



**İSTANBUL GELİŞİM ÜNİVERSİTESİ
İSTANBUL KALKINMA AJANSI**

Disk İmajının Adli Bilişim Teknikleriyle İncelenmesi

SİBER AKADEMİ PROJESİ

Samet ÜNSAL

Danışman: Mehmet Demir | Adli Bilişim Analisti

ARALIK 2024

ÖNSÖZ

Dijital dünyanın hızlı gelişimi, bireyler ve kurumlar için büyük fırsatlar sunarken, aynı zamanda siber tehditlerin de artmasına neden olmuştur. Bu tehditlere karşı koyabilmek ve dijital olayları doğru bir şekilde analiz edebilmek için adli bilişim, günümüzün en önemli disiplinlerinden biri haline gelmiştir. Dijital delillerin toplanması, analiz edilmesi ve raporlanması süreçlerini kapsayan adli bilişim, modern dünyada hem suç soruşturmalarında hem de bilgi güvenliği çalışmalarında kritik bir rol oynamaktadır. Çalışmada elde edilen bulgular, adli bilişim süreçlerinin ne kadar titizlikle ve metodolojik bir şekilde yürütülmesi gerektiğini de bir kez daha ortaya koymuştur. Bu çalışma süresince edindiğim bilgiler ve karşılaştığım zorluklar, siber güvenlik ve adli bilişim alanında kendimi geliştirmeme önemli bir katkı sağlamıştır. Dijital tehditlerle mücadelede bilgi paylaşımının ve öğrenmenin ne kadar kıymetli olduğunu fark etmiş bulunuyorum.

Aralık 2024

Samet ÜNSAL

TEŞEKKÜR

Siber Akademi Projesi kapsamında bilgi birikimleriyle beni aydınlatan başta Serkan GÖNEN olmak üzere, Ali ÇETİNKAYA, Ayşe Nur BAYRAM, Birkan ALHAN, Çisem YAŞAR, Elham PASHAEI, Furkan ONUR, Gökçe KARACAYILMAZ, Kübra ERDOĞAN, Mehmet Ali BARIŞKAN, Nihal ALTUNTAŞ, Uğur KAYA ve Utku YILDIZ hocalarıma; bu çalışma boyunca konu seçiminde, planlamada ve araştırmada ilgisini ve desteğini esirgemeyerek çalışmamı değerli bilgileriyle yönlendiren danışman hocam Mehmet DEMİR’e teşekkürlerimi sunarım.

Samet ÜNSAL

İÇİNDEKİLER

	<u>Sayfa</u>
ÖNSÖZ.....	ii
TEŞEKKÜR.....	iii
İÇİNDEKİLER	iv
KISALTMALAR.....	vi
ŞEKİL LİSTESİ	vii
ÖZET.....	ix
SUMMARY.....	x
1. GİRİŞ	1
1.1 Yarışma İçeriği.....	1
1.2 Yarışma Amaçları	2
2. METOT	3
2.1 FTK Imager.....	3
2.1.1 Disk İmajının Yüklenmesi.....	4
2.1.2 Dosya Sistemi İncelemesi.....	5
2.1.3 Disk İmajındaki Gizli Verilerin Analizi	5
2.2 AmcacheParser.exe	6
2.3 Registry Explorer.....	6
2.4 exiftool.....	6
2.5 PECmd.exe	6
2.6 Hashcat	7
2.7 BrowsingHistoryView.....	7
2.8 Timeline Explorer	7
2.9 ShellBags Explorer	7
2.10 GANTT Şeması	8
2.11 SWOT Analizi	8
3. BULGULAR VE SONUÇLAR	9
3.1 Soru 1	9
3.1.1 \$I Dosyaları	10
3.1.2 \$R Dosyaları	10
3.2 Soru 2	11
3.2.1 SOFTWARE.....	11
3.3 Soru 3	14

3.4 Soru 4	15
3.5 Soru 5	17
3.5.1 Metadata	17
3.6 Soru 6	18
3.6.1 Prefetch.....	18
3.7 Soru 7	21
3.8 Soru 8	21
3.8.1 Amcache.....	21
3.9 Soru 9	24
3.9.1 UsrClass	24
3.9.2 Shellbag.....	25
3.10 Soru 10	27
3.10.1 NTLM.....	27
3.11 Soru 11	29
3.11.1 SYSTEM	29
3.11.2 SAM	30
4. DEĞERLENDİRME.....	32
KAYNAKLAR.....	34

KISALTMALAR

UNODC	: United Nations Office on Drugs and Crime
CTF	: Capture the Flag
DFIR	: Digital Forensics and Incident Response
RAM	: Random Access Memory
NTFS	: New Technology File System
FAT	: File Allocation Table
EXT	: Extended File System
CSV	: Comma Separated Values
JSON	: JavaScript Object Notation
HTML	: Hyper Text Markup Language
NTLM	: New Technology LAN Manager
LAN	: Local Area Network
UTC	: Universal Time Coordinated
FTP	: File Transfer Protocol
IPv4	: Internet Protocol Version 4
EXE	: Executable File
MD5	: Message-Digest Algorithm 5
URL	: Uniform Resource Locator
JPG	: Joint Photographic Experts Group
DLL	: Dynamic-Link Library
NMAP	: Network Mapper
CMD	: Command Prompt
USB	: Universal Serial Bus
SAM	: Security Account Manager
SID	: Security Identifier

ŞEKİL LİSTESİ

Şekil 1.1: FTK Imager - Yüklenecek dosyanın türünün seçilmesi.....	3
Şekil 1.2: İmaj dosyası seçimi.....	4
Şekil 1.3: .e01 uzantılı dosyanın yüklenmesi.....	4
Şekil 2.1: NTFS biçimli diskin root dosyası incelenmesi.....	4
Şekil 3.1: GANTT Şeması.....	8
Şekil 4.1: \$I dosyası konumu ve değiştirilme zamanı.....	9
Şekil 4.2: Silinen dosyanın adını içeren \$I dosyası.....	10
Şekil 4.3: Silinen dosyanın içeriğini barındıran \$R dosyası.....	10
Şekil 5.1: Registry Explorer – Load hive seçimi.....	12
Şekil 5.2: SOFTWARE dosyası seçimi.....	12
Şekil 5.3: Uninstall dizinindeki önceden yüklenmiş programlar.....	12
Şekil 5.4: FileZilla programına ait recentservers.xml dosyası.....	13
Şekil 5.5: Bağlanılan FTP sunucusu IPv4 adresi.....	13
Şekil 6.1: Verify Drive/Image... seçimi.....	14
Şekil 6.2: İmajın MD5 hash değeri.....	14
Şekil 7.1: İncelenecek tarayıcı seçimi.....	16
Şekil 7.2: History dosyasının dizinini ekleme.....	16
Şekil 7.3: Şüphelinin ziyaret ettiği dizinler.....	16
Şekil 8.1: exiftool sentaks yapısı.....	17
Şekil 8.2: Metada içerisinden elde edilen koordinat bilgileri.....	17
Şekil 8.3: Koordinatın gösterdiği lokasyon.....	18
Şekil 9.1: PECmd.exe komut sentaksı.....	19
Şekil 9.2: Prefetch dosyasını parse etmek için kullanılan komut.....	19
Şekil 9.3: Timeline Explorer csv dosyası açma.....	19
Şekil 9.4: .csv uzantılı Prefetch çıktısı seçimi.....	20
Şekil 9.5: Prefetch çıktıları.....	20
Şekil 10.1: Şüphelinin ziyaret ettiği mail servisi.....	21
Şekil 11.1: AmcacheParser.exe örnek sentaks yapısı.....	22
Şekil 11.2: Amcache.hve dosyasını parse etme işlemi.....	22
Şekil 11.3: Amcache.hve dosyası çıktıları.....	23
Şekil 11.4: Konsolda çalıştırılan komutlar.....	24

