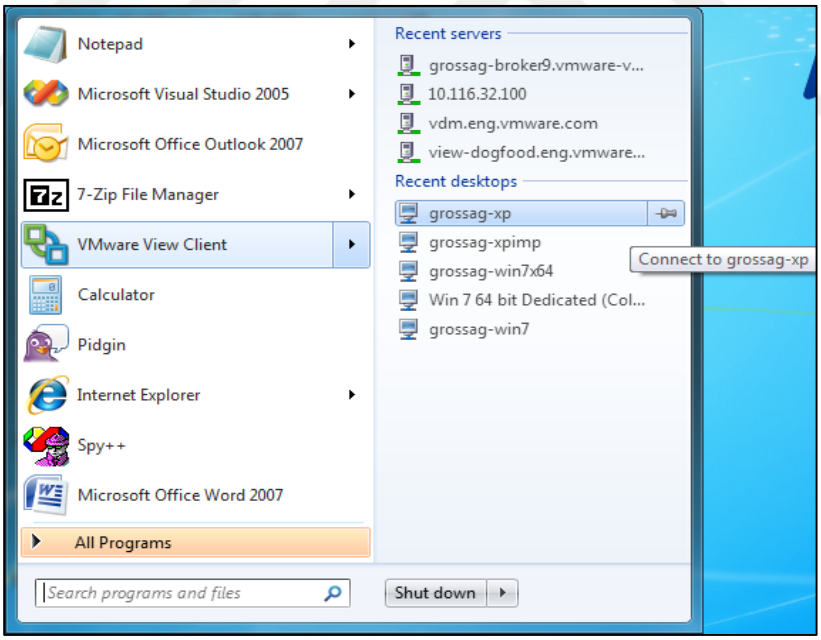
platformlarında bulunan Amcache.hve dosyası, son zamanlarda çalıştırılan programların kayıtlarını tutar. Tuttuğu en önemli kayıt ise çalıştırılan dosyanın SHA1 türünde imzasını da içermektedir.

Last-Visited MRU Kayıtları

Windows registry kayıtlarında, kullanıcılar tarafından gerçekleştirilen belirli aktivelerin bir çıktısı olarak MRU (Most Recently Used) kayıtlarında oluşturulur. RunMRU registry anahtarı, Başlat Menüsünde Çalıştır uygulamasında çalıştırılan yazılımları veya komutların kayıt altına alındığı anahtarları içermektedir [14].

Jump Lists

Jump List kavramı Windows 7 ile birlikte ortaya çıkan artifacts dosyasıdır. Kullanıcılar tarafından çok okunan, erişilen veya ziyaret edilen dosyalara, fotoğrafla, videolara veya web sitelerine erişimlerini daha hızlı gerçekleştirmelerine veya ilgili uygulama üzerinden en sık gerçekleştirilen aktiviteleri hızlıca erişim imkânı tanır [15]. Windows 7 görev çubuğu üzerinde yer alan uygulama ikonlarının üzerine sağ tıklayarak o uygulamaya ilişkin Jump List'e erişilebilir veya Başlat menüsünden ilgili uygulama üzerine gelinerek de Jump List'e erişilebilir. Şekil 3.5'de jumplist kalıntısına ait Windows arayüzünden gösterilen kayıtlar yer almaktadır.



Şekil 3.5. Jumplist Kaydı

System Resource Usage Monitor (SRUM)

Uygulamalara ait 30 ila 60 günlük geçmiş sistem performansını kaydeder. Sistem kaynak kullanımını izlemek için Windows 8 işletim sisteminden sonraki sürümlere dâhil edildi, özellikle ağ ve süreç ölçümleri yapmak için işletim sistemi tarafından kullanılan bir kaynaktır. SRUM uygulaması, geçmiş sistem kaynağı kullanımı hakkında önemli detaylardan oluşan sabit diskte depolanacak bir arka uç veri tabanı oluşturmaktadır [16]. Veri tabanı süreçlerle ilgili detayları

içerdiğinden, adli analistler, bu programdaki bilgileri, özellikle de Windows Sistemi üzerinde çalışan ve adli bilişim ve olay müdahalesi vakalarında son derece yararlı bilgiler olabilecek belirli bir programın ne kadar sürdüğünü öğrenmek için bu veri tabanındaki bilgileri kullanmaktadır.

Prefetch

Windows XP'de tanıtılan Windows Prefetch dosyaları, uygulama başlatma sürecini hızlandırmak için tasarlanmıştır. Ön bellek dosyaları, yürütülebilir dosyanın adını, bu yürütülebilir dosya tarafından kullanılan 'lerin Unicode listesini, yürütülebilir dosyanın kaç kez çalıştırıldığını ve programın en son çalıştırıldığı zamanı gösteren kayıtlar içermektedir [17].

BAM/DAM kayıtları

BAM, arka plan uygulamalarının etkinliğini kontrol eden bir Windows hizmetidir. Bu hizmet Windows 10'da yalnızca Fall Creators güncellemesinden sonra (sürüm 1709) mevcuttur. Sistemde çalıştırılan yürütülebilir dosyanın tam yolunu ve son yürütme tarih / saatini kayıt defterine kaydını sağlamaktadır.

Shortcut (LNK) Kayıtları

Kullanıcılar tarafından en son erişilen dosyaları tanımlamak için kullanılır ve bir adli bilişim incelemesinde, kullanıcı tarafından en son hangi uygulamaların görüntülendiğini ve hangi belgelerin görüntülendiğini belirlemek olay çözümünde kritik öneme sahip olabilir. Bir Windows işletim sisteminde, kullanıcı tarafından açılan dosyalar için bir kısayol dosyası, o kullanıcının hesabıyla ilişkilendirilmiş profil dizinindeki son dizinin altında oluşturulur [18]. Bu dosyalar, kullanıcının en son hangi dosyalara eriştiğini belirlemek için analiz edilebilir. Özellikle kullanıcı tarafından silinen dosyalar hakkında bilgiler yer almaktadır. LNK dosyalarında uygulamanın çalıştırıldığı makinenin MAC adres bilgisi de yer almaktadır.

Tablo 3.2'de programların çalıştırılmasına ilişkin kayıtların yer aldığı dizin bilgileri yer almaktadır.

Tablo 3.2. Programların Yürütülmesine İlişkin Kayıtlar

Artifact	Konumu
UserAssist	NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist
ShimCache	XP: SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatibility Win7/8/10:SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatCache
Amcache	C:\Windows\AppCompat\Programs\Amcache.hve
MRU	XP:NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU Win7/8/10:NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

Jump List	Win7/8/10:C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
SRUM	SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SRUM\Extensions {d10ca2fe-6fcf4f6d-848e-b2e99266fa89} Win8/10: C:\Windows\ System32\SRU\
Prefetch	C:\Windows\Prefetch
BAM/DAM	HKLM\SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}
Shortcut (LNK)	XP:C:\%USERPROFILE%\Recent Win7/8/10:C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\ Win7/8/10:C:\%USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent

3.2.3. Silinen Dosya Kayıtları

Adli bilişim ve olay müdahale süreçlerinde, silinen dosyalarla ilgili Windows sistemler üzerindeki kalıntıların analizi vaka için kanıt oluşturmaktadır. Örneğin, Siber saldırganın, Windows server sistemi üzerinde "mimikatz" yazılımı çalıştırdığını çıktılarını bir dosyaya kayıt ettiğini ve sonrasında sildiğini değerlendirelim. Vakayı analiz eden uzmanların, silinen dosya kayıtlarında söz konusu çıktının makine üzerinde oluşturulduğu ve sonrasında silindiğini tespit edecek ve vakanın süreci elde edilen kayıtlara göre şekillenecektir.

Thumbs.db Kayıtları

Makinede resimlerin bulunduğu dizindeki gizli dosya, daha küçük bir küçük resim grafiklerinde saklanır. thumbs.db resimler silinmiş olsa bile küçük resmin bir kopyasını saklar. Elde edilen kayıtlar aşağıdaki gibidir.

- Orijinal Resmin Küçük Resmi
- Belge Küçük Resmi - Silinmiş Olsa Bile
- Son Değiştirme Zamanı (Yalnızca XP)
- Orijinal Dosya Adı (Yalnızca XP)

Thumbcache

Resimlerin, ofis belgelerinin ve klasörlerin küçük resimleri thumbcache önbelleği adı verilen bir veri tabanında bulunur. Her kullanıcı, tarafından görüntülenen resim boyutlarına (küçük, orta, büyük ve ekstra büyük) göre veri tabanları yer almaktadır [19].

IE|Edge file://

IE uygulamasının web tarayıcı geçmiş bilgilerinin tutulmasının yanı sıra, açılan dosyalar ile ilgili bilgilerinde içermektedir. Geçmiş ayrıca yerel ve uzak (ağ paylaşımları yoluyla) dosya erişimini de kaydederek, sistemde her gün hangi dosyalara ve uygulamalara erişildiğini belirlememiz için analiz sağlamaktadır.

Recycle Bin Kayıtları

Geri dönüşüm kutusu, bir Windows dosya sisteminde silinen dosyalar ile ilgili kayıtların olduğu önemli kayıtları ve dosyaları içermektedir [20]. Konum altında yer alan kayıtlar ve bazı işlemler aşağıda belirtilmiştir.

- Gerçek konum ve dosya adı
- Silinme Tarihi
- Silinen verilerin geri kurtarılması

Windows sistemleri üzerinde silinen dosyalara ait kalıntılar Tablo 3.3'de belirtilen kayıtlarda yer almaktadır.

Tablo 3.3. Silinen Dosyalara Ait Kalıntılar

Artifact	**Konumu**
Thumbs.db	Tüm dizinler
Thumbcache	C:\%USERPROFILE%\AppData\Local\Microsoft\Windows\Explorer
IE|Edge file://	Internet Explorer: IE6-7 %USERPROFILE%\LocalSettings\History\History.IE5 IE8-9 %USERPROFILE%\AppData\Local\Microsoft\WindowsHistory\History.IE5 IE10-11 %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat
Search – WordWheelQuery	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery
Recycle Bin	Win7/8/10 • C:\$Recycle.bin

3.2.4. Kullanıcı Hesap kayıtları

Adli bilişim ve olay müdahalesi süreçlerinde, enfekte olmuş herhangi bir makine üzerinde oturum açan kullanıcının gerçekleştirdiği aktivitelerin tespiti için kullanıcı hesap kayıtlarının analizi sağlanmalıdır. Enfekte olan sunucuya veya makineye oturumun açıldığı ip adres veya bilgisayar adı bilgisi, başarılı açılan oturumların zamanı, başarısız oturum girişlerinin zamanı, oturumun açıldığı servisin tespiti sağlanabilir. Örneğin; bir domain ortamında, "appuser" kullanıcısının saldırgan tarafından ele geçirildiğine dair tespit sonrasında EDR veya SIEM üzerinde ele geçirilen kullanıcının aktivitelerine dair alarmların üretilmesi sağlanabilmektedir.

Last Login

Sistemin yerel hesaplarını ve eşdeğer güvenlik tanımlayıcılarını listeler. Söz konusu kayıtlarda kullanıcıların adları ve makine üzerindeki yetkileri yer almaktadır. Kayıt defteri anahtarında yalnızca son oturum açma zamanı yer almaktadır.

Oturum Açma Tipleri

Oturum Açma kayıtlarında, nereye bakacağımızı ve bulduğumuz verileri değerlendirebilirsek, bir sistemdeki hesap yetkileri hakkında bize çok özel bilgiler verebilir. Oturum açma işleminin tarihini, saatini, kullanıcı adını, ana bilgisayar adını ve başarı / başarısızlık durumunu bize bildirmenin yanı sıra, Logon Events ayrıca bir oturum açma girişiminin tam olarak ne şekilde yapıldığının tespitini sağlar.

Olay günlüğü kaydında yer alan oturum açma durumları Tablo 3.4'de sunulmuştur.

Tablo 3.4. Oturum açma tipine ait bilgileri

Oturum açma tipi	Açıklama
2	Logon via console
3	Network Logon
4	Batch Logon
5	Windows Service Logon
7	Credentials used to unlock screen
8	Network logon sending credentials (cleartext)
9	Different credentials used than logged on user
10	Remote interactive logon (RDP)
11	Cached credentials used to logon

Success/Fail Logons Kayıtları

Oturum açma girişimleri için hangi hesapların kullanıldığını belirlenir. Güvenliği ihlal eden hesaplar için aktivitelerin takibi yapılmalıdır [21].

Olay günlüğü kayıtlarında oturum aktiviteleri ile ilgili EventID bilgisi ve açıklamaları Tablo 3.5'de sunulmuştur.

Tablo 3.5. Event ID Bilgileri

EventID	Açıklama
4624	Successful Logon
4625	Failed Logon
4634 | 4647	Successful Logoff

4648	Logon using explicit credentials (Runas)
4672	Account logon with superuser rights (Administrator)
4720	An account was created
4726	An account was deleted

Services Events

Windows işletim sistemine sahip makineler üzerinde oluşturulan servislerin kontrolü sağlanmalıdır. Önyükleme sırasında çalışan şüpheli hizmetler için günlükleri analiz edilmesi ve şüpheli bir güvenlik ihlali anında başlatılan veya durdurulan hizmetler incelenmelidir.

Windows sistemleri üzerinde oluşturulan servislere ait kayıtlar Tablo 3.6'da sunulmuştur.

Tablo 3.6. Servis Durum Tipleri

EventID	**Açıklama**
7034	Service crashed unexpectedly
7035	Service sent a Start/Stop control
7036	Service started or stopped
7040	Start type changed (Boot | On Request | Disabled)
7045	A service was installed on the system (Win2008R2+)
4697	A service was installed on the system

Son kullanıcı aktivitelerine ait kayıtlar yer alacağı kalıntı bilgileri ve konumu Tablo 3.7'de yer almaktadır.

Tablo 3.7. Kullanıcı Aktivite Tespitine İlişkin Arfitact Kayıtları

Artifact	**Konumu**
Last Login	C:\windows\system32\config\SAM SAM\Domains\Account\Users
Logon Types	Win7/8/10: C:\Windows\System32\winevt\Logs\Security.evtx Event ID 4624
Success/Fail Logons	Win7/8/10: C:\Windows\System32\winevt\Logs\Security.evtx
Services Events	Win7/8/10: C:\Windows\System32\winevt\Logs\System.evtx Win7/8/10: C:\Windows\System32\winevt\Logs\Security.evtx

3.2.5. Bilgisayara takılan harici disk kayıtları

Adli bilişim incelemelerinde, Windows işletim sistemine sahip makinelere takılan herhangi bir harici disk kayıtlarının tespiti yapılmalıdır. Registry kayıtlarında, takılan diskin seri numarası, takılma tarihi ve takılma sayısı gibi kayıtlar yer almaktadır. Bu durumu sadece fiziksel olarak takılan disk olarak değerlendirmeyelim, günümüzde gelişmiş saldırgan gruplar(APT), farklı teknikler kullanarak kurumsal ağ üzerinde hızlı yayılım göstermektedir. Bu yayılımı sağlayan aktivitelerden birisi ise, bir sunucuda bulunan diski veya ortak alanı başka makinelere mount ederek sağlayıp veri kaçırılabilir veya zararlı dosyalara hızlıca erişebileceği bir ortam oluşturabilir.

Drive Letter and Volume Name Kayıtları

Makineye takılan USB aygıtlarının ve disk bölümlerinin son sürücü harfinin tespiti sağlanabilmektedir. Ayrıca GUID atayıp, cihazı takan kullanıcıyı tanımlamak için kullanılacaktır. Bu anahtarın son yazma süresi, aynı zamanda aygıtın o kullanıcı tarafından makineye en son takıldığı zamanı belirtir [22].

Volume Serial Number kayıtları

Makinelere takılan harici belleklere ve mount edilen disklere ait seri numarası kayıtları yer almaktadır.

Volume Mapped network drives kayıtları

Aynı ağ üzerinde yer alan makineler üzerinde disk paylaşımları yapılmaktadır. Saldırgan gruplar bu alanları kullanarak kurumsal ağ üzerinde hızlı yayılım sağlamaktadır. Olay müdahalesi süreçlerinde bu kayıtların analiz edilmesi ve alanlara erişimler konusunda EDR, SIEM üzerinde kurallar oluşturulmalıdır.

Tablo 3.8'de paylaşımlı veya paylaşımsız olarak kullanılan alanlara ait kayıtlar yer almaktadır [23].

Tablo 3.8. Bilgisayara Takılan Disklere Ait Artifacts Kayıtları

Artifact	Konumu
Drive Letter and Volume Name	Win7/8/10: SOFTWARE\Microsoft\Windows Portable Devices\Devices SYSTEM\MountedDevices NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2 XP: SYSTEM\CurrentControlSet\Enum\ USBSTOR
Volume Serial Number	SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ ENDMgmt
Mapped network drives	Win7/8/10: HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU
First/Last Times	(Win7/8/10 Only) System\CurrentControlSet\Enum\USBSTOR\Ven_Prod_Version\USBSerial#\Properties\{83da6326-97a6-4088-9453-a19231573b29}\####

3.3. Artifact Kayıtların Windows Sistemlere Göre Sınıflandırılması

Olay müdahale veya adli bilişim analistlerinin, herhangi bir güvenlik ihlalinin tespiti ve takibi için Windows işletim sistemlerinde Artifacts kayıtlarını analiz etmesi gerekebilir. Analizcinin, incelediği Windows sistemlerde yer alan artifacts kayıtlarına ve konumları hakkında bilgisi olması gerekmektedir. Olayın durumuna göre doğru artifact kaydını incelemelidir. Artifact kayıtları ve kayıtlarının yer aldığı Windows işletim sistemleri Tablo 3.9'da sınıflandırılmıştır.

Tablo 3.9. Artifact Kayıtlarının İşletim Sistemlerine Göre Sınıflandırılması

Kategori	Artifact	Windows XP	Windows VISTA	Windows 7	Windows 8	Windows 10
Registry Hive	SAM	✓	✓	✓	✓	✓
	SECURITY	✓	✓	✓	✓	✓
	SOFTWARE	✓	✓	✓	✓	✓
	SYSTEM	✓	✓	✓	✓	✓
	NTUSER.DAT	–	✓	✓	✓	✓
	DEFAULT	✓	✓	✓	✓	✓
	USRCLASS.DAT	✓	✓	✓	✓	✓
File System	$MFT	✓	✓	✓	✓	✓
	$Logfile	✓	✓	✓	✓	✓
	$J (Journal)	✓	✓	✓	✓	✓
User or System	Amcache	–	–	✓	✓	✓
	Prefetch	✓	✓	✓	✓	✓
	Shimcache	✓	–	✓	✓	✓
	UserAssist	✓	✓	✓	✓	✓
	SRUM	–	–	–	✓	✓
	Jump Lists	–	–	✓	✓	✓
	Shellbags	–	–	✓	✓	✓
	Shortcut (LNK)	✓	✓	✓	✓	✓
	Audit log (.evtx)	–	–	–	✓	✓
	Audit log (.evt)	✓	✓	✓	–	–

4. TRİYAJ TOPLAMA YÖNTEMLERİ

Bir Windows aktif dizini üzerinde yaklaşık 100 makinenin enfekte olduğunu veya güvenliğinin ihlal edildiğini değerlendirelim. Bu 100 adet makinenin sabit disklerin fiziksel veya mantıksal kopyasını almak, disk sayısına ve boyutuna göre değişiklik gösterebileceğinden ötürü ortalama 1 - 2 saat sürmektedir. Saldırganın aktif dizin üzerindeki yayılımını durdurmak için, enfekte olmuş makinelerde hızlıca disk imajı almak yerine, bazı önemli dosya sistem, kullanıcı aktivite ve günlük log kayıtlarını içeren veriler toplanabilir. Bu verilerin toplama türüne "**triyaj alma**" denir. Böylece bir makine üzerinde yaklaşık 5 – 10 dakika arasında triyaj kaydın alınması ve toplu analiz yöntemleri ile analizi sağlaması, olay müdahalesi süreçlerini hızlandırmaktadır. Her diskin imajını almak yerine bazı önemli dosyaların toplanması analiz için yeterli olabilir [24].

Ayrıca triyaj, Olay Müdahale sürecinde, makineler üzerinde gerçekleşen kötücül aktivitelerin hızlı tespitini sağlamak için makineden otomatik olarak bilgi toplama şeklidir. Aktiviteye göre, analizcinin takibi ve analizi değişiklik göstereceğinden dolayı makine üzerinde toplanması gereken veriler ve triyaj alma yöntemleri de değişiklik göstermektedir.

Makine üzerinde anlık olarak çalışan processler, komut satırı, ağ bağlantıları, ortak alan erişim kayıtları, zararlı dosyaların konum bilgileri gibi verilerin toplanması olayı sistemin triyaj kaydın oluşturulması şeklinde değerlendirilebilir [25].

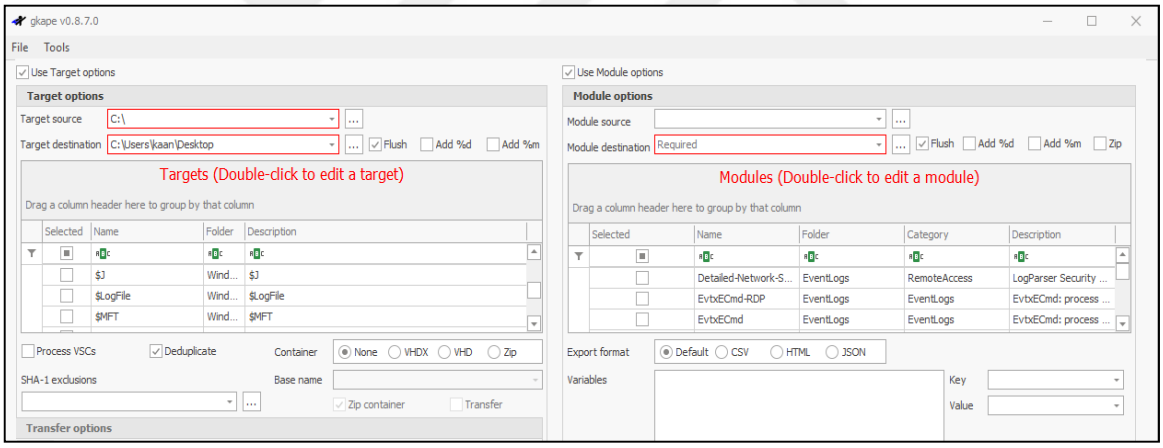
4.1. Local makinelerde Triyaj Toplama

Adli bilişim ve olay müdahale uzmanının, fiziksel olarak eriştiği güvenlik ihlali yaşanan Windows sistemine sahip makine üzerinde disk imajı elde etmeden triyaj veri toplayabilmektedir.

4.1.1. Kroll Artifact Parser and Extractor (KAPE)

Kroll Artifact Parser and Extractor (KAPE), öncelikle bir cihazı veya depolama konumunu hedefleyen, adli bilişim ve olay müdahalesinde analizi sağlanan, güvenlik ihlali ile artifactleri (analize göre) bulan ve birkaç dakika içinde toplayan programdır. KAPE, hızı nedeniyle araştırmacılara göre daha kritik ve önceliklendirilmiş sistemlerinden triyaj toplamak için kullanılır. Ek olarak KAPE, toplanan verilerin(Artifactlerin) toplu veya tekil analizini sağlamaktadır [26]. KAPE yazılımın 2 temel kullanımı mevcut olup şu şekildedir; dosyaları toplanması ve toplanan dosyaları bir veya daha fazla programla analiz edilmesini sağlamaktadır. KAPE kendi başına aksiyon almaz; daha ziyade, yapılandırma dosyalarını anında okuyarak ve bu dosyaların içeriğine bağlı olarak dosyaları toplayarak ve işleyerek elde edilirler. KAPE yazılımına analizci tarafından modül ekleme veya yazılımın kullanım amacını genişletme açısından eklemeler yapılabilmektedir. Ayrıca, KAPE'in kullanımı SANS eğitmenleri tarafından desteklenmektedir [27].

KAPE yazılımı hem GUI(GKape) hem de komut satırı(kape) olarak yer almaktadır. GKAPE'in arayüzüne ilişkin ekran görüntüsü Şekil 4.1'de sunulmuştur.



Şekil 4.1. KAPE Yazılımı

KAPE yazılımı parametre olarak verilen modüllere göre, çalıştırıldığı makine üzerinde veri toplamaktadır. Modüller içerisinde de toplanması istenen artifacts kaydının adı ve konumu yer almaktadır. KAPE yazılımı ile makine üzerinde triyaj verilerinin toplanmasında en çok "**!SANS_Triage.tkape**" isimli modül kullanılmaktadır.

"**SANS_Triage.tkape**" modülünün içeriği Şekil 4.2'de verilmiştir.

```
        Name: Event logs Win7+
        Category: EventLogs
        Path: C:\Windows.old\Windows\System32\winevt\logs\
        FileMask: '*.evtx'

# Evidence of Execution
    -
        Name: Prefetch
        Category: Prefetch
        Path: C:\Windows\prefetch\
        FileMask: '*.pf'
    -
        Name: Prefetch
        Category: Prefetch
        Path: C:\Windows.old\Windows\prefetch\
        FileMask: '*.pf'
```

Şekil 4.2. SANS Triage Artifact

"**SANS_Triage.tkape**" modülü ile hedef sistemlerden toplanan artifacts kayıtları Tablo 4.1'de sunulmuştur.

Tablo 4.1. SANS Modül Triage Kayıtları

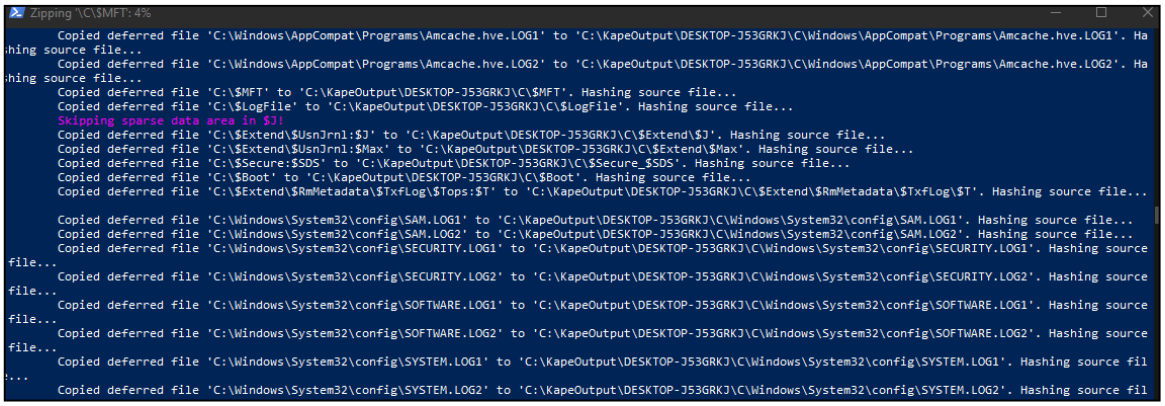
Event Logs	LNK files
Prefetch	$Recycle.Bin
RecentFileCache	System Registry Files(SYSTEM, SOFTWARE, SAM, NTUSER.DAT, UsrClass.dat, *.LOG*)
Amcache	Scheduled Tasks
Syscache	SRUM
PowerShell Console Log	Thumbcache.db
$MFT	Outlook PST and OST files
$LogFile	Skype
$J	Web Browser Artifacts

Tablo 4.2'de KAPE yazılımına ait parametreler ve açıklamaları yer almaktadır.

Tablo 4.2. KAPE Parametreleri

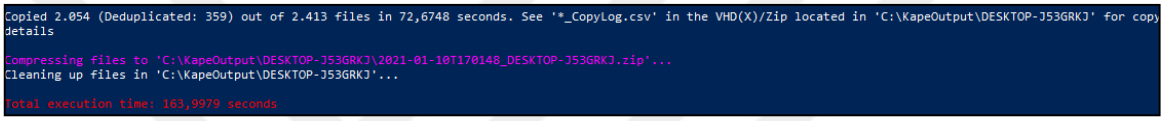
Parametre	**Değer**	**Açıklama**
--tsource	C:	C:\ volume içerisindeki artifact kayıtları topla
--tdest	C:\KapeOutput\%m	Elde edilen kayıtlar "**C:\KapeOutput**\" dizini altında hostname adına sahip klasör ile kayıt et
--tflush		Recursive Mod Kullan
--target	!SANS_Triage	Modül içerisinde yer alan kayıtlar elde et
--zip	%m	Hostname adına sahip zip dosyasında kayıtları ekle

"**Kape.exe --tsource C: --tdest C:\KapeOutput\%m --tflush --target !SANS_Triage --zip %m**" komutu ile hedef makine üzerindeki triyaj kayıtlarının toplanması gerçekleştirilecektir. KAPE yazılımın çalıştırıldığında ekrana sunulan çıktı Şekil 4.3'de sunulmuştur.



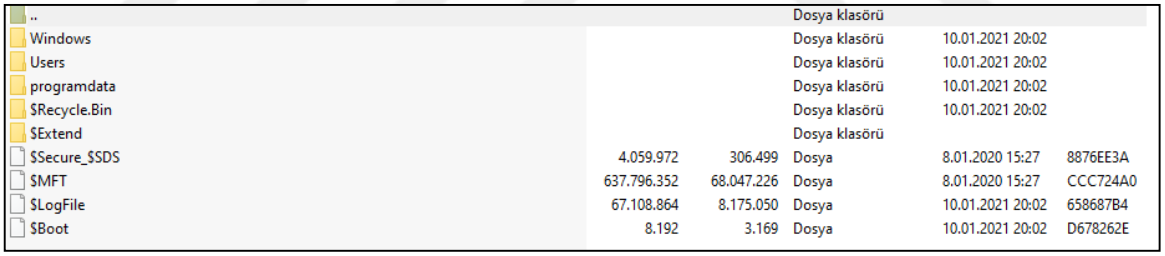
Şekil 4.3. KAPE yazılımı ile triyaj kaydının elde edilmesi

KAPE ile **"!SANS_Triage**" modülünde yer alan artifactleri kopyalaması ve sıkıştırması yaklaşık 3 dakika sürdüğü görülmüştür. KAPE yazılımın çalışma süresi Şekil 4.4'de sunulmuştur.



Şekil 4.4. KAPE Yazılımın triyaj kayıtlarını toplama süresi

Elde edilen triyaj kayıtlarına ilişkin ekran görüntüsü aşağıdaki gibidir. Elde edilen kayıtlar ile adli bilişim ve olay müdahale uzmanı hızlı bir şekilde analiz işlemi gerçekleştirmektedir. KAPE yazılımı ile elde edilen dosya sistem ve uygulama kayıtları Şekil 4.5'de yer almaktadır.



Şekil 4.5. KAPE ile Toplanan Veriler

4.1.2. FTK Imager

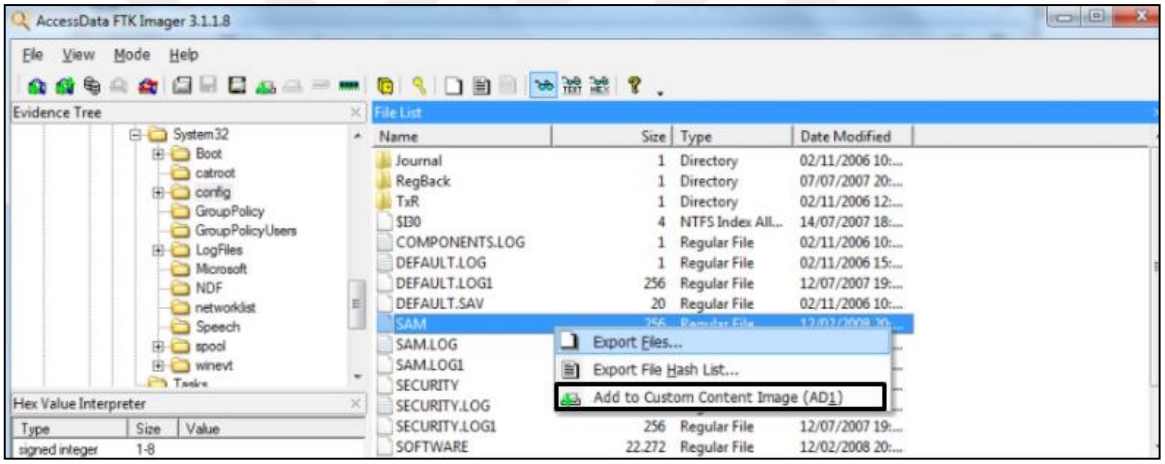
FTK yazılımı ile adli bilişim analizi için hedef sistemlerde yer alan disklerin fiziksel veya mantıksal imajını elde edilebilir [28]. FTK yazılımını kullanarak, bir disk bölümün dosyaları arasından triyaj kaydı toplanabilir.

FTK yazılımın "**Custom Contect Image**" özelliği ile disk imajı elde etmeden belirli dosyaların ".**ad1**" formatında kaydı oluşturabilir [29]. Hedef sistem üzerinde triyaj toplamak isteyen analizci, FTK aracı ile disk bölümlerini gezinerek, manuel olarak dosya sistem, registry, amcache vs gibi dosyaları "**Custom Contect Image**" alanına ekleyerek triyaj kaydı alabilir [30].

Analizci, alınan triyaj kayıtlarının depolandığı ".ad1" formatındaki dosyayı tekrardan FTK yazılımı ile okuyabilir, triyaj kayıtlarını tek tek dışarıya çıkartıp analizini sağlayabilir.

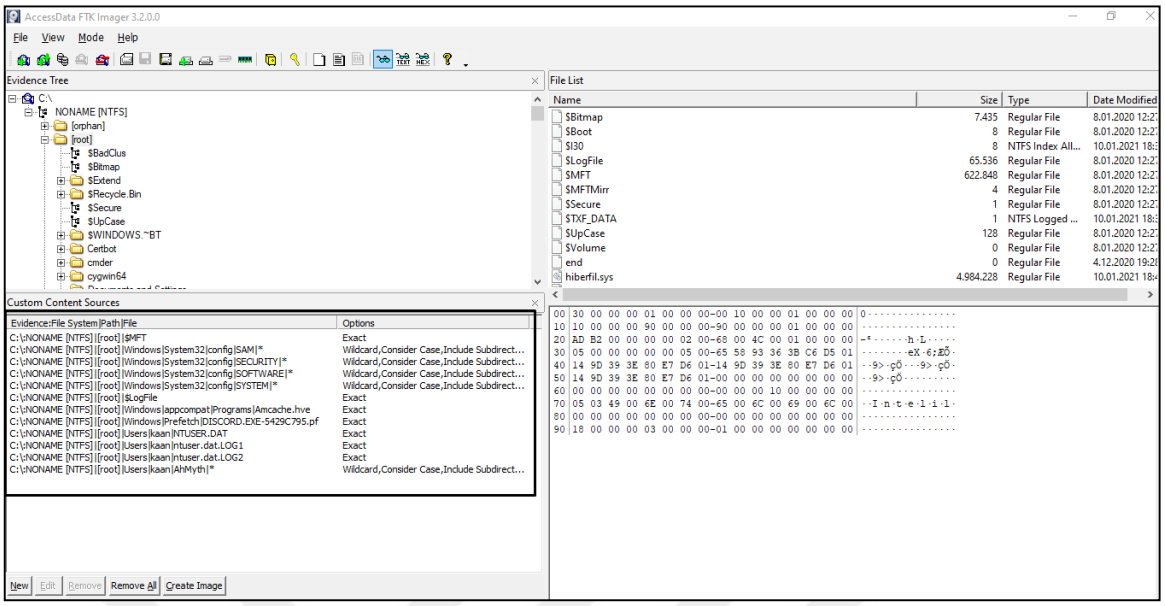
FTK yazılımı ile triyaj kayıt oluşturma adımları aşağıdaki gibidir.