Şekil 12.1: Registry kaydı seçimi.....	25
Şekil 12.2: UsrClass.dat dosyası seçimi.....	26
Şekil 12.3: Mobil cihaza ait Shellbag bilgileri.....	26
Şekil 13.1: Hashcat hash tipleri kodları.....	28
Şekil 13.2: Hashcat için kullanılan komut.....	28
Şekil 13.3: Hash kırma işlemi sonucu.....	29
Şekil 14.1: SYSTEM ve SAM kayıtlarının işlenmesi.....	30
Şekil 14.2: NT hashinin girilmesi.....	31
Şekil 14.3: NT hashi çıktısı.....	31
Şekil 15.1: SWOTT Analizi.....	32

DİSK İMAJININ ADLİ BİLİŞİM TEKNİKLERİYLE İNCELENMESİ

ÖZET

Amaç: Bu çalışmanın amacı, bir CTF yarışmasında kullanılan disk imajını adli bilişim teknikleriyle analiz ederek, şüpheli aktiviteleri tespit etmek, dijital delilleri ortaya çıkararak Adli Bilişim araçlarını kullanarak pratik sağlamak ve incelenen öğeler hakkında bilgi sahibi olmaktır . Çalışma, adli bilişim araçlarının etkin kullanımını ve inceleme sürecinin nasıl yürütüldüğünü göstermek üzere tasarlanmıştır.

Metot: Bu çalışmada, disk imajı FTK Imager kullanılarak analiz için hazırlanmış ve içeriğindeki dosya yapıları detaylı bir şekilde incelenmiştir. Ardından, sistem kayıtları ve kullanıcı aktivitelerine dair bilgi toplamak amacıyla AmcacheParser, PECmd ve Registry Explorer gibi araçlar kullanılmıştır. Dosya meta verileri ExifTool ile analiz edilmiş, zaman çizelgesi oluşturmak için Timeline Explorer'dan faydalanılmıştır. Ayrıca, ShellBag Explorer ve BrowsingHistoryView gibi araçlar yardımıyla kullanıcının sistemdeki davranışları detaylandırılmıştır.

Değerlendirme: Bu çalışma, Adli Bilişim alanındaki teknik becerilerin geliştirilmesine katkı sağlayarak, dijital kanıtların elde edilmesi ve analiz edilmesi konusunda derinlemesine bir deneyim sunmaktadır. Kullanılan araçlar, dijital suç izlerini sürme ve veri analizi süreçlerini öğrenme fırsatı sağlamış, kullanıcı davranışlarının ve potansiyel suç unsurlarının tespiti konusunda önemli bir anlayış kazandırmıştır. Siber Güvenlik açısından yapılan değerlendirmelerde, ağ güvenliği ve kullanıcı kimlik doğrulama mekanizmalarının iyileştirilmesi gerektiği görülmüştür. Nmap ile yapılan güvenlik taramaları ve NTLM hash'leri gibi zayıf güvenlik protokolleri, sistemlerin tehdit altında olduğunu göstermektedir. Güçlü şifreleme algoritmaları, modern doğrulama yöntemleri ve güvenlik açıklarının hızlıca giderilmesi, güvenliği artırmak için temel gerekliliklerdir.

Anahtar kelimeler: adli bilişim, siber güvenlik, disk imajı, dijital delil, registry, şifreleme, hash

ANALYSIS OF DISK IMAGE USING DIGITAL FORENSICS TECHNIQUES

SUMMARY

Objective: The aim of this study is to analyze a disk image used in a CTF competition through digital forensics techniques, identify suspicious activities, uncover digital evidence, and gain hands-on experience with forensic tools while acquiring knowledge about the examined elements. The study is designed to demonstrate the effective use of forensic tools and the systematic execution of the analysis process.

Method: In this study, the disk image was prepared for analysis using FTK Imager, and the file structures within were examined in detail. System records and user activities were analyzed using tools such as AmcacheParser, PECmd, and Registry Explorer. File metadata was analyzed with ExifTool, and a timeline was created using Timeline Explorer. Additionally, user behaviors on the system were detailed with tools such as ShellBag Explorer and BrowsingHistoryView.

Conclusion: This study contributes to the development of technical skills in the field of digital forensics, providing in-depth experience in obtaining and analyzing digital evidence. The tools used offered opportunities to track digital crime traces and learn data analysis processes, enhancing understanding of user behaviors and potential criminal indicators. From a cybersecurity perspective, the findings highlight the need for improved network security and user authentication mechanisms. The use of tools like Nmap for security scanning and reliance on outdated and weak protocols such as NTLM hashes show significant vulnerabilities in systems. Implementing strong encryption algorithms, modern authentication methods, and promptly addressing security gaps are fundamental requirements for enhanced security.

Keywords: digital forensics, cybersecurity, disk image, digital evidence, registry, encryption, hash

1. GİRİŞ

Adli bilişim, bilişim sistemleri ve üzerinde bulunan depolama ünitelerinin, herhangi bir suçu işlemede veya yasaklanmış bir faaliyette kullanılıp kullanılmadığını tespit etmek amacıyla yapılan çalışmaların tümüdür. Terim olarak İngilizce "Computer Forensic" deyiminden çevrilerek/uyarlanarak Türkçeye kazandırılmıştır. Adli bilişimin temel amacı, dijital veriler ile olay arasındaki bağlantıyı veya fiil ile işlenen veriler ve kullanıcı arasındaki bağlantıyı açığa çıkarmaktır.. Genellikle çalışma alanları, sabit diskler, flash bellekler, CD/DVD vb. depolama aygıtları olsa da, sistemler üzerindeki incelemeler de dahil olmak üzere bu konuda çok çeşitli ve geniş bir çalışma sahasından söz etmek mümkündür. Adli bilişim, adli bilimlerin diğer dallarında olduğu gibi, "Kim?", "Neden?", "Nerede?", "Ne zaman?", "Nasıl?" sorularına cevap aranan bir bilim dalıdır. Fakat bilgisayar üzerinde bulunan veriler/dokümanlar narindir ve kolaylıkla değişikliğe uğrayabilir. Belgeler üzerindeki her türlü değişikliğin tespiti ve soruşturma esnasında mümkün olan en iyi şekilde korunarak sunulması özel yöntemler gerektirmektedir. Dijital delillerin elde edilebilmesi için, adli bilişim teknik ve yöntemleri kullanılır. Yetkisiz erişimler, bilgisayarların kötü amaçla kullanımı, dolandırıcılık ve endüstriyel casusluk gibi konularla günlük hayatta karşılaşma riski artmış ve bu nedenle kayıtlarını bilişim sistemleri üzerinde bulunduran tüm kurum ve kuruluşların adli bilişim ile tanışması bir ihtiyaç haline gelmiştir.

5/3/2021 tarihinde Birleşmiş Milletler Uyuşturucu ve Siber Suç Ofisi (United Nations Office on Drugs and Crime - UNODC), Afrika'nın dört bir yanındaki tüm siber güvenlik uzmanlık alanlarını kapsayan ve 4 haftadan oluşan, Carmen Corbin liderliğinde Afrika Dijital Adli Bilişim CTF (Capture the Flag) yarışması düzenlemiştir. Yarışmaya 29 Afrika ülkesi ve 282 katılımcı katılmıştır. Yarışma içeriği DFIR.Science tarafından hazırlanmıştır. Bu çalışmada, yarışma soruları üzerinden Adli Bilişim teknikleriyle inceleme yapıp sonuçları ortaya konacaktır.

1.1 Yarışma İçeriği

Bu yarışma, katılımcıların Adli Bilişim alanındaki bilgi ve becerilerini test etmek amacıyla tasarlanmış dört haftalık bir CTF etkinliğini içermektedir. Her hafta, dijital delil analizi üzerine farklı bir alana odaklanılacak olup, adli bilişim araçları kullanılarak çeşitli dijital artifactler incelenecektir.

CTF, aşağıdaki 4 başlıkta ve içerikten oluşmaktadır:

1. **Hafta:** Disk Analizi
2. **Hafta:** RAM Analizi
3. **Hafta:** Ağ Analiz
4. **Hafta:** Android Analizi

1.2 Yarışma Amaçları

- Katılımcıların, farklı dijital ortamlarda (disk, RAM, ağ, mobil cihaz) adli bilişim analiz yeteneklerini geliştirmek.
- Adli bilişim araçlarının ve tekniklerinin etkin bir şekilde kullanılmasını teşvik etmek.
- Katılımcıların dijital delil incelemesi konusundaki pratik bilgilerini artırmak.
- Dosya sistemlerinin yapısını incelenmesi
- Disk imajında gizli veya şifreli dosyaların tespiti
- Disk imajındaki dosyaların erişim, yazma ve oluşturulma tarihlerinin incelenmesi
- Sistem loglarının analizi
- Dosya ve klasörlerin metadata bilgilerinin analizi
- Kullanıcı profilleri ve şifreleri incelenmesi

2. METOT

Bu çalışmada FTK Imager, AmcacheParser.exe, exiftool, PECmd.exe, Registry Explorer, hashcat, BrowsingHistoryView, TimelineExplorer, ShellBags Explorer araçları kullanılacaktır. Adli Bilişim sürecinde kullanılan çeşitli araçları ve bu araçlarla ilgili genel bilgiler verilmektedir. Belirtilen araçlar, dijital delillerin toplanması, incelenmesi ve raporlanması sürecinde kritik bir rol oynamaktadır. FTK Imager haricinde kullanılan araçların analiz adımları Bulgular ve Sonuçlar bölümünde açıklanacaktır.

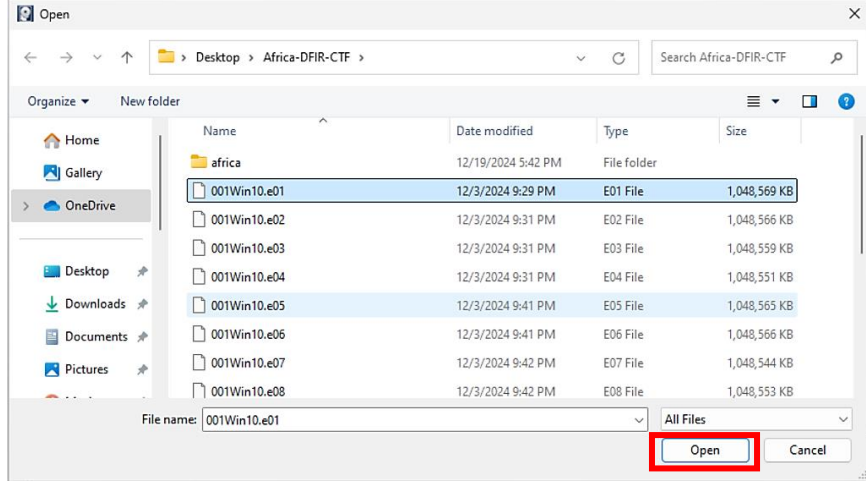
Ayrıca, projenin planlama ve analiz aşamalarında Gantt Şeması ve SWOT Analizi kullanılacaktır. Gantt şeması, projedeki adımların zamana göre ayrıştırılmasını ve sırasını belirlemek için kullanılırken, SWOT analizi, projenin güçlü ve zayıf yönlerini, fırsatları ve tehditleri değerlendirmek amacıyla uygulanacaktır. Bu araçlar, yapılan çalışmanın etkin bir şekilde planlanmasına ve analiz sürecinin daha verimli hale getirilmesine yardımcı olacaktır.

2.1 FTK Imager

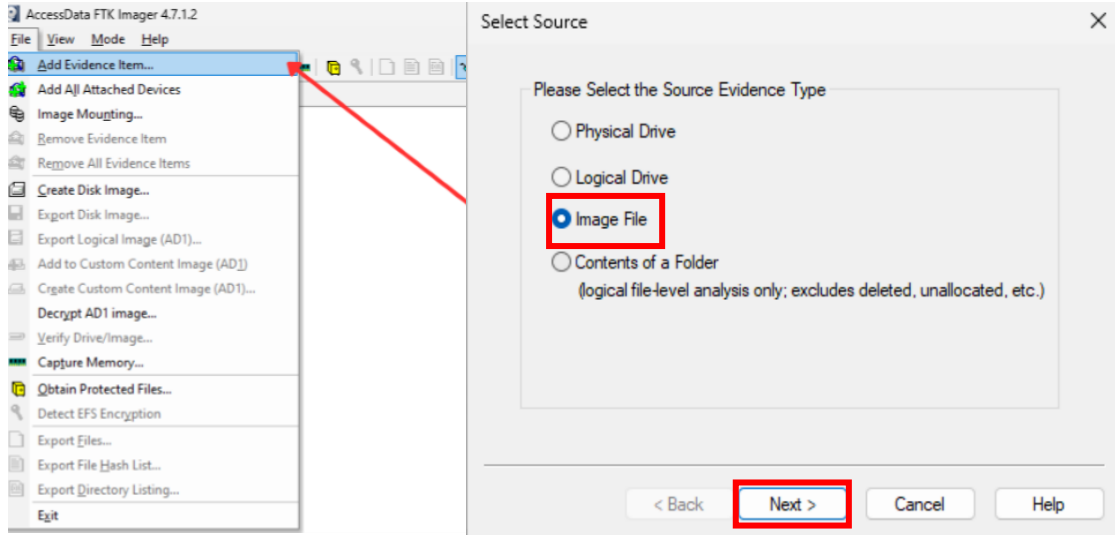
Disk imajı analizi için FTK Imager aracı kullanılacaktır. FTK Imager, verilerin bozulmadan alınmasını sağlayan, güvenli ve etkili bir disk görüntüleme aracıdır. Bu araç, farklı dosya sistemleriyle uyumlu olup, dijital delilleri toplama ve daha sonra bunlar üzerinde analiz yapma sürecinde güvenliği sağlar. Analiz süreci, aşağıdaki adımları içerecek şekilde yapılacaktır:

2.1.1 Disk İmajının Yüklenmesi

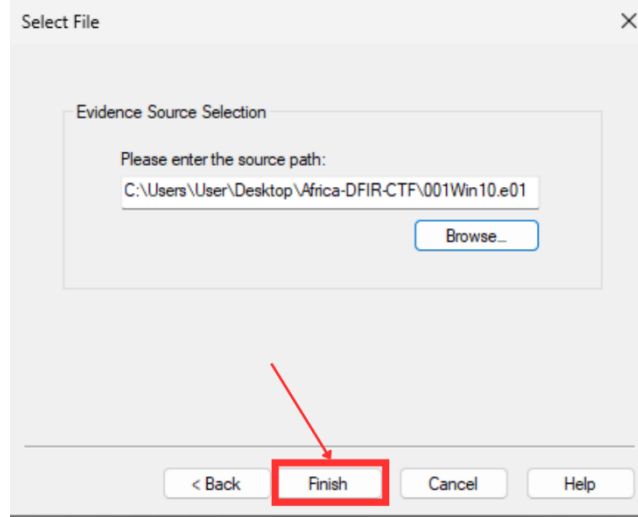
İlk adım olarak, FTK Imager aracılığıyla disk imajı yüklenir. Disk imajı, fiziksel bir diskin tam bir kopyasını içerdiği için, orijinal veriye zarar vermeden detaylı bir inceleme yapılmasına olanak sağlar.



Şekil 1.1: FTK Imager - Yüklenecek dosyanın türünün seçilmesi



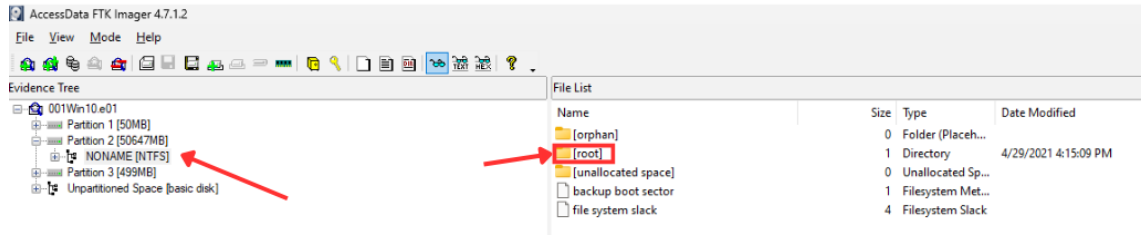
Şekil 1.2: İmaj dosyası seçimi



Şekil 1.3: .e01 uzantılı dosyanın yüklenmesi

2.1.2 Dosya Sistemi İncelemesi

Disk imajı, FTK Imager üzerinde açıldığında, dosya sisteminin yapısı (örneğin NTFS, FAT, EXT) analiz edilir. Bu aşamada, dosya ve dizinlerin yapılandırması, metadata bilgileri (oluşturulma, değiştirilme tarihleri, dosya boyutları vb.) detaylı bir şekilde gözden geçirilir.



Şekil 2.1: NTFS biçimli diskin root dosyası incelenmesi

2.1.3 Disk İmajındaki Gizli Verilerin Analizi

Disk üzerinde gizli veya şifreli dosyaların varlığı kontrol edilir. FTK Imager'ın sunduğu araçlarla, gizli dosyalar, geçici dosyalar, geçmiş veriler ve şifrelenmiş içerikler incelenir.

2.2 AmcacheParser.exe

AmcacheParser.exe, Windows sistemlerinde önemli verileri sağlayan Amcache.hve dosyasını incelemek için kullanılmıştır. Bu araç, sistemde yüklü olan uygulamaların geçmişini ve yüklenme zamanlarını gösterir. Bu sayede şüpheli yazılımlar veya şüpheli zaman dilimlerinde yapılan işlemler tespit edilmektedir.

2.3 Registry Explorer

Registry Explorer, Windows kayıt defteri üzerinde yapılan değişiklikleri ve sistem ayarlarını incelemek için kullanılmıştır. Windows kayıt defteri, kullanıcının davranışlarını, sistemdeki uygulamaların çalıştığı zaman dilimlerini ve daha birçok kritik bilgiyi barındırır. Bu araçla:

- Kullanıcı aktiviteleri ve sistem yapılandırmaları detaylı şekilde gözden geçirilmiştir.
- Sistem geçmişi, zaman damgaları ve yapılan değişiklikler analiz edilmiştir.

2.4 exiftool

exiftool, dijital dosyaların metadatalarını incelemek için kullanılmıştır. Bu araç, özellikle fotoğraf ve belge dosyaları üzerinde yapılan incelemelerde önemli bilgiler sunar. Dosya oluşturulma tarihi, son değiştirilme tarihi, yazar bilgileri ve coğrafi konum gibi veriler toplanmış ve analiz edilmiştir. Bu sayede:

- Dosyaların geçmişi, kaynağı ve olası manipülasyon izleri incelenmiştir.

2.5 PECmd.exe

PECmd, Eric Zimmerman tarafından geliştirilen, Windows işletim sistemlerinde Prefetch dosyalarını (.pf) işlemek ve aşağıdaki öğeleri tanımlamak için kullanılan bir komut satırı aracıdır:

- Volume bilgisi
- Çalıştırma süresi
- Toplam çalıştırma sayısı

PECmd, parse edilmiş (ayrıştırılmış) prefetch dosyalarını daha ileri analiz için .csv, json ve HTML formatlarına çıktı olarak verebilir.

2.6 Hashcat

Hashcat, parolaların hash'lerini kırmak için kullanılan güçlü bir şifre çözme aracıdır. Bu araç, şüpheli kullanıcı parolalarını çözmek için kullanılmıştır. Kullanıcıların parolaları, NTLM veya diğer hash algoritmalarında şifrelenmiş olabilir. Hashcat ile yapılan analizle:

- Şüpheli parolaların çözülmesi sağlanmıştır.

2.7 BrowsingHistoryView

BrowsingHistoryView, web tarayıcılarında kaydedilen geçmiş verilerini incelemek için kullanılmıştır. Bu araç, kullanıcıların tarayıcı geçmişi, çerezler ve indirme geçmişi gibi bilgileri detaylı şekilde gösterir. Elde edilen verilerle:

- Kullanıcıların internet aktiviteleri ve şüpheli bağlantılar belirlenmiştir.
- Zaman dilimleri içinde gerçekleşen internet aktiviteleri incelenmiştir.