Adım 1 - Şekil 4.6'da Dosya sistem, olay günlüğü veya registry dosyalarının "**Custom Contect Image**" alanına eklenmesine ilişkin ekran görüntüsü sunulmuştur.



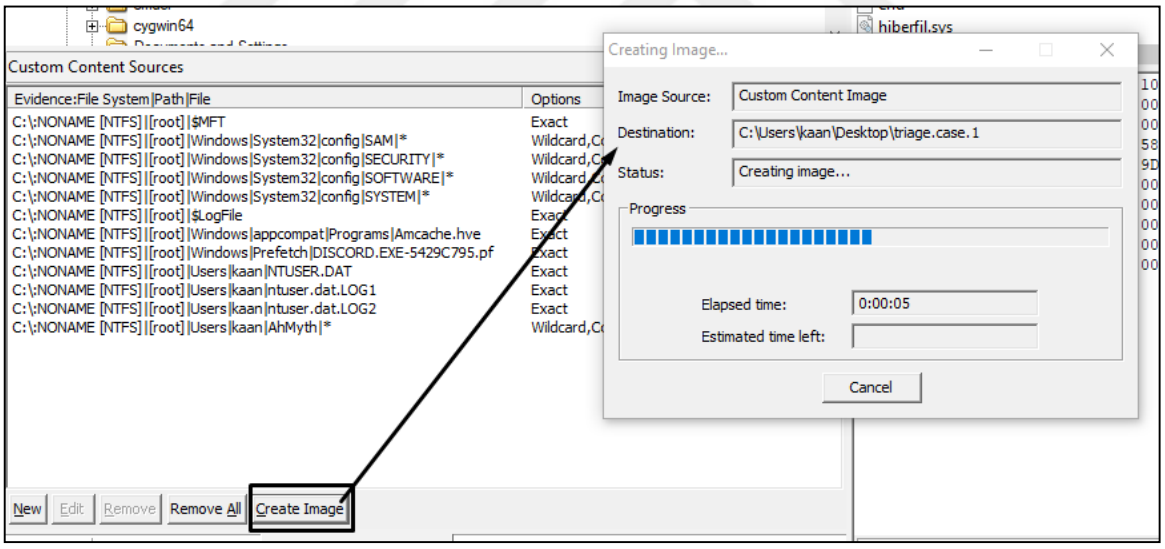
Şekil 4.6. FTK ile özel kayıtların eklenmesi

Adım 2 – Şekil 4.7'de toplanan kayıtlara ait bilgi yer almaktadır.



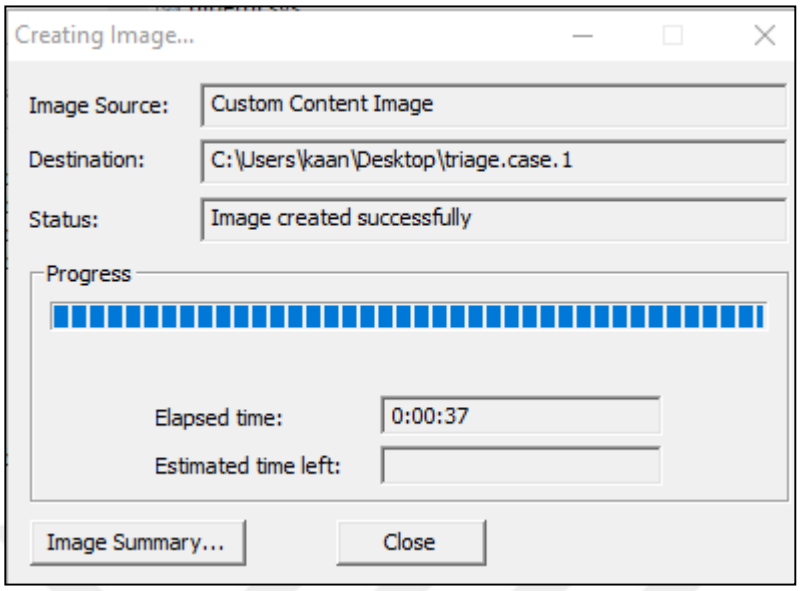
Şekil 4.7. FTK ile toplanan kayıtların bilgileri

Adım 3 – Şekil 4.8'de toplanan artifact dosyalarına ait triyaj imajının oluşturulmasına ait işlem sunulmuştur.



Şekil 4.8. FTK Imager yazılımına ait triyaj toplama süreci

Adım 4 – Şekil 4.9'da triyaj kaydının başarılı şekilde oluşturulmasına ilişkin çıktı sunulmuştur.



Şekil 4.9. FTK yazılımın başarılı olarak triyaj kayıtlarını özel imaj içerisinde oluşturması

FTK yazılımı ile hedef sistemlerde triyaj toplama aşaması KAPE yazılımın aksine manuel olarak yapılmaktadır. Yani analizci tek tek analiz edeceği artifacts dosyalarını özelleştirilmiş imaj içerisine ekleyip triyaj kaydını oluşturmaktadır [31]. Bu yöntemle analizcinin, bir Windows dosya sisteminde artifactlerin yer aldığı konumlarını bilmesi ve artifacts toplarken dikkatli olması beklenmektedir.

4.2. Uzak makinelerde triyaj kaydın alınması

Windows aktif dizin ortamında, yer alan makinelere fiziksel erişim sağlamadan uzaktan triyaj kaydı elde edilmektedir. Bu sayede olay müdahale ve adli bilişim uzmanı, hedef makine üzerindeki zararlı aktivitelerin tespiti için toplaması gereken triyaj kayıtlarını uzaktan alabilir.

4.2.1. EDR ajanları ile triyaj veri toplama

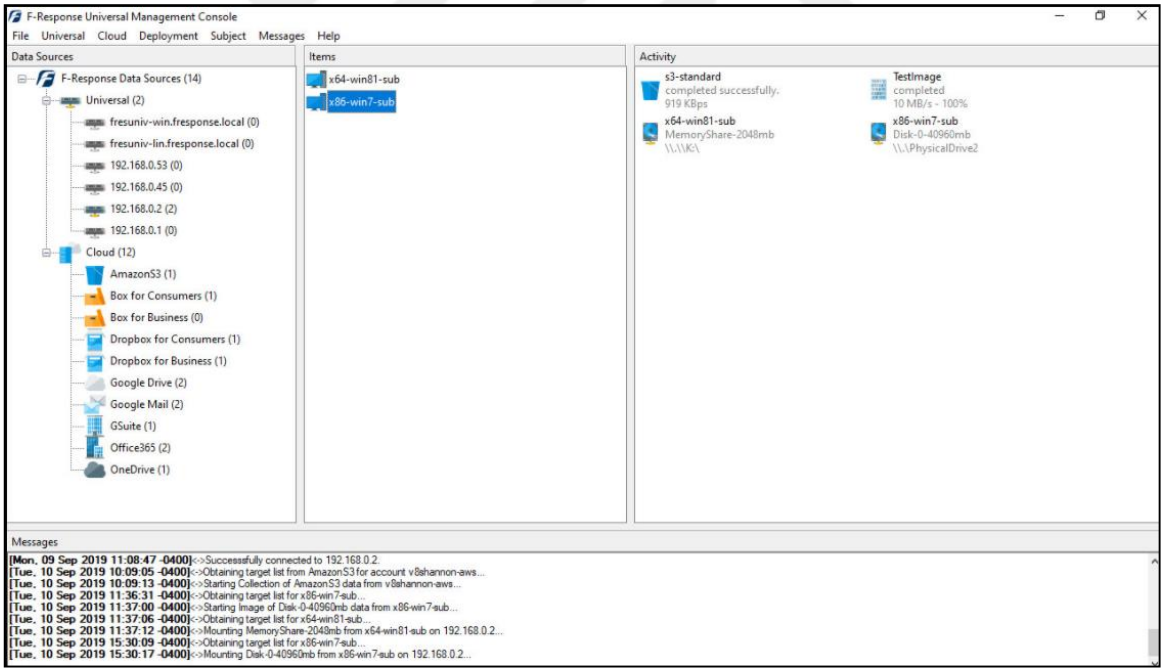
Analizci, EDR ajanı ile uzakta bulunan makine üzerinde canlı analiz yapabilir ve komut satırından KAPE programını çalıştırarak triyaj kayıt elde edilebilir [32]. Bazı EDR ürünlerinde hedef makine üzerinde triyaj kaydın elde edilmesi için arayüz mevcuttur.

4.2.2. SCCM Aracılığıyla triyaj veri toplama

SCCM, Active Directory(üzerinde sunucu, bilgisayar, yazıcı ve kullanıcı bilgilerini tutan bir dizin servisidir) ile entegre ederek sisteme bağlı tüm bilgisayarın yönetimini gerçekleştirebilirsiniz. Domaine alınan her bilgisayar sisteme dahil olur ve bu entegrasyon ile bilgisayar üzerinde ki kullanıcı problemlerini kullanıcıların yanına gitmeden uzaktan çözebilme imkanı sunar. Ayrıca bilgisayarlar üzerine uzaktan yazılımların çalıştırılması sağlanabilir. Aynı şekilde KAPE tarzı yazılımlar ile hedef sistem üzerinde triyaj veri toplanabilir.

4.2.3. F-Response ile triyaj veri toplama

F-Response, uzak bilgisayardaki depolama cihazlarını, yerel veya disk olarak analizcinin bilgisayarında erişimi sağlamaktadır [33]. Bir nevi, uzakta yer alan bilgisayarın diskini analiz bilgisayarında mount edebilirsiniz. F-response uzaktan mount ettiği disk üzerinde yazma-okuma koruması sağlamaktadır. Analizci, bilgisayarına mount edilen uzaktaki bir makinenin disk bölümleri üzerinde triyaj kayıtlarını elde edebilirler. F-Response yazılıma ait ekran görüntüsü Şekil 4.10'da yer almaktadır.



Şekil 4.10. F-Response Yazılımı

4.2.4. Sistem araçları aracılığıyla triyaj veri toplama

Domain ortamında, ssh veya psexec sistem araçlarıyla hedef makinelere yetkili bir kullanıcı ile uzaktan erişim sağlayıp, triyaj toplamak için hazırlanan özel script dosyaları ile makinenin triyaj kaydı alınmaktadır [34]. Yetkili kullanıcı ile ilgili güvenlik cihazlarında alarm yazdırılmalıdır.

Komut: "**psexec /HEDEFİPADRES cmd /c .\kape.exe --tsource C: --tdest C:\triyaj\%m --tflush --target $LogFile,$MFT,Amcache –gui**"

5. ÇOKLU MAKİNELERDEN TRİYAJ TOPLAMA YÖNTEMLERİ

Kurumsal ağ üzerinde saldırganların zararlı aktiviteler gerçekleştirdiği Windows işletim sistemine sahip ve aynı domainde yer alan yaklaşık 50 adet makinelerden triyaj veri topladığımızı değerlendirelim. Öncelikle bu makinelere triyaj kaydını toplayacak yazılımların SCCM veya EDR üzerinden iletilmesi ve toplu olarak çalıştırılması sağlanmalıdır. 50 adet makinede çalışan triyaj toplama yazılımlarının makine üzerinde oluşturduğu kayıtları ortak bir alan iletmesi beklenmektedir. Bu sayede 50 adet makinenin triyaj kayıtları bir alanda yer alacak ve analizcinin bu kayıtlara ulaşması kolaylaşacaktır.

Triyaj toplama yazılımlarının elde ettikleri kayıtları ortak bir alana ileteceği özelliklerinin olması gerekmektedir. Aksi takdirde triyaj kayıtları alınan makineler üzerinde oluşacak ve analizcinin bu kayıtlara ulaşması için tek tek triyaj yazılımının çalıştığı makinelere erişim sağlaması gerekecektir.

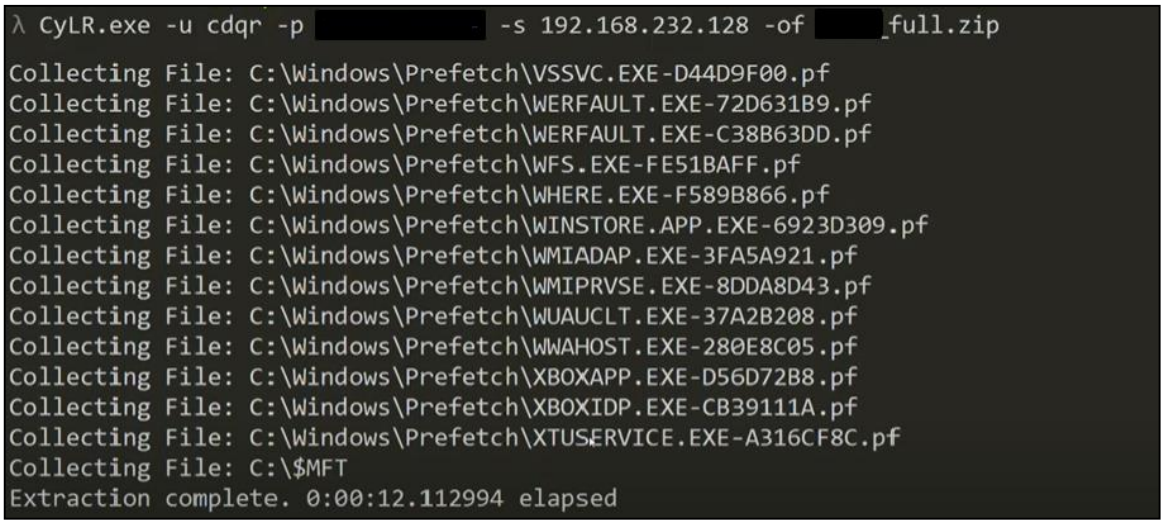
5.1. CyLR (Live Response Collection tool)

Açık kaynak kodlu CyLR (Live Response Collection tool) yazılımı hedef makine üzerinde topladığı triyaj kayıtlarını SFTP sunucuna transferini sağlayabilmektedir [35]. CyLR, yazılımı hedef makine üzerinde yer alan dosya sistem, kullanıcı aktivite ve registry hive dosyalarının triyaj kaydını oluşturmaktadır. KAPE gibi esneklik sağlamazken, kullanımı alanı ve toplayacağı dosya sayısı sınırlıdır. Açık kaynak kodlu CyLR yazılımı üzerinde analizcinin ihtiyaçlarına göre geliştirmeler yapılabilir.

Analistin, CyLR yazılımı ile triyaj verilerinin toplanması ve STFP alanına göndermesi için kullanılan komut şu şekildedir.

“**CyLR.exe -u username -p password -s 10.120.5.8”**

CyLR yazılımı, -u parametresi ile STFP alanına erişmek isteyen kullanıcı adı, -p parametresiyle SFTP alanının şifresini ve –s parametresiyle ise STFP alanının IP adresini içeren değerler almaktadır. CyLR yazılımı ile sadece port numarası 22 olan STFP alanında toplanan triyaj kayıtlarının gönderilmesini sağlamaktadır. CyLR yazılıma ait işlem çıktısı Şekil 5.1’de yer almaktadır.



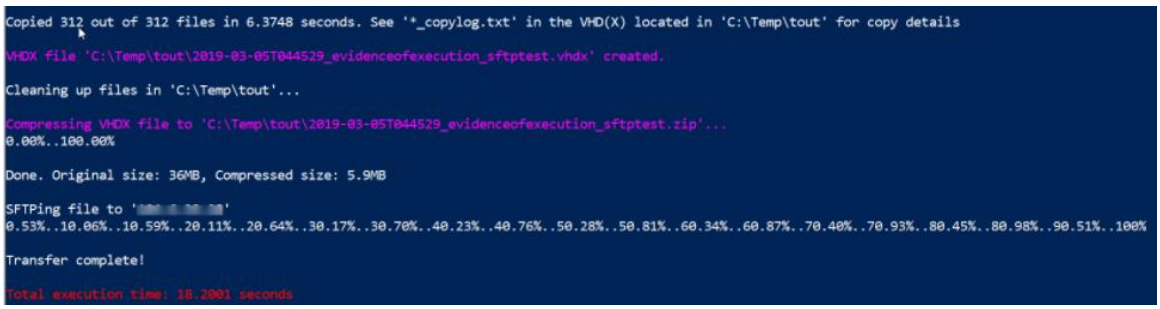
Şekil 5.1. CyLR Yazılımı

5.2. KAPE

Aşağıdaki komut ile KAPE yazılımı ile makine üzerinde toplanan triyaj kaydını SFTP alanına iletimini sağlayabilirsiniz.

.\kape.exe --tsource C: --tdest C:\triyaj --tflush --target $Boot,$J,$LogFile,$MFT,Amcache --scs 10.4.150.50 --scp 22 --scu root --scpw Password123!

KAPE ile toplanan triyaj kaydının ortak alana iletilmesine ilişkin çıktı Şekil 5.2'de yer almaktadır.



Şekil 5.2. KAPE ile Toplu Triyaj Kaydı Oluşturma

6. MATERYAL VE METOT

Olay müdahale çalışmalarında, kötücül aktivitenin kurumsal ağ üzerinde yayılımın tespiti ve analizi için cihazlardan dosya sistem ve uygulama kayıtları toplanmaktadır. Kayıtların hızlı şekilde toplanması ve olay müdahale analistinin önüne sunulması, kötücül aktivitenin tespiti ve engellenmesi hususunda önem arz etmektedir.

Bu tez çalışması kapsamında geliştirilen PS-TRIAGE yazılımı ile Windows aktif dizini üzerinde yer alan cihazlara uzaktan bağlanarak triyaj toplanmasını sağlamakla beraber toplanan triyaj kayıtlarının ön analizini gerçekleştirerek olay müdahale analistinin önüne çıktı olarak vermektedir.

Powershell betiği geliştirilmiş PS-TRIAGE isimli yazılıma ait kullanım ve detaylar aşağıdaki başlıklarda sunulmuştur.

6.1. Materyal

PS-TRIAGE yazılımın uçtan uça çalıştırılmasında kullanılan 3.parti yazılımlar/servisler Tablo 6.1'de belirtilmiştir.

Tablo 6.1. 3. Parti servis ve yazılımlar

Materyal	**Kullanım Amacı**
AmcacheParser.exe	Cihazlar üzerinden toplanan Amcache dosyasının parse edilmesi işleminde kullanılmaktadır.
RawCopy.exe	PS-TRIAGE yazılımı "RawCopy.exe" yazılımını, hedef makineye kopyalayarak dosya sistem kayıtlarının elde edilmesini sağlamaktadır.
Hobocopy.exe	PS-TRIAGE yazılımı "Hobocopy.exe" yazılımını, hedef makineye kopyalayarak triyaj kayıtlarının elde edilmesini sağlamaktadır.
7za.exe	Toplanan triyaj kayıtların, hedef makine üzerinde sıkıştırılmasını sağlamaktadır. Bu işlem ile toplanan triyaj kayıtlarının boyutunun daha az olmasını sağlamakla beraber, sıkıştırılan triyaj kaydının ortak alana taşınması sırasında ağ trafiğinde yükü azaltmaktadır.
Abuseipdb[.]com	Cihazlar üzerinden toplanan Netstat kayıtlarında yer alan gerçek IP adreslerinin, Abuseipdb[.]com servisi üzerinde API ile sorgulaması yapılmaktadır.

6.1.1. AmcacheParser yazılımı

Amcache.hve, programların çalıştırılması ilgili bilgileri depolamak için Microsoft tarafından oluşturulmuş bir kayıt defteri dosyasıdır [36]. Söz konusu dosya içerisinde aşağıdaki bilgiler Tablo 6.2'de sunulmuştur.

Tablo 6.2. Amcache.hve kaydında yer alan bilgiler

Çalıştırılabilir Dosya adı	Dosya açıklaması
Geliştirici İmza	Çalıştırılan dosyasının tam yolu
Çalıştırılabilir dosya sürümü	Son değiştirilme zamanı
Program Kimliği	Çalıştırılma zamanı
Dosya boyutu	SHA1 dosya karması

Amcache dosyasının parse edilmesi için kullanılan yazılım, "**Eric Zimmerman**" tarafından geliştirilmiştir [37].

6.1.2. RawCopy yazılımı

RawCopy, düşük seviyeli disk okuma kullanan ve $MFT'yi ayrıştırarak veri kümelerini çözen NTFS için bir dosya kopyalayıcıdır [38].

İşletim sistemi tarafından kullanılan herhangi bir dosyayı kopyalayabilmelidir. Kayıt defteri(Registry Hives), $MFT ve $LogFile gibi gibi NTFS sistem dosyalarını yedekleyebilmektedir.

6.1.3. Hobocopy yazılımı

"**Hobocopy.exe**", cihaz üzerinde dosya sistem katmanı seviyesinde yer alan dosyaları kopyalabilmek için geliştirilen bir yazılımdır [39].

6.1.4. 7za yazılımı

"**7za**", yazılımı Windows işletim sistemlerinde komut satırından, dosya veya klasörleri sıkıştırmak için kullanılmaktadır. Ayrıca, sıkıştırılmış dosyaları açmak için tercih edilen küçük boyutlu ve hızlı bir yazılımdır.

6.1.5. Abuseipdb servisi

Abuseipdb[.]com, bilgisayar korsanlarının, spam göndericilerin ve internetteki kötüye kullanım faaliyetlerinin yayılmasıyla mücadeleye yardımcı olan servistir. Kötü amaçlı aktiviteler ile ilişkilendirilmiş IP adreslerini bildirmeleri ve bulmaları için merkezi bir kara liste sağlayarak Web'i daha güvenli hale getirmeye yardımcı olmaktır [40].

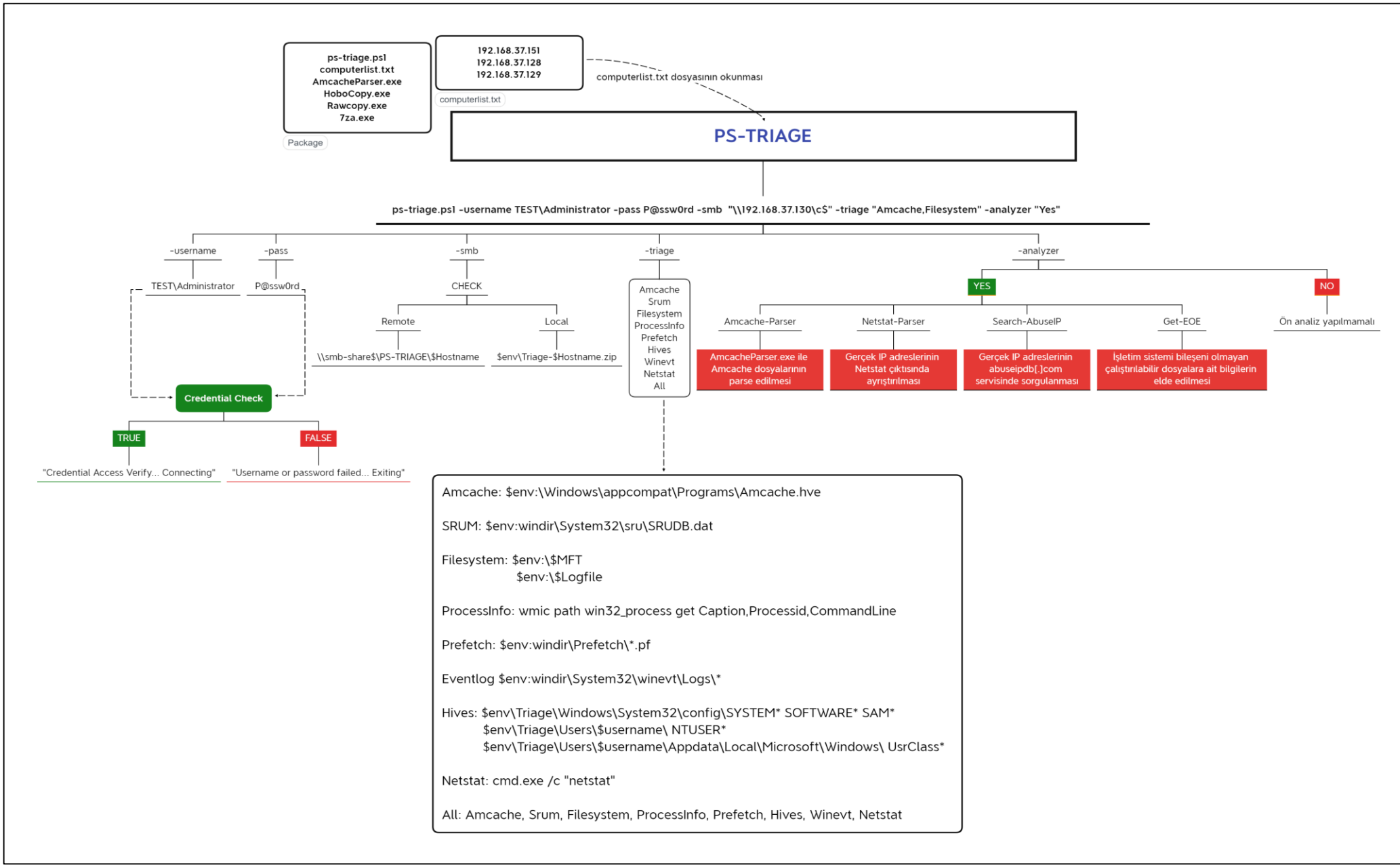
PS-TRIAGE yazılımı ise, cihazlar üzerinden topladığı IP adreslerini, Abuseipdb[.]com servisinde yer alan kara liste kontrolünü api yoluyla gerçekleştirmektedir.

6.2. Metot

Bu tez çalışmasında, olay müdahale aşamalarında Windows işletim sistemlerine sahip cihazlardan triyaj kayıtlarının toplanmasını sağlayan PS-TRIAGE isimli yazılım geliştirilmiştir. PS-TRIGAE yazılımın çalıştırılmasına ilişkin detaylı bilgiler bu başlığa ait alt başlıklarda verilmiştir.

6.2.1. PS-TRIAGE yazılımı akış şeması

PS-TRIAGE isimli yazılımın akış şeması Şekil 6.1'de sunulmuştur. Söz konusu şema üzerinde PS-TRIAGE yazılımına verilen parametreler ve açıklamaları "**6.2.4 Yazılım Parametreleri**" başlığı altında sunulmuştur.



Şekil 6.1. PS-TRIAGE yazılıma ait akış şeması

6.2.2. Gereksinimler

PS-TRIAGE yazılımın çalıştırılmasından önce, triyaj kaydı alınacak cihazlarda winrm servisi açık olmalıdır. Yazılım, winrm servisi ile triyaj kaydı alınacak cihazlara bağlanarak işlemler gerçekleştirmektedir.

Windows aktif dizini üzerinde yer alan cihazlarda winrm servisinin aktif olması için "**Enable-PSRemoting**", "**winrm quickconfig**" komutlarının çalıştırılması gerekmektedir [41]. PS-TRIAGE yazılımın çalıştırılacağı makinede çalıştırılması gereken komutlar ve açıklamaları Tablo 6.3'de belirtilmiştir.

Tablo 6.3. Yazılımın çalıştırılması için izinlerin verilmesi

Komut	**Açıklama**
Set-ExecutionPolicy RemoteSigned	Powershell ile geliştirilen yazılımlara güvenilmesi için çalıştırılan komuttur.
Set-Item WSman:localhost\client\trustedhosts -value *	Winrm servisi ile bağlantı sağlanacak cihazlara güvenilmesi için çalıştırılan komuttur.

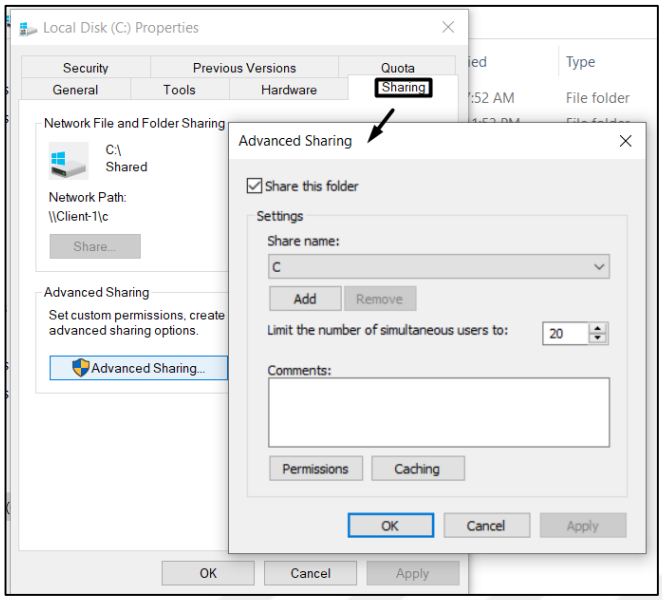
Tez çalışmasında, PS-TRIAGE yazılımın çalıştırılmasın kullanılan test ortamına ait bilgiler Tablo 6.4'de sunulmuştur.

Tablo 6.4. Test ortam bilgisi

İşletim Sistemi	**Cihaz Adı**	**Açıklama**
Windows Server 2019	Server-DC	Triyaj kaydı toplanacak cihaz
Windows 10 Pro 64 bit	Client-1	PS-TRIAGE yazılımın çalıştırılacağı ve triyaj kaydının toplanacağı cihaz
Windows 10 Pro 64 bit	Client-2	Triyaj kaydı toplanacak cihaz

PS-TRIAGE yazılımın, hedef makinelere winrm servisi ile bağlantı sağlayacağı yüksek yetkili hesap aktif dizin üzerinde tanımlanmalıdır. PS-TRIAGE yazılımına özel olarak tanımlanan hesabın aktiviteleri, güvenlik çözümleri(EDR, SIEM, EPP, AV) ile 7/24 ilgili ekipler ile takibi yapılmalıdır.

Triyaj kayıtların depolanacağı SMB uzak paylaşımlı alanın oluşturulması gerekmektedir. Söz konusu alan, tüm cihazların erişebileceği şekilde konumlandırılmalıdır. Windows sistemleri üzerinde uzak paylaşımlı alan aşağıdaki gibi tanımlanabilir. SMB uzak paylaşımlı alanın oluşturulmasına ilişkin ekran görüntüsü Şekil 6.2'de yer almaktadır.



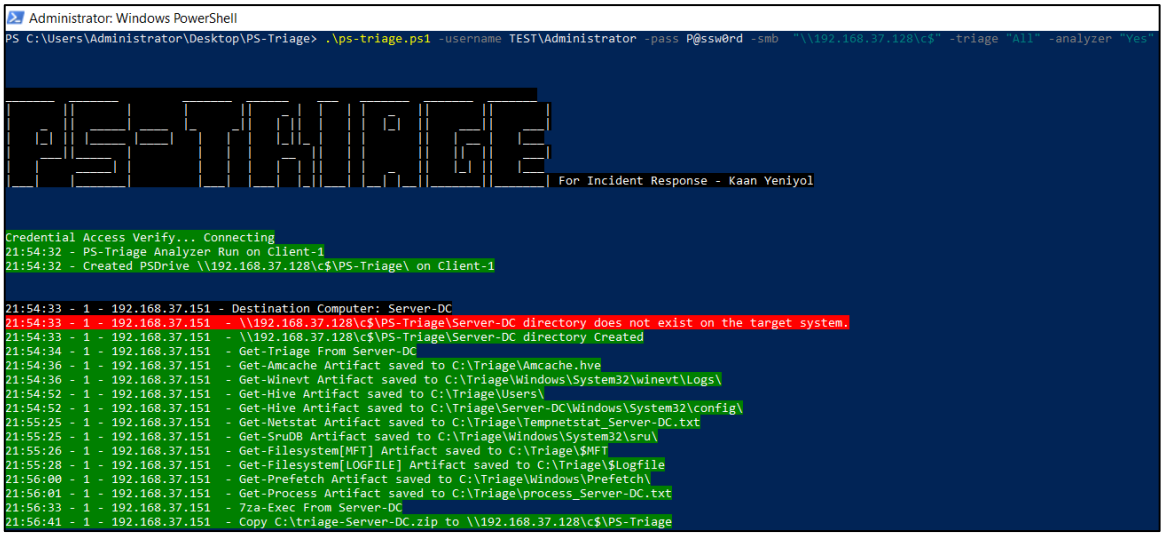
Şekil 6.2. Uzak paylaşımlı alanın oluşturulması

6.2.3. PS-TRIAGE Yazılımı

Windows aktif dizini üzerinde yer alan cihazların, PS-TRIAGE yazılımı ile triyaj kayıtları elde edilebilmektedir. Elde edilen triyaj kayıtlarından Amcache dosyasının analizi sağlanarak, cihazlar üzerinde çalışan şüpheli kayıtların ön analiz aşamasında çıktısı alınabilmektedir.

PS-TRIAGE yazılımı, powershell kod betiği ile geliştirilmiş olup Windows sistemleri üzerinde uyumlu olarak çalışmaktadır. Yazılım, toplanan triyaj kayıtları uzak paylaşım alanında veya hedef makine üzerinde kayıt edilmesini sağlayabilmektedir.

PS-TRIAGE isimli yazılımın çalıştırıldığında ekrana sunulan çıktı Şekil 6.3'de yer almaktadır.



Şekil 6.3. PS-TRIAGE yazılımına ait ekran görüntüsü

PS-TRIAGE yazılımı ile Windows işletim sistemlerinden toplanan kayıtlar ve konumları Tablo 6.5'de belirtilmiştir.

Tablo 6.5. Yazılım ile toplanan triyaj kayıtları

Artifact Kaydı	**Konum/Komut**
Amcache	$env:\Windows\appcompat\Programs\Amcache.hve
Eventlog	$env:windir\System32\winevt\Logs*
Registry Hives	$env\Triage\Windows\System32\config\
- Software*	$env\Triage\Users\$username
- System*	$env\Triage\Users\$username\Appdata\Local\Microsoft\Windows\
- Sam*	
- Ntuser*	
- UsrClass*	
MFT	$env:\$MFT
Logfile	$env:\$Logfile
SRUDB.dat	$env:windir\System32\sru\
Prefetch	$env:windir\Prefetch*.pf
Netstat çıktısı	netstat
Çalışan İşlemler ve Komut çıktısı	wmic path win32_process get Caption,Processid,CommandLine

Yazılım, aktif dizin ortamında oluşturulmuş yüksek yetkili hesap ile hedef makinelere winrm servisini kullanarak erişim sağlamaktadır.