2.8 Timeline Explorer

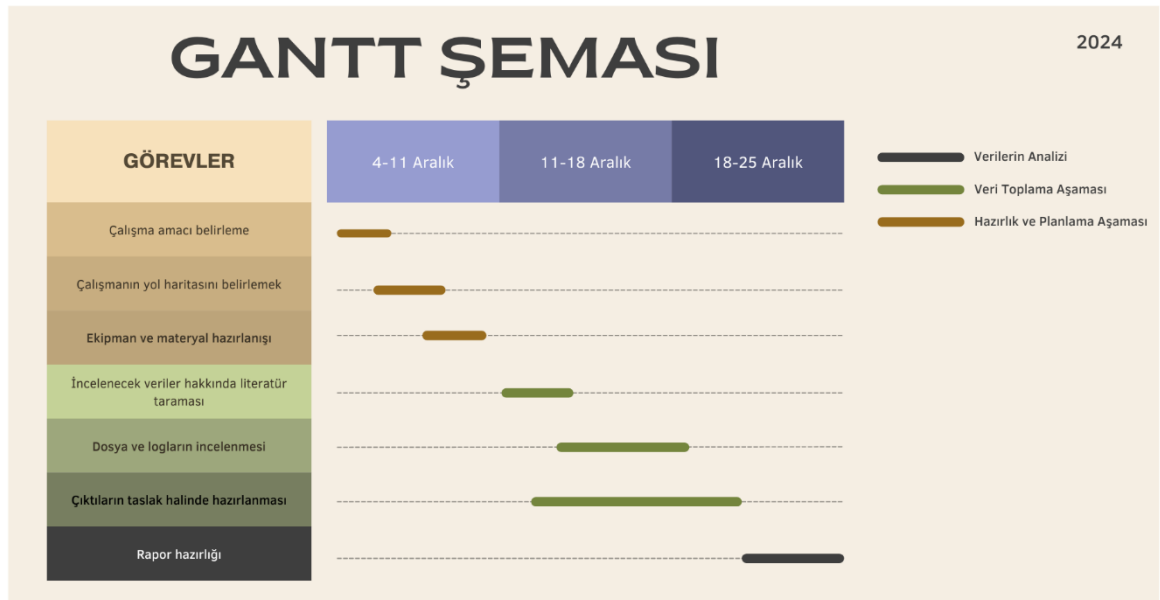
.csv uzantılı dosyaların verilerini parametrelerine göre bölerek incelemeye olanak sağlayan bir Eric Zimmerman aracıdır. TimelineExplorer, olayların zaman sırasına göre organize edilmesi için kullanılmıştır. Bu araç, şüpheli aktivitelerin sistemde ne zaman ve hangi koşullarda gerçekleştiğini daha net bir şekilde anlamayı sağlamaktadır. Elde edilen tüm dijital izler, bu araç ile birleştirilerek, daha kapsamlı bir analiz yapılmıştır.

2.9 ShellBags Explorer

ShellBags Explorer, Windows işletim sistemlerinde dosya ve klasörlere erişim tarihlerini ve yapılandırmalarını incelemek için kullanılmıştır. Bu araç, kullanıcıların sistemdeki belirli dosyalara ve klasörlere erişim geçmişini gösterir. Eric Zimmerman tarafından geliştirilmiştir.

2.10 GANTT Şeması

Gantt şeması, bir proje yönetim aracıdır ve projedeki görevlerin sırasını, süresini ve birbirleriyle olan ilişkilerini görsel olarak sunar. Bu şema, projelerin zaman yönetimini kolaylaştırmak, görevlerin tamamlanma sürelerini takip etmek ve olası gecikmeleri önceden görerek düzenlemeler yapmak için kullanılır. Gantt şeması, özellikle büyük ve karmaşık projelerde ilerlemenin izlenmesi için oldukça etkilidir. Her görev için başlangıç ve bitiş tarihleri belirlenir ve proje zaman çizelgesi üzerinde bir takvim üzerinde gösterilir.



Şekil 3.1: GANTT Şeması

2.11 SWOT Analizi

SWOT analizi, bir organizasyonun, projenin veya bireysel bir stratejinin güçlü yönlerini (Strengths), zayıf yönlerini (Weaknesses), fırsatlarını (Opportunities) ve tehditlerini (Threats) değerlendirerek stratejik kararlar almak için kullanılan bir araçtır. Bu analiz, içsel faktörleri (güçlü ve zayıf yönler) ve dışsal faktörleri (fırsatlar ve tehditler) inceleyerek kapsamlı bir değerlendirme yapmayı amaçlar.

3. BULGULAR VE SONUÇLAR

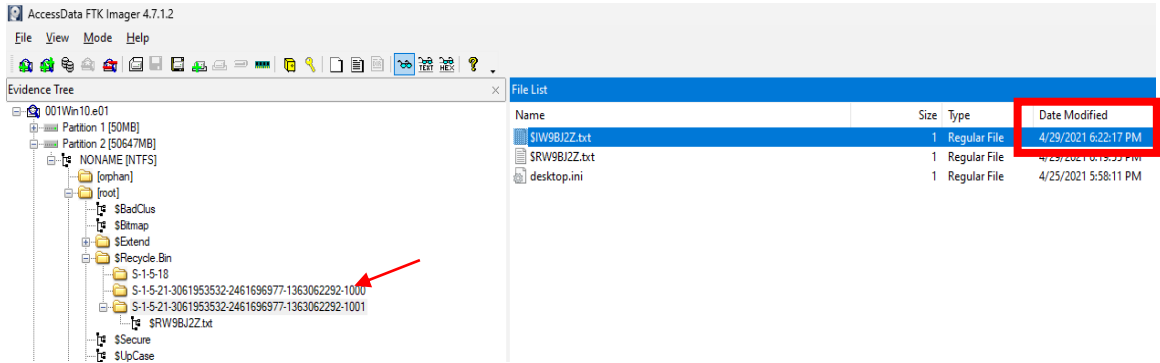
Yapılan incelemeler kapsamında her bir soru hakkında elde edilen sonuçlar tek tek açıklanacaktır. Her bir sorunun nasıl çözüldüğüne dair açıklamalar yapılacak, teknik detaylarla birlikte çözüm adımlarını açıkça belirtilecektir.

3.1 Soru 1

UTC zaman dilimine göre bir parola listesi hangi tarih ve saatte silinmiştir?

Bu soruyu cevaplamadan önce sahip olmamız gereken bazı bilgiler var. Geri Dönüşüm Kutusu'na gönderilen yani silinen dosyaları disk imajını incelerken nasıl bulabiliriz? Bu sorunun cevabı ise şöyle:

Windows 10 ve Windows 8 ve Windows 7 dahil olmak üzere Windows'un yeni sürümlerinde değişikliğe gidilmiştir ve Geri Dönüşüm Kutusu verileri diskteki kök dizininde (Örneğin C:\\$Recycle.Bin\S-1-5-21-...) her bir kullanıcı için farklı bir "\$Recycle.Bin" adlı gizli dosyada depolanmaktadır.