Winrm ile erişim sağlanan makinelere, "**Rawcopy**", "**Hobocopy**" ve "**7za.exe**" yazılımları "**$env:\Triage**" isimli dizin altına kopyalanmaktadır. Hedef cihaz üzerinde "**Rawcopy**" ve "**Hobocopy**" yazılımları ile triyaj kayıtları "**$env:\Triage**" isimli dizin altında toplanmaktadır. Toplanan triyaj kayıtları, "**7za.exe**" yazılımı ile makine üzerinde sıkıştırılmakta olup uzak paylaşımlı alana veya yerel cihaz üzerinde depolanmaktadır.

PS-TRIAGE yazılımı ile analist, hedef makine üzerinde toplanması gereken triyaj kayıtlarını özelleştirebilir veya tüm triyaj kayıtlarını toplayabilmektedir. Elde edilen triyaj kayıtlarında ön analiz sonucu çıktı elde edilebilmektedir. PS-TRIAGE yazılımının hedef makine üzerinde gerçekleştirebileceği örnek çıktılar aşağıdaki Tablo 6.6'da yer almaktadır.

Tablo 6.6. Yazılıma ait örnek çıktılar

IP Adresi	Bilgisayar Adı	Sonuç
10.120.10.5	EXC01	\\192.168.37.130\c$\PS-Triage\EXC01 **directory Created** **Get-Triage From** EXC01 **Get-Amcache Artifact saved to** C:\Triage\Amcache.hve **Get-Hive Artifact saved to** C:\Triage\EXC01\Users\ **Get-Filesystem[MFT] Artifact saved to** C:\Triage\$MFT **7za-Exec From** EXC01 **Copy** C:\triage-EXC01.zip **to** \\192.168.37.130\c$\PS-Triage **Suspicious files run on** EXC01 **SHA1 Hash** : 7fc3b9a35ca5856e449a2c67371d1bf13d0be000 **Path** : c:\beacon.exe **Execution Time**: 2021-06-23 02:58:41
10. 120.10.7	DB01	\\192.168.37.130\c$\PS-Triage\DB01 **directory Created** **Get-Triage From** DB01 **Get-Amcache Artifact saved to** C:\Triage\Amcache.hve **Get-Filesystem[MFT] Artifact saved to** C:\Triage\$MFT **7za-Exec From** DB01 **Copy** C:\triage-DB01.zip **to** \\192.168.37.130\c$\PS-Triage **Suspicious files run on** DB01 **SHA1 Hash** : EXC01 **Path** : c:\windows\temp\mimi.exe **Execution Time**: 2021-06-19 17:01:47
10. 120.10.8	FTPSERVER	\\192.168.37.130\c$\PS-Triage\FTPSERVER **directory Created** **Get-Triage From** FTPSERVER **Get-Winevt Artifact saved to** C:\Triage\Windows\System32\winevt\Logs\ **Get-Hive Artifact saved to** C:\Triage\FTPSERVER\Users\ **Get-Hive Artifact saved to** C:\Triage\FTPSERVER\Windows\System32\config\ **Get-Netstat Artifact saved to** C:\Triage\Tempnetstat_FTPSERVER.txt **Get-SruDB Artifact saved to** C:\Triage\Windows\System32\sru\ **Get-Prefetch Artifact saved to** C:\Triage\Windows\Prefetch\ **Get-Process Artifact saved to** C:\Triage\process_FTPSERVER.txt **7za-Exec From** FTPSERVER
10. 120.10.12	CLIENT01	**AbuseIPDB Search Starting** Client01 **IP Adress :** 93.184.220.29 - Score : 0 **IP Adress :** 51.103.5.159 - Score : 28 **IP Adress :** 40.113.10.47 - Score : 0

6.2.4. Yazılım Parametreleri

PS-TRIAGE yazılımın çalıştırılmasında kullanılan parametreler ve açıklamaları Tablo 6.7'de yer almaktadır.

Tablo 6.7. PS-TRIAGE parametreleri

Parametre	Açıklama
-username	Hedef makinelere winrm servisi ile bağlantı sağlayacak kullanıcı adı
-pass	Hedef makinelere winrm servisi ile bağlantı sağlayacak kullanıcı parolası
-smb	Makineler üzerinde toplanan triyaj kayıtlarının taşınacağı uzak paylaşım adresi
-triage	Hedef makineler üzerinde toplanacak triyaj kayıtlarının belirlenmesi Kullanılması gereken değerler: - Amcache - Srum - Filesystem

	- ProcessInfo - Prefetch - Winevt - Netstat - All
-analyzer	Toplanan triyaj kayıtlarının ön analizinin sağlanması Kullanılması gereken değerler: - Yes - No

PS-TRAGE yazılımında kullanılan "**-triage**" parametresinin alabileceği seçenekler ve seçenekler bağlı olarak toplanan triyaj kayıtları Tablo 6.8'de sunulmuştur.

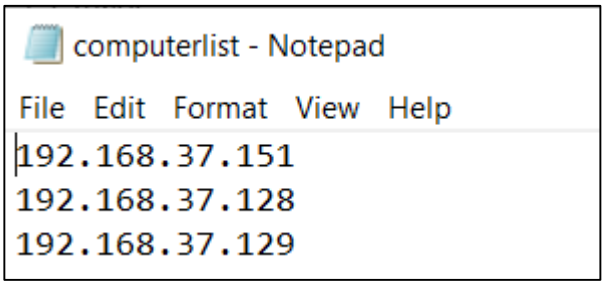
Tablo 6.8. PS-TRIAGE yazılımın ile toplanabilecek triyaj kayıtları

Seçenek	**Toplanan Triyaj Kayıtları ve Konumları**
Amcache	$env:windir\appcompat\Programs\Amcache.hve
SRUM	$env:windir\System32\sru\SRUDB.dat
Filesystem	$env:\$MFT
	$env:\$Logfile
ProcessInfo	wmic path win32_process get Caption,Processid,CommandLine
Prefetch	$env:windir\Prefetch*.pf
Eventlog	$env:windir\System32\winevt\Logs*
Hives	$env\Triage\Windows\System32\config\SYSTEM* SOFTWARE* SAM*
	$env\Triage\Users\$username\ NTUSER*
	$env\Triage\Users\$username\Appdata\Local\Microsoft\Windows\ UsrClass*
Netstat	cmd.exe /c "netstat"
All	Amcache, Srum, Filesystem, ProcessInfo, Prefetch, Hives, Winevt, Netstat

6.2.5. Triyaj Kayıtlarının uzak paylaşımlı alanda depolanması

PS-TRIAGE yazılımı ile toplu olarak cihazlar üzerinden triyaj kaydı toplanabilir ve toplanan triyaj kayıtları uzak paylaşımlı alanda depolanabilir. Bu yöntem ile analizciler toplanan triyaj kayıtlarına tek bir alan üzerinden ulaşabilir ve toplu analiz işlemlerini zaman kaybetmeksizin gerçekleştirebilirler.

Triyaj toplanması gereken makinelerin IP adresleri, "**computerlist.txt"** isimli metin dosyasında belirtilmelidir. "**computerlist.txt"** isimli metin dosyasına ait içerik Şekil 6.4'de verilmiştir.

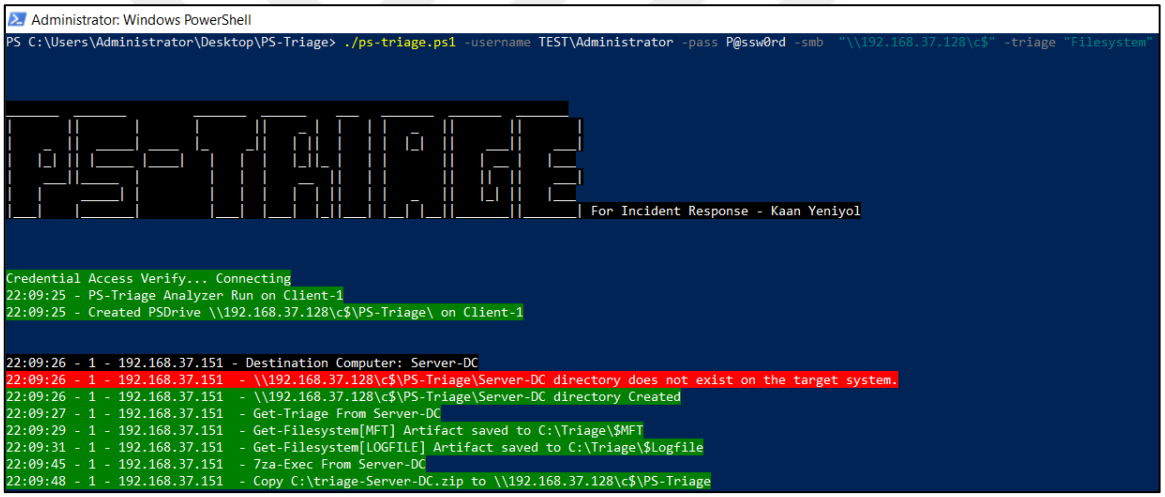


Şekil 6.4. Triyaj kaydı alınacak makineler

Dosya sistemi($MFT,$LOGFILE) kayıtlarının paylaşımlı alanda depolanması için gereken komut satırı aşağıdaki gibidir.

ps-triage.ps1 **-username** TEST\Administrator **-pass** P@ssw0rd **-smb** "\\192.168.37.128\c$" **-triage** "Filesystem"

Şekil 6.5'de yer alan ekran görüntüsünde 192.168.37.151(Server-DC) IP adresli cihaz üzerinden dosya sistem kayıtlarının elde edilmesine ilişkin çıktılar yer almaktadır.

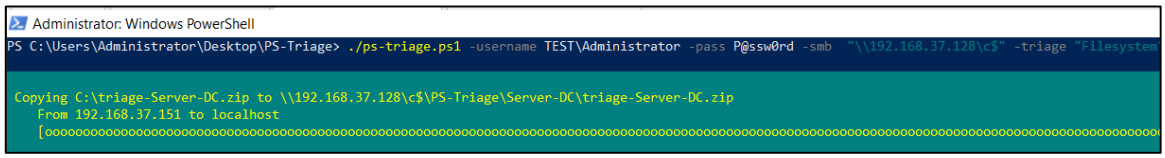


Şekil 6.5. "Server-DC" isimli cihazdan triyajın elde edilmesi

Şekil 6.5'de yer alan ekran görüntüsünde ise Server-DC isimli cihazın triyaj kaydı şu şekilde elde edilmektedir.

- "**\\192.168.37.128\c$**" paylaşımlı alanda "**PS-TRIAGE**" isimli klasör oluşturulması,
- Server-DC isimli cihaza ilgili kullanıcı adı ve şifre ile oturum açılması,
- "**Rawcopy.exe**", "**Hobocopy.exe**" ve "**7za.exe**" isimli yazılımların hedef makine üzerinde kopyalanması
- "**$MFT**" ve "**$Logfile**" dosya sistem kayıtlarının hedef makine üzerinde "**C:\Triage**" dizini altında kayıt edilmesi
- "**C:\Triage**" isimli dizinin "**C:**" isimli disk bölümü altında "**triage-Server-DC.zip**" isimli dosya olarak sıkıştırılması,

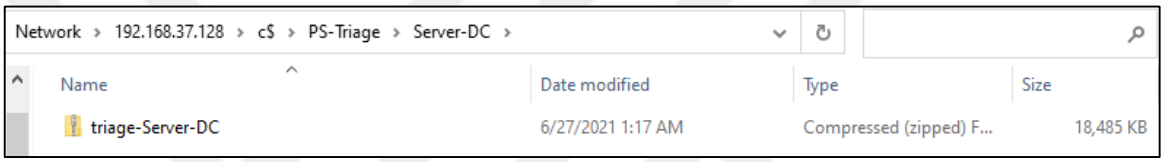
- "**\\192.168.37.128\c$\PS-TRIAGE**" paylaşımlı dizin altında triyaj kaydı alınan cihazın adı(Server-DC) ile klasör oluşturulması,
- "**triage-Server-DC.zip**" isimli dosyanın local cihazdan, **"\\192.168.37.128\c$\PS-TRIAGE\Server-DC"** paylaşımlı alana taşınmasına ait işlem Şekil 6.6'da verilmiştir.



Şekil 6.6. Triyaj kaydının uzak alana kopyalanması

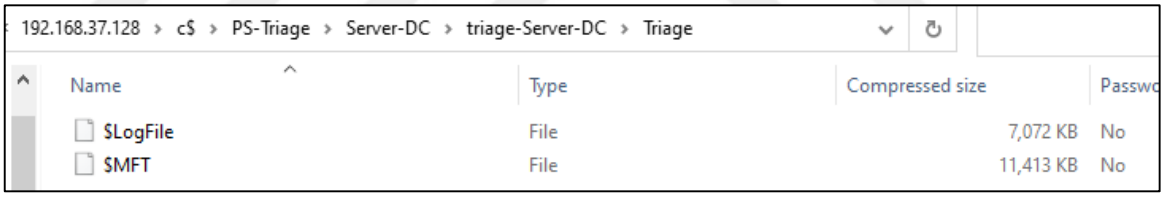
- Hedef makine üzerinde, "**C:\Triage**", "**triage-Server-DC.zip**", "**Rawcopy.exe**", "**Hobocopy.exe**" ve "**7za.exe**" isimli dosya ve klasörlerin silinmesi

Paylaşımlı alan üzerinde oluşturulan triyaj kaydı Şekil 6.7'de sunulmuştur.



Şekil 6.7. Triyaj kaydını içeren sıkıştırılmış dosyanın uzak paylaşımlı alanda oluşturulması

Paylaşımlı alanda yer alan "**triage-Server-DC.zip**" isimli dosyanın içeriği Şekil 6.8'de verilmiştir.



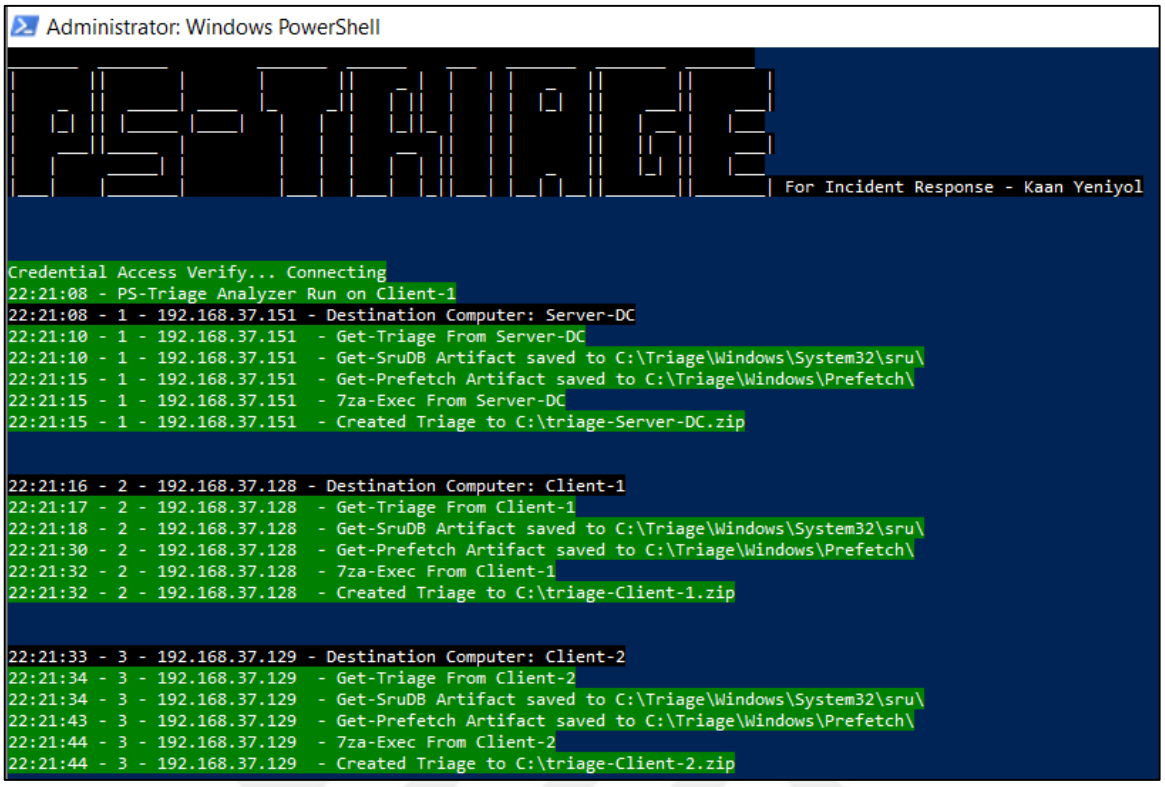
Şekil 6.8. Sıkıştırılmış dosya içerisinde yer alan triyaj kayıtları

6.2.6. Triyaj Kayıtlarının local cihaz üzerinde depolanması

PS-TRIAGE yazılımı ile elde edilen triyaj kayıtlarını paylaşımlı ortak alana taşıyabileceğiniz gibi local makine(Triyaj kaydı alınan cihaz) üzerinde de oluşturulmaktadır.
Srumdb ve **Prefetch** kayıtlarının local makine üzerinde depolanması için gereken komut satırı aşağıdaki gibidir.

ps-triage.ps1 **-username** TEST\Administrator **-pass** P@ssw0rd **-triage** "Srum,Prefetch"

Aşağıdaki ekran görüntüsünde Şekil 6.4'de yer alan cihazlardan **Srumdb** ve **Prefetch** kayıtlarının elde edilmesine ilişkin çıktılar Şekil 6.9'de yer almaktadır.