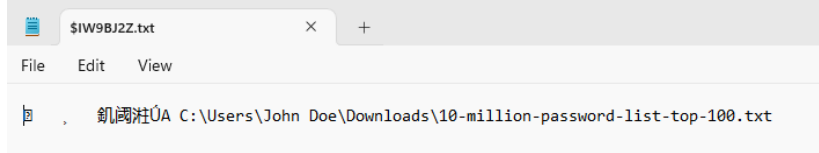


Şekil 4.1: \$I dosyası konumu ve değiştirilme zamanı

Neden \$R dosyasını değil de \$I dosyasını ele aldığımızı açıklayalım. Windows işletim sisteminde, Geri Dönüşüm Kutusu ile ilişkili \$I ve \$R ile başlayan adlara sahip dosyalar vardır. Bu dosyalar, silinen dosyalar hakkında bilgi yönetmek ve depolamak için Geri Dönüşüm Kutusu tarafından dahili olarak kullanılır. Bir dosya silindiğinde, Geri Dönüşüm Kutusu dosyayı dahili yapısına taşır. \$I dosyaları ve \$R dosyaları burada oluşturulur.

3.1.1 \$I Dosyaları

\$I ile başlayan adlara sahip dosyalar INFO2 dosyaları olarak bilinir. Her silinen dosya hakkında orijinal dosya adı, silindiği tarih ve saat ve diğer öznitelikler gibi meta veri bilgilerini depolarlar.



Şekil 4.2: Silinen dosyanın adını içeren \$I dosyası

3.1.2 \$R Dosyaları

\$R ile başlayan adlara sahip dosyalar Geri Dönüşüm Kutusu veri dosyaları olarak bilinir. Bu dosyalar silinen dosyaların gerçek verilerini depolar. İçeriğini kontrol etmek için bu dosyayı Geri Dönüşüm Kutusu dizininin dışına kopyalamak gerekir.



Şekil 4.3: Silinen dosyanın içeriğini barındıran \$R dosyası

Geri Dönüşüm Kutusu boşaltıldığında, ilişkili '\$I' (INFO2) ve '\$R' dosyaları genellikle silinen dosyalarla birlikte kaldırılır. Geri Dönüşüm Kutusu'nu boşaltmak, içerdiği öğeleri kalıcı olarak silmek anlamına gelir.

Cevap: 2021-04-29 18:22:17 UTC

3.2 Soru 2

Şüphelinin bağlandığı FTP sunucusunun IPv4 adresi nedir?

Kullanıcının sisteminde yüklü programları inceleyip FTP sunucusu ile ilişkili bir program var mı araştırıyoruz. Sistemdeki yüklü uygulamaları bulmak için bir registry (kayıt defteri) verisi olan SOFTWARE dosyasını inceliyoruz. Registry kayıtları, Windows'un ve Windows'ta çalışan uygulamaların ve hizmetlerin çalışması için kritik öneme sahip verileri içeren hiyerarşik bir veritabanıdır.

3.2.1 SOFTWARE

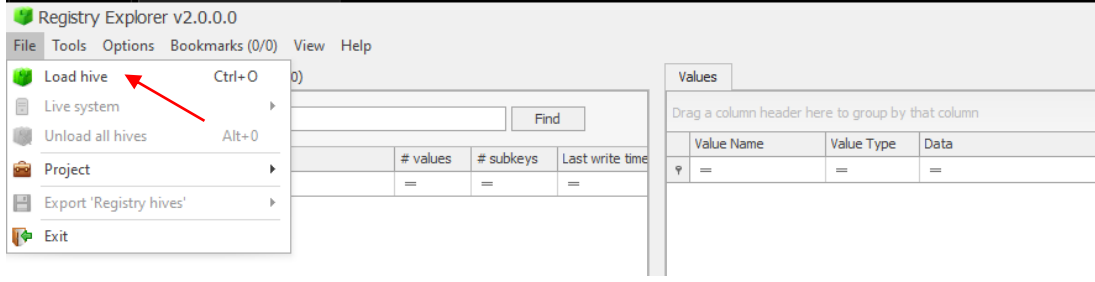
Windows Kayıt Defteri, sistem yapılandırması, kullanıcı etkinliği gibi bilgileri tutar. Yüklü programlar artifacti, kayıt defteri verilerinden elde edilir ve sisteme yüklenen uygulamalar hakkında ayrıntılar içerir. Yüklenen uygulamanın adı, sürümü, boyutu, yayıncısı, uygulamanın en son yüklendiği veya güncellendiği tarih, uygulamanın yürütülebilir (.exe) dosyasının konumu ve sisteme yüklenen uygulamalarla ilgili diğer birçok ayrıntı gibi bilgileri tutar. SOFTWARE dosyasının dizini:

- C:\Windows\System32\config\SOFTWARE

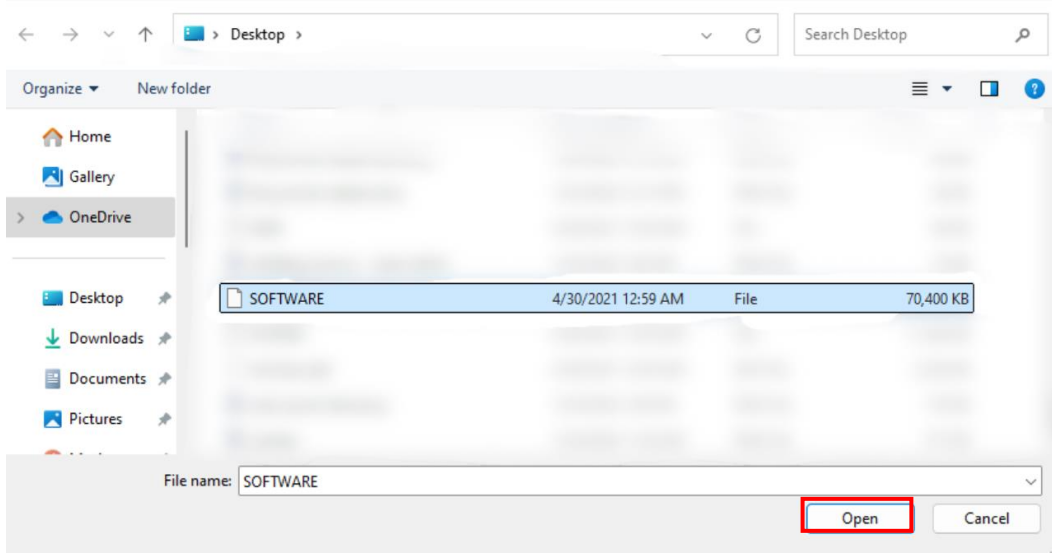
Yüklü programlar ile ilgiliyi bilgiye, SOFTWARE registry dosyasının aşağıdaki dizinlerinden ulaşılabilir:

- Microsoft\Windows\CurrentVersion\Uninstall
- WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall

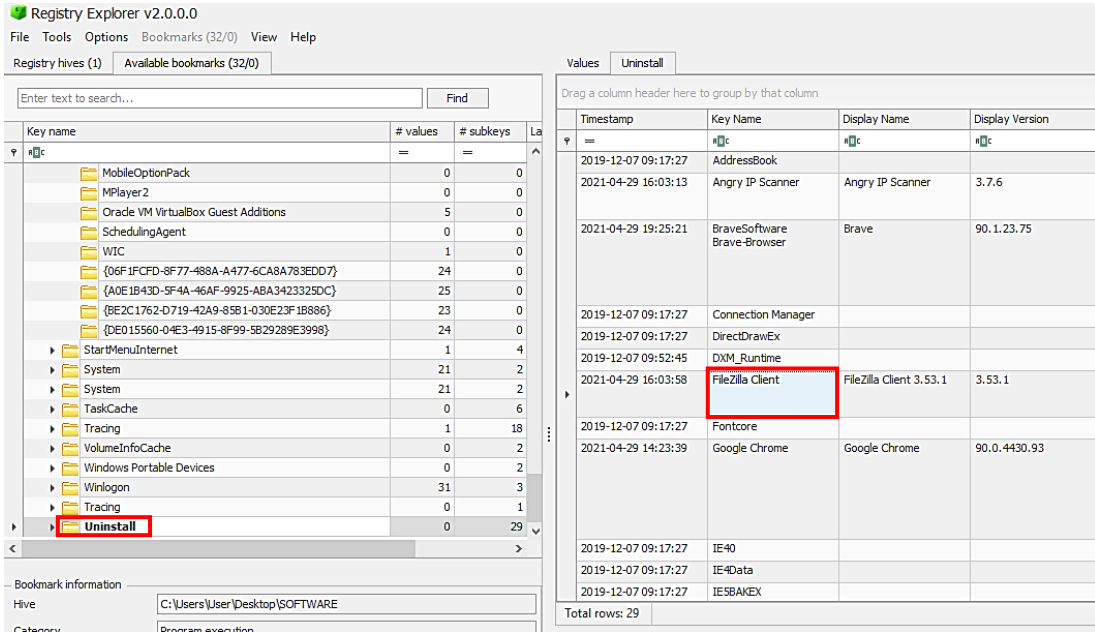
SOFTWARE dosyasını incelemek için Eric Zimmerman'ın geliştirmiş olduğu Adli Bilişim araçlarından biri olan Registry Explorer programını kullanıyoruz.



Şekil 5.1: Registry Explorer – Load hive seçimi

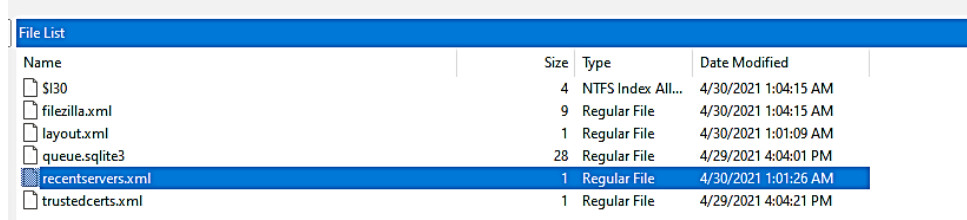


Şekil 5.2: SOFTWARE dosyası seçimi



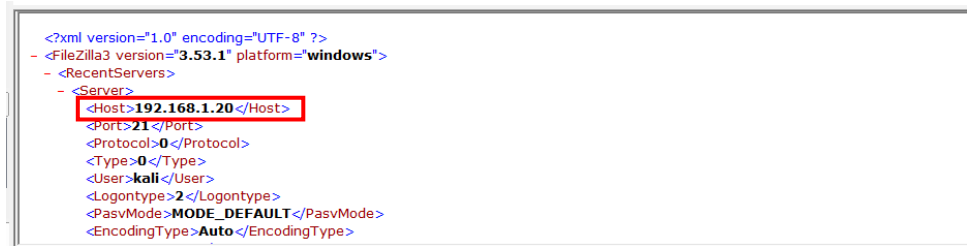
Şekil 5.3: Uninstall dizinindeki önceden yüklenmiş programlar

Kayıtta FTP sunucusu işlemlerini gerçekleştiren FileZilla isimli programın yüklü olduğunu görüyoruz. İlgili programın loglarını incelemek için *C:\Users\John Doe\AppData\Roaming\FileZilla* dizininde bulunan *recentservers.xml* isimli dosyaya erişiyoruz. Burada bağlantı yapılan FTP sunucusunun IPv4 adresini görebiliriz.



Name	Size	Type	Date Modified
\$I30	4	NTFS Index All...	4/30/2021 1:04:15 AM
filezilla.xml	9	Regular File	4/30/2021 1:04:15 AM
layout.xml	1	Regular File	4/30/2021 1:01:09 AM
queue.sqlite3	28	Regular File	4/29/2021 4:04:01 PM
recentservers.xml	1	Regular File	4/30/2021 1:01:26 AM
trustedcerts.xml	1	Regular File	4/29/2021 4:04:21 PM

Şekil 5.4: FileZilla programına ait recentservers.xml dosyası



```
<?xml version="1.0" encoding="UTF-8" ?>
- <FileZilla3 version="3.53.1" platform="windows">
- <RecentServers>
- <Server>
- <Host>192.168.1.20</Host>
  <Port>21</Port>
  <Protocol>0</Protocol>
  <Type>0</Type>
  <User>kali</User>
  <Logontype>2</Logontype>
  <PasvMode>MODE_DEFAULT</PasvMode>
  <EncodingType>Auto</EncodingType>
```

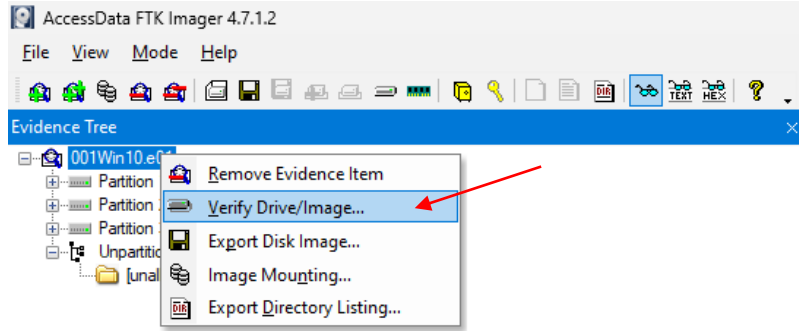
Şekil 5.5: Bağlanılan FTP sunucusu IPv4 adresi

Cevap: 192.168.1.20

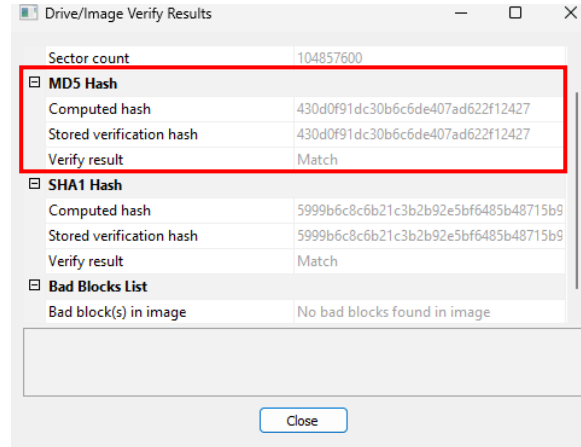
3.3 Soru 3

Şüpheli diskin MD5 hash değeri nedir?