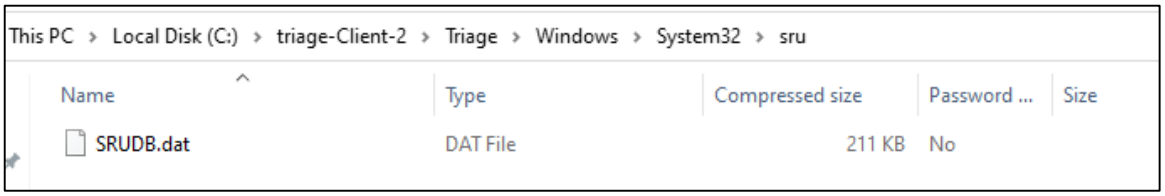


Şekil 6.9. Cihazlardan "Prefetch" ve "SRUM" kayıtlarının toplanması

Yukarıdaki ekran görüntüsünde ise Server-DC isimli cihazın triyaj kaydı şu şekilde elde edilmektedir.

- "**Rawcopy.exe**", "**Hobocopy.exe**" ve "**7za.exe**" isimli yazılımların hedef makine üzerinde kopyalanması
- "**SrumDB**" ve "**Prefetch**" dosya sistem kayıtlarının hedef makine üzerinde "**C:\Triage**" dizini altında kayıt edilmesi
- "**C:\Triage**" isimli dizinin "**C:**" isimli disk bölümü altında "**triage-{Hostname}.zip**" isimli dosya olarak sıkıştırılması,
- Hedef makine üzerinde, "**C:\Triage\",** "**Rawcopy.exe**", "**Hobocopy.exe**" ve "**7za.exe**" isimli dosya ve klasörlerin silinmesi

Local makine üzerinde oluşturulan triyaj kaydı Şekil 6.10'da sunulmuştur. Cihazlar üzerinde Prefetch kayıtlarının yer almadığı görülmüştür.



Şekil 6.10. Toplanan triyaj kaydı

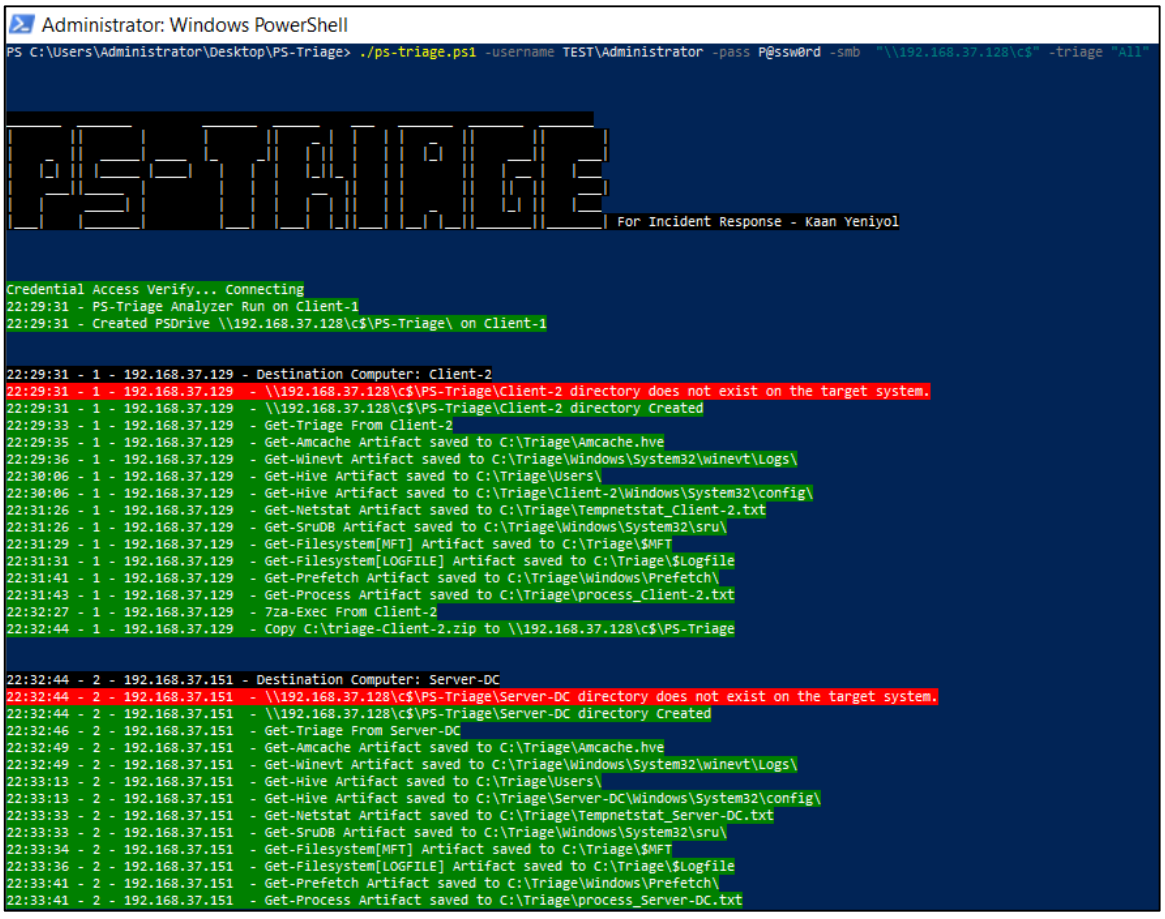
6.2.7. PS-TRIAGE ile tüm triyaj kayıtlarının toplanması

PS-TRIAGE yazılımı ile toplu olarak cihazlar üzerinden tüm triyaj kayıtları toplanabilir ve toplanan triyaj kayıtları uzak paylaşımlı alanda veya local cihaz üzerinde depolanabilir. Toplanan tüm triyaj kayıtları ile olay müdahale analistleri cihazların uçtan uça analizini yapabilir.

Tüm triyaj kayıtlarının uzak paylaşımlı alanda depolanması için gereken komut satırı aşağıdaki gibidir.

ps-triage.ps1 **-username** TEST\Administrator **-pass** P@ssw0rd **-smb** "\\192.168.37.128\c$" **-triage** "All"

Aşağıdaki ekran görüntüsünde Şekil 6.4'de yer alan cihazlardan tüm triyaj kayıtlarının elde edilmesine ilişkin çıktılar Şekil 6.11'de yer almaktadır.



Şekil 6.11. Cihazlardan tüm triyaj kayıtların toplanması

Şekil 6.11'de yer alan çıktılar şu şekilde elde edilmektedir.

- "**\\192.168.37.128\c$**" paylaşımlı alanda "**PS-TRIAGE**" isimli klasör oluşturulması,
- Triyaj kaydı alınacak cihazlarda ilgili kullanıcı adı ve şifre ile oturum açılması,
- "**Rawcopy.exe**", "**Hobocopy.exe**" ve "**7za.exe**" isimli yazılımların hedef makineler üzerinde kopyalanması

- **Amcache, Eventlog(Olay Günlüğü), Registry, Netstat, Srumdb, Filesystem($MFT,$Logfile), Prefecth, Process** kayıtlarının hedef makine üzerinde "**C:\Triage**\" dizini altında toplanması,
- "**C:\Triage**\" isimli dizinin "**C:**\" isimli disk bölümü altında "**triage-{Hostname}.zip**" isimli dosya olarak sıkıştırılması,
- "**\\192.168.37.128\c$\PS-TRIAGE**" paylaşımlı dizin altında triyaj kaydı alınan cihazın adı ile klasör oluşturulması,
- "**triage-{Hostname}.zip**" isimli dosyanın local cihazdan, **"\\192.168.37.128\c$\PS-TRIAGE\{Hostname}"** paylaşımlı alana taşınması
- Hedef makine üzerinde, "**C:\Triage\", "triage-{Hostname}.zip",** "**Rawcopy.exe**", "**Hobocopy.exe**" ve "**7za.exe**" isimli dosya ve klasörlerin silinmesi

Paylaşımlı alan üzerinde oluşturulan triyaj kayıtlarını içeren klasörlere ait ekran görüntüsü Şekil 6.12'de sunulmuştur.

Şekil 6.12. Hedef makinelerden toplanan triyaj kayıtları

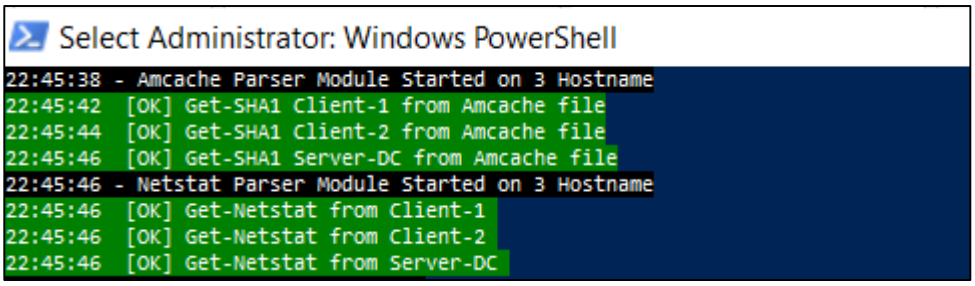
6.2.8. PS-TRIAGE ile ön analiz

PS-TRIAGE yazılımın "**analyzer**" modülü kullanılarak, toplanan triyaj kayıtları arasından Amcache ve Netstat artifact kayıtları parse edilebilmektedir. Parse edilen Amcache kaydında işletim sistemi bileşeni olmayan yani 3. Parti yazılımların cihazlar üzerinde **çalıştırılma tarihi**, **çalıştrılan dosya yolu** ve **hash bilgisi** analiz edilmektedir. Netstat çıktısında ise elde edilen gerçek IP adresleri abuse-ip isimli siber istihbarat servislerinde sorgulanmaktadır.

PS-TRIAGE ön analiz ile analizci uçtan uça tüm triyaj kaydını analiz etmeden makine üzerinde gerçekleştirilmiş kötücül aktiviteler hakkında bilgi sahibi olabilmektedir. PS-TRIAGE yazılımı ile elde edilen tüm artifact kayıtlarının ön analiz aşamasından geçirilmesini sağlayan komut satırı aşağıdaki gibidir.

ps-triage.ps1 **-username** TEST\Administrator **-pass** P@ssw0rd **-smb** "\\192.168.37.128\c$" **-triage** "All" **-analyzer** "Yes"

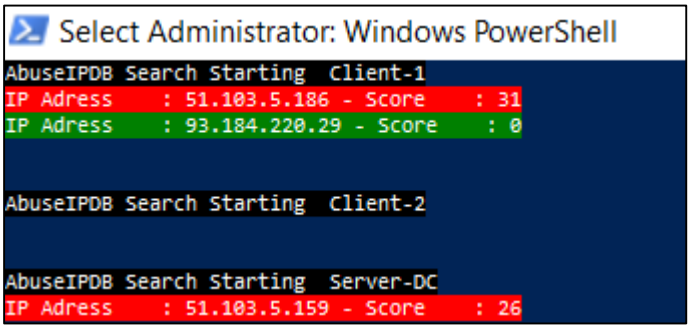
Şekil 6.4'de yer alan cihazlardan elde edilen Amcache ve Netstat kayıtlarının parse edilmesine ait işlem kayıtları Şekil 6.13'de yer almaktadır.



Şekil 6.13. Ön analizin gerçekleştirilmesi

Yukarıda yer alan komut çalıştırıldığında toplanan triyaj kayıtlarına ait ön analiz çıktıları aşağıdaki gibidir.

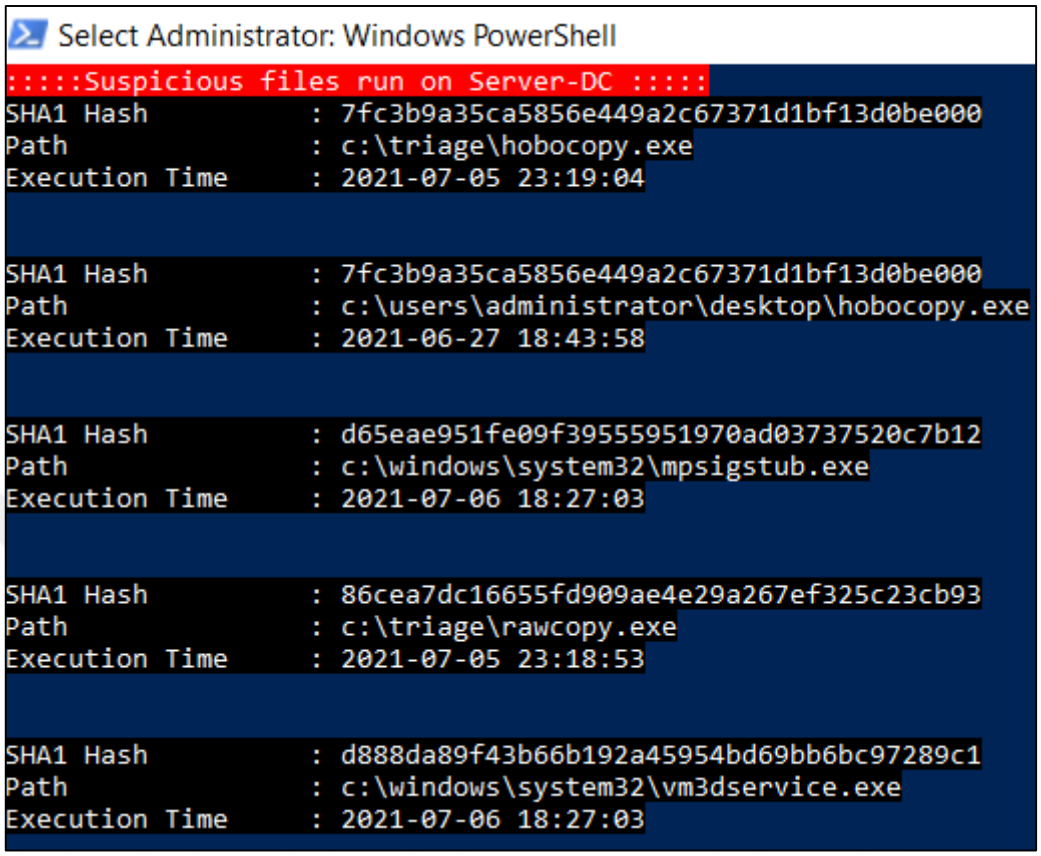
- "**PS-TRIAGE ile tüm triyaj kayıtlarının toplanması**" başlığı altında yer alan işlemlerin gerçekleştirilmesi
- "**\\192.168.37.128\c$\PS-TRIAGE**" paylaşımlı dizin altında yer alan triyajların toplandığı makine isimlerinin belirlenmesi,
- Triyaj kayıtları içerisinden Amcache dosyasının parse edilmesi ve Amcache dosyasından "**Hash**", "**Çalıştırılma Zamanı**", "**Dosya yolu**" ve "**Bilgisayar adı**" gibi başlıkların çıkartılması,
- Triyaj kayıtlarından Netstat çıktısında yer alan gerçek IP adreslerinin ayıklanması ve tekilleştirilmesi,
- Netstat çıktısından elde edilen gerçek IP adreslerinin abuse-ip platformunda sorgulanması ve skor değerlerinin çıkartılmasına ilişkin kayıtlar Şekil 6.14'de verilmiştir.



Şekil 6.14. AbuseIPDB servisinde sorgulanan IP adresleri

- Sorgulanan IP adresleri, IP reputasyon skoru ve IP adresinin tespit edildiği bilgisayar adının, "**\\192.168.37.128\c$\PS-TRIAGE"** dizini altında "**AbuseSearch-Total.txt**" isimli dosyada yazdırılması
- Amcache dosya analizinde, işletim sistemi bileşenlerinin ayıklanması ve şüpheli çalıştırılabilir dosyaların çıktı olarak verilmesi

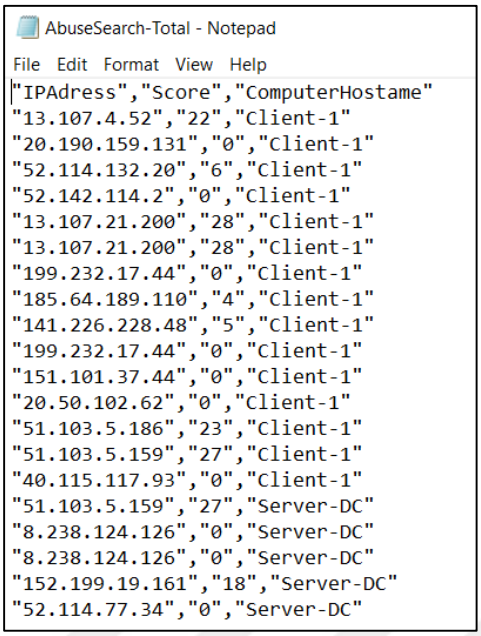
Amcache kaydının analizi sonucunda, şüpheli olarak değerlendirilen çalıştırabilir dosyalara ait bilgiler Şekil 6.15'de sunulmuştur.



Şekil 6.15. Ön analiz işlemine göre çalıştırılan dosyalara ait bilgiler

- Tüm cihazların Amcache dosyası analizi çıktılarının **"\\192.168.37.128\c$\PS-TRIAGE"** dizini altında **"SuspiciousEOE.txt"** isimli dosyada kayıt edilmesi

"\\192.168.37.128\c$\PS-TRIAGE" dizini altında oluşan "**AbuseSearch-Total.txt**" isimli dosyanın içeriği Şekil 6.16'da yer almaktadır.



Şekil 6.16. AbuseIPDB servisinde sorgulanan IP adreslerine ait çıktılar

"\\192.168.37.128\c$\PS-TRIAGE" dizini altında "**SuspiciousEOE.txt**" isimli dosyanın içeriği Şekil 6.17'de sunulmuştur.

Şekil 6.17. Ön analiz sonucunda çalıştırılmış şüpheli dosyalara ait bilgiler

6.2.9. PS-TRIAGE ile örnek analizi

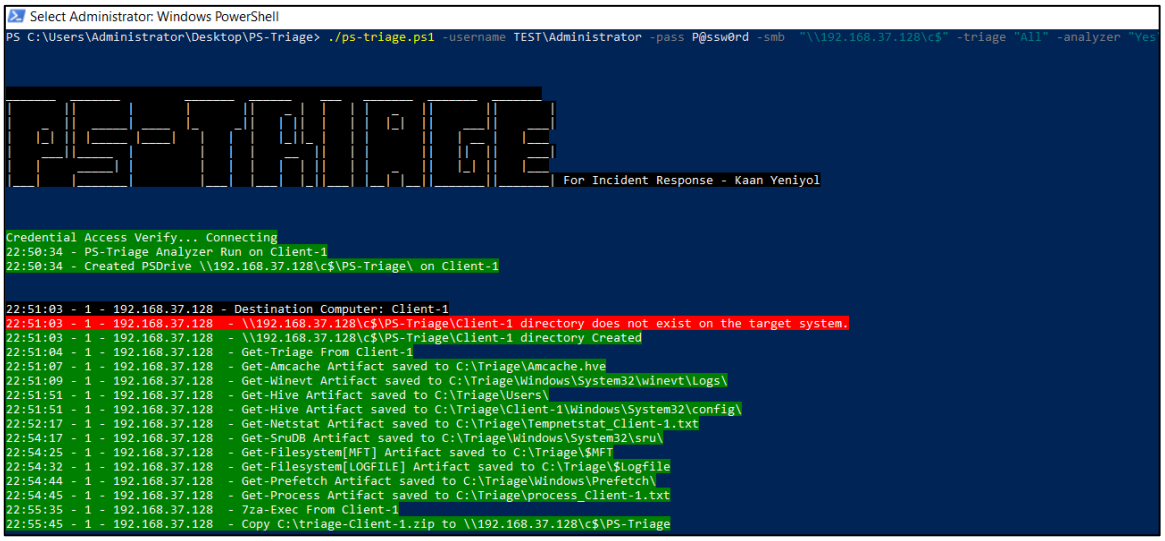
PS-TRIAGE yazılımı ile Şekil 6.4'de yer alan IP adreslerine sahip cihazlardan full triyaj kaydının toplanmasını ve toplanan triyaj kaydının SMB paylaşımlı alanda depolanmasını sağlayalım.

Toplanan triyaj kayıtlarında, Amcache ve Netstat kayıtlarının otomatik olarak analizi yapılarak şüpheli/kötücül aktivitelerin tespitini yapabiliriz.

Söz konusu aktivitelerin tespiti için aşağıdaki komutu çalıştırmanız yeterli olacaktır.

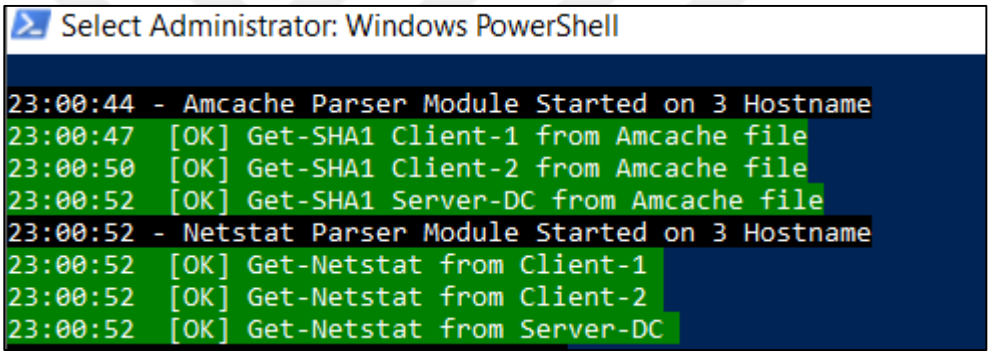
ps-triage.ps1 **-username** TEST\Administrator **-pass** P@ssw0rd **-smb** "\\192.168.37.128\c$" **-triage** "All" **-analyzer** "Yes"

Triyaj kaydının toplanmasına ilişkin program çıktısı Şekil 6.18'de sunulmuştur.



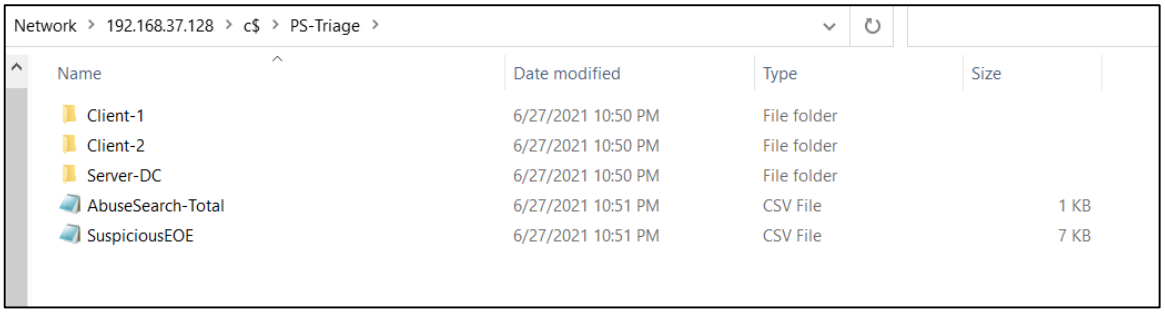
Şekil 6.18. **"**Full" parametresi içeren PS-TRIAGE yazılımın çalıştırılması sonucunda elde edilen çıktılar

Netstat ve Amcache kayıtlarının parse edilmesine ilişkin çıktı Şekil 6.19'da beyan edilmiştir.



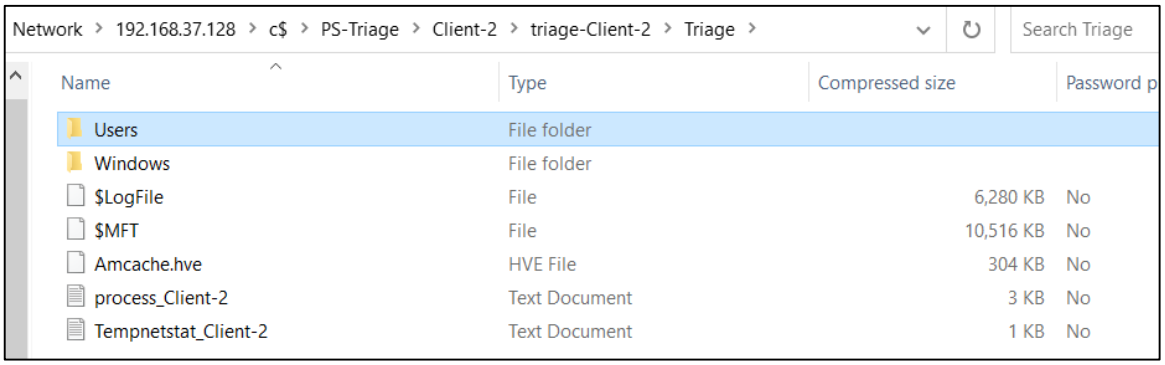
Şekil 6.19. PS-TRIAGE yazılımı ile ön analizi sağlanan kayıtlar

Triyaj kayıtları ve çıktılar **"\\192.168.37.128\c$\PS-Triage"** paylaşımlı alanda oluşturulduğu görülmektedir. Triyaj kayıtlarının toplandığı cihazlara ait isim ile oluşturulan klasör bilgileri Şekil 6.20'de yer almaktadır.



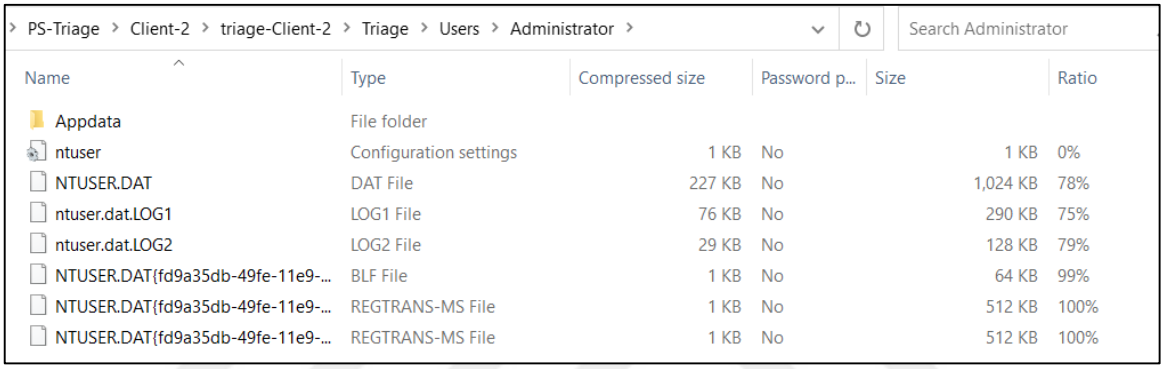
Şekil 6.20. Uzak paylaşımlı alanda oluşturulmuş triyaj kayıtları

"**Client-2**" isimli cihaza ait triyaj kayıtları Şekil 6.21.'de verilmiştir.



Şekil 6.21. "Client-2" isimli cihaza ait uzak paylaşımlı alanda oluşturulan triyaj kayıtları

"**Client-2**" isimli cihazdan toplanan registry kayıtları Şekil 6.22'de yer almaktadır.



Şekil 6.22. "Client-2" isimli cihazdan elde edilen bazı registry dosyaları

PS-TRIAGE yazılımın topladığı triyaj kayıtlarında gerçekleştirdiği ön analizlerde, processlerin işlem kurduğu şüpheli IP adresleri aşağıdaki gibidir. Söz konusu kayıtlar **"\\192.168.37.128\c\PS-Triage**" ortak alanında "**AbuseSearch-Total.txt**" isimli dosyada tutulmaktadır. "**AbuseSearch-Total.txt**" dosya içeriği Tablo 6.9'da sunulmuştur.

Tablo 6.9. "AbuseSearch-Total.txt" dosya içeriği

Cihaz Adı	IP Adresi	Skoru
Client-1	51.103.5.186	31
Client-1	20.54.110.119	1
Server-DC	51.103.5.159	27

Amcache dosyasının parse edilmesi ile şüpheli olarak işaretlenen ve işletim sisteme ait bileşeni olmayan çalıştırılmış dosyalar **"\\192.168.37.128\c\PS-Triage**" paylaşımlı alan altında yer alan "**SuspiciousEOE.txt**" isimli dosyada tutulmaktadır.

"**SuspiciousEOE.txt**" isimli dosyanın içeriği Şekil 6.23'de yer almaktadır.

SHA1Hash	SuspiciousPath	Hostname	ExecutionTime
86cea7dc16655fd909ae4e29a267ef325c23cb93	c:\users\administrator\desktop\ps-triage\rawcopy.exe	Client-1	6/23/2021 2:51
14edac1cab36b89a3d52d455216034a4ff681b40	c:\windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.18362.1610_none_16d8d2032a45b189\tiworker.exe	Client-1	6/27/2021 0:27
66ffd779db1c85f47a014f4f9d840536617c0f94	c:\windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.18362.590_none_5efc551459114cb9\tiworker.exe	Client-1	6/1/2021 13:12
9-3bdb-4f2c-9c38-ab25cd5102e2}		Client-1	6/23/2021 19:54
1ca358ca5530fe6a0b775d252f7ef34008dabb7e	c:\users\administrator\appdata\local\microsoft\onedrive\21.099.0516.0003\filesynchelper.exe	Client-1	6/23/2021 19:54
41ac7a4a45bfbe6dceec416151d92315efc34fc8	c:\users\administrator\appdata\local\microsoft\onedrive\21.099.0516.0003\microsoft.nucleus.exe	Client-1	6/23/2021 19:54
34b1b3d5c45b5c42b5284ecff80a1c41315a194e	c:\users\administrator\appdata\local\microsoft\onedrive\21.099.0516.0003\microsoft.nucleus.nativemessagingclient.exe	Client-1	6/23/2021 19:54
3948fc622192c52f52eaaaa2a0662286da05be94	c:\users\administrator\appdata\local\microsoft\onedrive\21.099.0516.0003\onedrivefilelauncher.exe	Client-1	6/23/2021 19:54
bbf1e5e66e4ce70ab3cfd03236cb36be346cf3d8	c:\users\administrator\appdata\local\microsoft\onedrive\21.099.0516.0003\onedrivesetup.exe	Client-1	6/23/2021 19:54
b05525d58153db16c26654fb95cabe3afc7b53af	c:\users\analist02\appdata\local\microsoft\onedrive\update\onedrivesetup.exe	Client-2	6/23/2021 2:29
a614dc42455195bbd17ea6370fd71565c946b3bb	c:\users\administrator\appdata\local\microsoft\onedrive\onedrivestandaloneupdater.exe	Client-2	6/27/2021 17:39
66ffd779db1c85f47a014f4f9d840536617c0f94	c:\windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.18362.590_none_5efc551459114cb9\tiworker.exe	Client-2	6/1/2021 13:10
f70eca243b0409cea2f8f642274cc13f23a22a25	c:\programdata\microsoft\windows defender\platform\4.18.2105.5-0\msmpeng.exe	Server-DC	6/26/2021 13:59
aa187eba07bed0f6f5f77e19d5cc8d6c3eb6f104	c:\programdata\microsoft\windows defender\platform\4.18.2105.5-0\nissrv.exe	Server-DC	6/27/2021 19:00
86cea7dc16655fd909ae4e29a267ef325c23cb93	c:\triage\rawcopy.exe	Server-DC	6/26/2021 22:15
8c53e8a7a9e5a272029f65194540ec2490101a48	c:\users\public\sharphound.exe	Server-DC	6/27/2021 18:40
33aa88655f38d218c6e07888157117680ee082bf	c:\windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.17763.733_none_7e30c51b4cee0b94\tiworker.exe	Server-DC	6/1/2021 12:50
d888da89f43b66b192a45954bd69bb6bc97289c1	c:\windows\system32\vm3dservice.exe	Server-DC	6/26/2021 20:54

Şekil 6.23. "SuspiciousEOE.txt" dosya içeriği

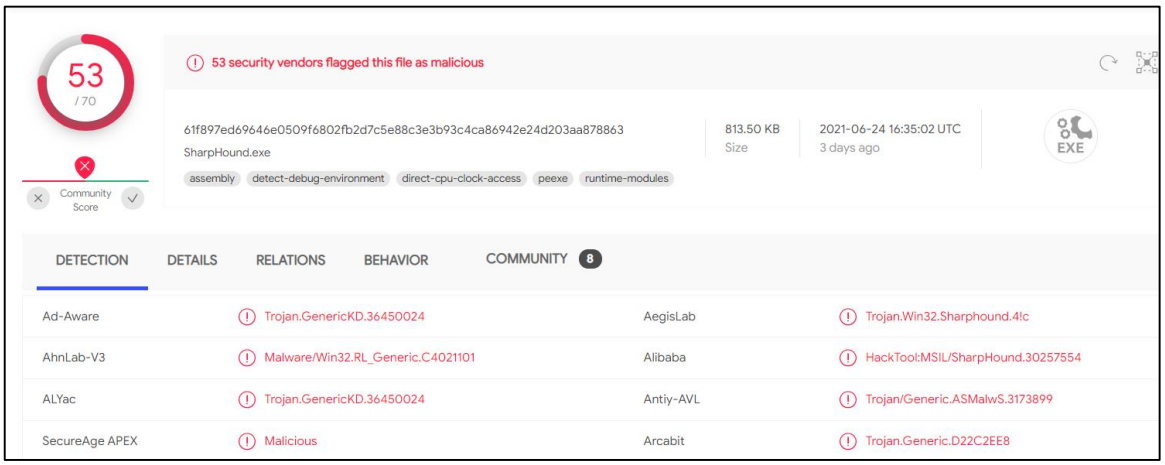
Yukarıda ekran görüntüsünde yer alan çalıştırılma kayıtlarında şüpheli olarak görülen kayıt Tablo 6.10'da verilmiştir.

Tablo 6.10. PS-TRIAGE yazılımına ait ön analiz aşamasında tespit edilen şüpheli kayıt

SHA1	Path	Hostname	Çalıştırılma Zamanı
8c53e8a7a9e5a272029f65194540ec2490101a48	c:\users\public\sharphound.exe	Server-DC	27/06/2021 18:40

Server-DC isimli cihazda çalıştırılan şüpheli yazılıma ait hash bilgisi siber istihbarat kayıtlarında sorgulandığına "**sharphound**" yazılımı olduğu görülmüştür. Söz konusu "**sharphound**" yazılımı, genellikle siber suçlular ve pentest ekipleri tarafından aktif dizin üzerinde bilgi toplamak için kullanılmaktadır [42].

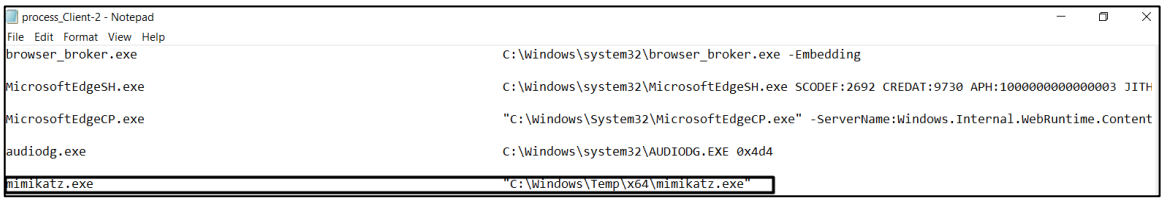
"**8c53e8a7a9e5a272029f65194540ec2490101a48**" hash değerine ait "virustotal[.]com" çıktısı Şekil 6.24'de yer alan ekran görüntüsünde beyan edilmiştir.



Şekil 6.24. Virustotal[.]com çıktısı

PS-TRIAGE yazılımı ile cihazlar üzerinden toplanan çalışan işlemlere ait komut satırları incelendiğinde "**Client-2**" isimli cihazda "**mimikatz.exe**" yazılımın "**C:\Windows\Temp\x64**" dizini altında aktif olarak çalıştığı gözlemlenmiştir. Söz konusu kayıt, cihaza ait triyaj kayıtlarının yer aldığı "**triage-Client-2.zip**" isimli sıkıştırılmış dosyada bulunan **"process_Client-2.txt"** isimli çıktıda yer almaktadır. **"process_Client-2.txt"** dosyasında processlere ait komutlar yer almaktadır.

“**Client-2**” isimli cihazda tespit edilen kötücül işlem kaydı Şekil 6.25’de sunulmuştur.



Şekil 6.25. “Client-2” isimli cihazda tespit edilen şüpheli işlem kaydı

7. BULGULAR VE TARTIŞMA

Olay müdahale kapsamında siber saldırının etkisini veya yayılımın hızlıca tespiti için, enfekte olmuş cihazlardan elektronik delillerin toplanması ve kötücül aktivitenin analizi sağlanmalıdır. Saldırgan gruplar, kurum veya kuruluşlara ait aktif dizin üzerinde yanal hareket sağlayarak birçok cihazı enfekte edebilir, dosyalarınızı şifreleyebilir, hizmet sağlayan servis veya uygulamaları durdurabilir. Saldırganların, kurumsal ağ üzerindeki yayılımını hızlıca tespit etmek ve gerekli önlemleri almak, kurumsal ağ üzerinde sağlanan servis veya hizmetin devam ettirilebilmesi açısından önem arz etmektedir.

Kötücül aktiviteleri tespit etmek için, enfekte olan cihazlardan fiziksel veya mantıksal imaj almak yerine, hızlı bir şekilde triyaj kayıtlarını toplayabilir ve aktivitenin dosya sistemi üzerindeki kayıtlarını hızlı bir şekilde analiz edilebilmektedir.

Kötücül aktivite ile ilişkili cihazlardan triyaj kayıtlarının toplanmasının avantajları şu şekilde sıralanabilir.

- Analiz edilecek dijital veri miktarının az olması
- Triyaj verilerini depolamak için yüksek kapasiteli disklere ihtiyaç yoktur.
- Az adam ve gün maliyetinin azalması
- Kısa ve hızlı analiz sonucunda kötücül aktivitenin durumunu ortaya çıkarmak
- Analizler sonucu elde edilen saldırı göstergelerinin(IOC) çıkartılması
- İlgili IOC'ler ile kurumsal ağda yer alan güvenlik çözümlerinde(EDR, EPP, SIEM, SOAR) saldırının yayılımı gözlemlemek için kural yazılması
- Dosya sistem ve uygulama kayıtlarının analizi sonrasında saldırı haritası ve zaman çizelgesinin hızlı bir şekilde çıkartılması

Olay müdahale sürecinde, aktivitenin yayılımı ortaya çıkarmak ve ön analizini sağlamak için bu tez çalışması kapsamında yazılan "**PS-TRIAGE**" yazılımı kullanılabilir. "**PS-TRIAGE**" yazılımı ile uzakta bulunan windows işletim sistemi cihazlardan toplu veya belirlenen kayıtların triyajlarını elde edebilirsiniz. Elde edilen triyaj kayıtları, uzak bir depolama alanında veya local alanda tutulmaktadır. "**PS-TRIAGE**" yazılımı ön analiz kapsamında, "**Amcache.hve**" dosyasını analiz ederek çalıştırılan 3.parti şüpheli uygulamaların, çalıştırılma tarihi, hash bilgisi, çalıştırıldığı dosya yolu ile ilgili çıktıları analizciye sunmaktadır. Ayrıca yazılım, makine üzerinde çalışan işlemlerin iletişim halinde olduğu IP adreslerinin, siber istihbarat servislerinde sorgulayarak reputasyon kontrolünü yapmaktadır.

"**PS-TRIAGE**" yazılımın triyaj kayıtları üzerinde gerçekleştirdiği ön analizlerde, analizciye cihazlar üzerinde oluşmuş aktiviteler ile ilgili ön bilgileri çıktı olarak sunmaktadır.

7.1. Triyaj toplama yazılımların karşılaştırılması

Olay müdahale süreçlerinde, triyaj kayıtlarının toplanması için sıklıkla kullanılan KAPE ve CyLR araçlarının, bu tez çalışması kapsamında kodlanan PS-TRIGAE yazılımı ile ana özellikler altında karşılaştırılmasına ilişkin Tablo 7.1'de sunulmuştur.

Tablo 7.1. Triyaj alma yazılımların karşılaştırılması

ÖZELLİK	PS-TRIGAE	KAPE	CyLR
Uzaktan, hedef makinelere ait triyaj kayıtlarının toplanması	✓	✗	✗
Ön Analiz	✓	✓	✗
Triyaj kayıtların local veya uzak alanda depolanması	✓	✓	✓
Dosya sistem kayıtların elde edilmesi	✓	✓	✓
Çalıştırılabilir dosyalara ait çalıştırma kayıtlarının elde edilmesi	✓	✓	✓
Registry dosyalarının toplanması	✓	✓	✓
Triyaj kayıtlarının özelleştirilmesi	✗	✓	✓
NBI değerlerinin sorgulanması	✓	✗	✗
Sıkıştırma Desteği	✓	✓	✓
.NET yazılımı ihtiyacı	✗	✓	✗
Aktif işlem kayıtlarının toplanması	✓	✗	✗
İşlemlere ait, IP ve port iletişim bilgilerinin toplanması	✓	✗	✗
Uygulama log çıktısı	✗	✓	✓
Geliştirilebilir durumu / Açık kaynak	✓	✗	✓

8. SONUÇLAR

Bu tez çalışmasında, olay müdahalesi ve döngüsünde yer alan kanıt dijital delillerin toplanması aşamasından, Windows işletim sistemine sahip önemli artifact kayıtlarından ve bu kayıtları, sistemin fiziksel veya mantıksal disk imajı almadan triyaj kaydı oluşturularak elde edilmesi yöntemlerinden bahsedilmiştir. Olay müdahale kapsamında veya güvenliği ihlal edilmiş aynı ağ üzerinde yer alan onlarca sistemlerden disk imajı alma işlemleriyle uğraşmadan, elde edilen triyaj kayıtlarının analizlerinin sağlanması gerektiği belirtilmiş ve local veya uzak sistem fark etmeksizin Windows işletim sistemi tabanlı makinelerden triyaj kayıtlarının elde edilebilirliği gösterilmiştir. Ayrıca kurumsal ağ üzerinde yer alan makinelerden toplu olarak triyaj kayıtlarının alınması ve ortak alana kopyalanmasında kullanılan teknikler uygulanmıştır.

Windows aktif dizini üzerinde yer alan cihazlardan triyaj kaydının toplanması ve toplanan triyaj kaydının ön analizini sağlayan Powershell betiğinde PS-TRIAGE isimli yazılım geliştirilmiştir. Geliştirilen yazılım, olay müdahale süreçlerinde detaylı analiz için hızlı bir şekilde dosya sistem ve uygulama kayıtlarını toplamaktadır. Söz konusu yazılımı, triyaj kaydı toplamak için hedef cihazlar üzerinde çalıştırılmasına gerek yoktur. PS-TRIAGE ile windows aktif dizininde yer alan herhangi bir cihaz üzerinde uzaktan triyaj kaydını toplayabilmekte ve toplanan triyaj kaydını uzak paylaşımlı alanda veya hedef makine(local) üzerinde oluşturabilmektedir.

Triyaj kaydı toplanan cihazlarda, çalıştırılmış şüpheli dosyaların bilgilerini ve işlemlerin(process) iletişim kurduğu IP adreslerini siber istihbarat servislerinde sorgulayarak repustasyon değerini analizcinin önüne sunmaktadır.

Olay müdahale analistleri, uzak makinelerden toplanan triyaj kayıtlarını gelişmiş yöntemler ile analiz ederek kötücül aktivitenin yayılımı, etkisini, saldırı göstergelerini(IOC), zaman çizelgesini ve saldırı haritasını ortaya çıkartmaktadır.

ÖNERİLER

PS-TRIAGE yazılımının mevcut özellikleri Tablo 7.1'de sunulmuştur. Bu tez çalışmasında, kayıtların toplanacağı makinelere ajan veya uygulama kurmadan triyaj kaydının uzaktan toplanmasını sağlayan projenin geliştirilmesi hedeflenmiştir.

PS-TRIGAE yazılımı triyaj kaydı toplanacak ve aktif dizin üzerinde yer alan cihazlara winrm servisi ile uzaktan bağlantı oluşturmaktadır. Oluşturulan bağlantı aracılığıyla hedef makine üzerinden toplanan triyaj kayıtları uzak veya local sistemlerde depolanmaktadır.

Toplanan triyaj kayıtlarından, Amcache.hve ve Netstat çıktılarının analizi sağlanarak ön analiz çıktısı, analizciye sunulmaktadır.

Yazılımın daha yetkin ve hızlı çalışması için aşağıdaki modüllerin geliştirilmesi yapılmaktadır.

- Eş zamanlı olarak daha fazla cihazdan triyaj toplanması,
- Toplanan dosya sistem ve uygulama kayıtlarına ait hash bilgisinin hesaplanması,
- Son kullanıcı tarafından özelleştirilen kayıtların toplanması

KAYNAKLAR

[1] A. Moser and M. I. Cohen, Hunting in the enterprise: Forensic triage and incident response, Digit. Investig., vol. 10, no. 2, pp. 89–98, 2013, doi: 10.1016/j.diin.2013.03.003.

[2] David A. Coughanour , REMOTE FORENSICS IN INCIDENT RESPONSE, UMI Number: 1571398.

[3] URL-1, https://axaxl.com/fast-fast-forward/articles/the-cyber-incident-response-lifecycle, [Çevrimiçi] [Erişim: 05-Ağustos-2021].

[4] Mundie, D., Ruefle, R., Dorofee, A., McCloud, J., Perl, S., & Collins, M. (2014). An incident management ontology. CEUR Workshop Proceedings, 1304, 62–71

[5] John Sammons Windows System Artifacts., In book: The Basics of Digital Forensics (pp.65-82)

[6] URL-2, https://www.itshacked.com/835/hackers-using-anydesk-accessing-upi-wallets-to-wipe-out-your-money.html, [Çevrimiçi]. [Erişim: 05-Ağustos-2021].

[7] Lahaie, C., & Leberfinger, D. (2013). TeamViewer Forensics.

[8] K. Zhang, E. Cheng, and Q. Gao, Analysis and implementation of NTFS file system based on computer forensics, 2nd International Workshop on Education Technology and Computer Science, ETCS 2010, vol. 1. pp. 325–328, 2010, doi: 10.1109/ETCS.2010.434.

[9] Alazab, M., & Watters, P. (2009). Digital forensic techniques for static analysis of NTFS images. 4th International Conference of Information Technology, ICIT, February

[10] Zareen, M. S., & Aslamy, B. (2015). $LogFile of NTFS: A blueprint of activities. 17th IEEE International Multi Topic Conference: Collaborative and Sustainable Development of Technologies, IEEE INMIC 2014 - Proceedings, 305–310. https://doi.org/10.1109/INMIC.2014.7097356

[11] Kahvedžić, D., & Kechadi, T. (2008). Extraction of user activity through comparison of windows restore points. Proceedings of the 6th Australian Digital Forensics Conference, 98–112.

[12] Singh, B., & Singh, U. (2016). Leveraging the Windows Amcache.hve File in Forensic Investigations. Journal of Digital Forensics, Security and Law, 11(4). https://doi.org/10.15394/jdfsl.2016.1429

[13] URL-3, https://www.difose.com.tr/windowsda-program-yurutme-artifactlerinin-analizi/, [Çevrimiçi]. [Erişim: 05-Ağustos-2021].

[14] Liew, S. P., & Ikeda, S. (2019). Detecting Adversary using Windows Digital Artifacts. Proceedings - 2019 IEEE International Conference on Big Data, Big Data 2019, 3210–3215.

[15] Singh, B., & Singh, U. (2016). A forensic insight into Windows 10 Jump Lists. Digital Investigation, 17, 1–13. https://doi.org/10.1016/j.diin.2016.02.001

[16] Khatri, Y. (2015). Forensic implications of System Resource Usage Monitor (SRUM) data in Windows 8. Digital Investigation, 12, 53–65.

[17] Shashidhar, N., & Novak, D. (2015). Digital Forensic Analysis on Prefetch Files. International Journal of Information Security Science, 4(2), 39–49.

[18] Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2020). D4I - Digital forensics framework for reviewing and investigating cyber attacks. Array, 5 (December 2019), 100015.

[19] Quick, D., Tassone, C., & Choo, K. K. R. (2014). Forensic analysis of windows thumbcache files. 20th Americas Conference on Information Systems, AMCIS 2014, 990 (July 2006), 1–13.

[20] Leschke, T. R. (2010). Cyber Dumpster-Diving: $Recycle.Bin Forensics for Windows 7 and Windows Vista. Forensic Computer Engineer.

[21] Prudente, C., Tixteco, L. P., Pérez, G. S., & Toscano, L. K. (2016). IOCs with Windows events.c,29–37.c

[22] K. Chang, G. Kim, K. Kim, and W. Kim, Initial case analysis using windows registry in computer forensics, Proceedings of Future Generation Communication and Networking, FGCN 2007, vol. 1. pp. 564–569, 2007, doi: 10.1109/fgcn.2007.151.

[23] Ramani, A., & Dewangan, S. K. (2014). Auditing Windows 7 Registry Keys to track the traces left out in copying files from system to external USB Device. 5(2), 1045–1052.

[24] URL-4, https://code.google.com/archive/p/triage-ir/, [Çevrimiçi]. [Erişim: 05-Ağustos-2021].

[25] A. S. Narayanan and M. M. Ashik, Computer forensic first responder tools, Proceedings of the 2012 International Conference on Advances in Mobile Networks, Communication and Its Applications, MNCApps 2012. pp. 156–159, 2012, doi: 10.1109/MNCApps.2012.38.

[26] Åsenbrygg, I. (2019). Triage-työkalujen kyvykkyyksien vertailu ja todentaminen.

[27] URL-5, https://www.sans.org/webcasts/triage-collection-timeline-analysis-kape-109840, Triage Collection and Timeline Analysis with KAPE. [Çevrimiçi]. [Erişim: 05-Ağustos-2021].

[28] Dykstra, J., & Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. Proceedings of the Digital Forensic Research Conference, DFRWS 2012 USA, 9, S90–S98. https://doi.org/10.1016/j.diin.2012.05.001

[29] K. Kröger and R. Creutzburg, A practical overview and comparison of certain commercial forensic software tools for processing large-scale digital investigations, Mob. Multimedia/Image Process. Secur. Appl. 2013, vol. 8755, p. 875519, 2013, doi: 10.1117/12.2017906.

[30] Dykstra, J., & Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. Proceedings of the Digital Forensic Research Conference, DFRWS 2012 USA, 9, S90–S98. https://doi.org/10.1016/j.diin.2012.05.001

[31] Roussev, V. (2011). Building open and scalable digital forensic tools. 2011 6th IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, SADFE 2011.

[32] Hassan, W. U., Bates, A., & Marino, D. (2020). Tactical provenance analysis for endpoint detection and response systems. Proceedings - IEEE Symposium on Security and Privacy, 2020-May, 1172–1189. https://doi.org/10.1109/SP40000.2020.00096

[33] F-Response Manual. (n.d.). Provides a complete breakdown of leveraging F-Response to perform expert remote e-discovery, computer forensics, and incident response.

[34] Adams, R., Mann, G., & Hobbs, V. (2017). Iseek, a tool for high speed, concurrent, distributed forensic data acquisition. Proceedings of the 15th Australian Digital Forensics Conference, ADF 2017, December, 19–25. https://doi.org/10.4225/75/5a838d3b1d27f

[35] URL-6, https://github.com/orlikoski/CyLR, [Çevrimiçi]. [Erişim:05-Ağustos-2021].

[36] Kim, M., Lee, S., October 6-8, 2015. Forensic analysis using amcache.hve. In: Digital Forensics and Cyber Crime: 7th International Conference, ICDF2C 2015, vol. 157. Springer, Seoul, South Korea, p. 215. Revised Selected Papers

[37] URL-7, https://github.com/EricZimmerman/AmcacheParser, [Çevrimiçi]. [Erişim: 05-Ağustos-2021].

[38] Science, B. C., & Bouma, J. (2019). Open University of the Netherlands Interpreting NTFS Time-stamps.

[39] Shiaeles, S., Chryssanthou, A., & Katos, V. (2013). On-scene triage open source forensic tool chests: Are they effective? Digital Investigation, 10(2), 99–115. https://doi.org/10.1016/j.diin.2013.04.002

[40] URL-8, abuseipdb.com, [Çevrimiçi]. [Erişim: 05-Ağustos-2021].

[41] Maduranga, K. A. M. (2016). Investigate Windows Management Instrumentation (WMI) Attacks in Windows Operating Systems A dissertation submitted for the Degree of Master of Science in Information Security.

[42] K. Kröger and R. Creutzburg, Readiness for Tailored Attacks and Lateral Movement Detection, 2018

ÖZGEÇMİŞ

Kaan YENİYOL

[redacted]