Hash değeri, bir verinin (örneğin bir dosya, metin veya şifre) belirli bir algoritma kullanılarak oluşturulan benzersiz bir dijital parmak izi ya da özetidir. Bu değer, genellikle sabit uzunluktadır ve verinin içeriğine dayalı olarak hesaplanır. Hash değeri dosya adının veya tarihinin değişmesiyle değişmez. Sadece içindeki veri değeri değişirse hash değeri değişir.



Şekil 6.1: Verify Drive/Image... seçimi



Şekil 6.2: İmajın MD5 hash değeri

Cevap: 430d0f91dc30b6c6de407ad622f12427

3.4 Soru 4

Şüpheli 2021-04-29 18:17:38 UTC tarihinde hangi ifadeyi aradı? (üç kelime)

Adli Bilişim’de tarayıcı (browser) incelenmesi, bir kullanıcının çevrimiçi faaliyetlerine ilişkin değerli bilgiler sunar ve olay müdahalesinde hayati bir rol oynar. Ziyaret edilen web siteleri, oturum açma kimlik bilgileri, indirme geçmişi, yer imleri ve yüklü uzantılar veya eklentiler gibi bilgileri içerir.

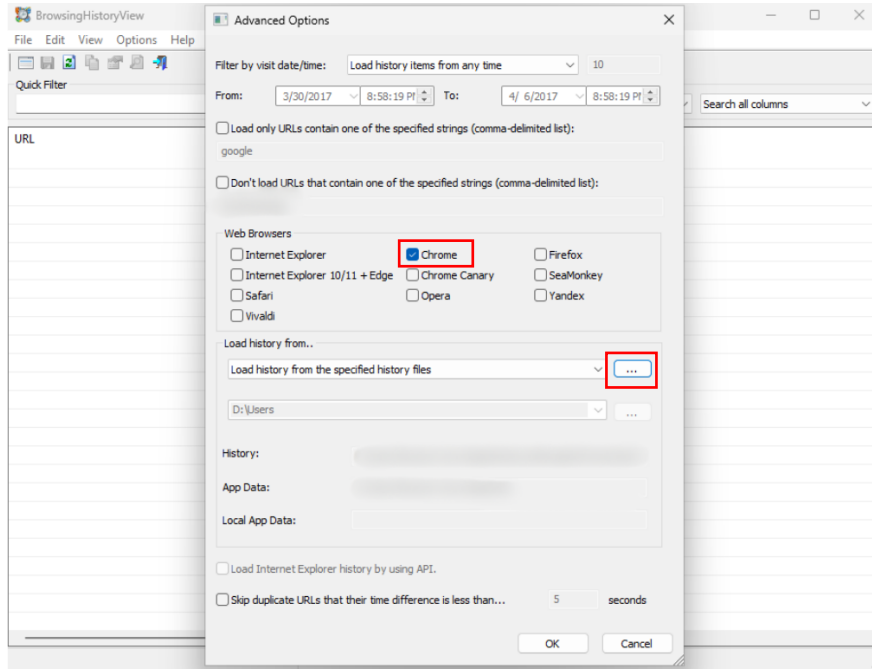
Tarayıcı loglarının incelenmesi için her bir tarayıcının kendine ait olan kayıtlarını ele almak gerekir. Şüphelinin aramış olduğu ifadeyi bulmak için sisteminde yüklü olan tarayıcıları buluyoruz. Tarayıcı analizinde geçmiş aramalara ulaşmak için History dosyasını inceleyerek aşağıdaki bilgileri gözden geçiriyoruz:

- Son X günde hangi siteler ziyaret edildi?
- Her ziyaret için URL, sayfa başlığı ve yönlendiren site
- Bir sitenin kaç kez ziyaret edildiği
- Her ziyaretin belirli tarihi ve saati
- Siteyi ziyaret etmek için kullanılan kullanıcı hesabı

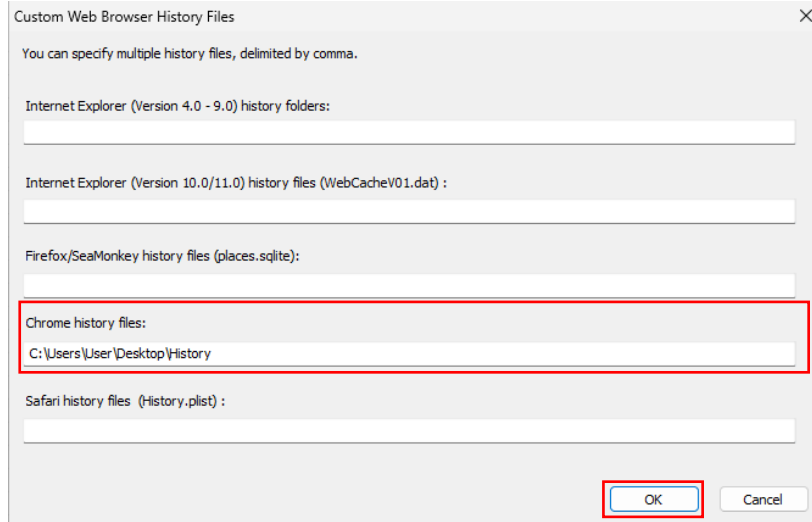
Tarayıcılarda History dosyasının tutulduğu dizinler:

- AppData\\Local\\Microsoft\\Edge\\User Data\\Default
- AppData\\Local\\Google\\Chrome\\User Data\\Default
- AppData\\Local\\BraveSoftware\\Brave-Browser\\User Data\\Default

Her bir tarayıcının History dosyasını incelediğimizde aradığımız sonucun Chrome tarayıcısı kayıtlarında olduğunu buluyoruz. History kayıtlarını incelemek için Nir Sofer’in geliştirdiği BrowsingHistoryView aracını kullanıyoruz.



Şekil 7.1: İncelenecek tarayıcı seçimi



Şekil 7.2: History dosyasının dizinini ekleme

rockyou text download - Google Search	4/29/2021 6:16:40 PM
rockyou text download - Google Search	4/29/2021 6:16:41 PM
password cracking lists - Google Search	4/29/2021 6:17:37 PM
password cracking lists - Google Search	4/29/2021 6:17:38 PM

Şekil 7.3: Şüphelinin ziyaret ettiği dizinler

Kayıtları incelediğimizde 2021-04-29 18:17:38 UTC tarihine ait aramanın “password cracking list” olduğunu görüyoruz.

Cevap: password cracking list

3.5 Soru 5

"20210429_152043.jpg" adlı fotoğraf hangi ülkede çekilmiştir?

Bu soruyu cevaplayabilmek için .jpg formatlı dosyanın metadatasını incelememiz gerekmektedir. Peki metadata nedir?

3.5.1 Metadata

Metadata, kısaca veri hakkındaki veri olarak tanımlanabilir. Bir veri setinin veya bilgi kaynağının içeriği, yapısı ve özellikleri hakkında bağlam ve detaylar sağlar. Başlık, yazar, oluşturma tarihi, dosya formatı, boyut ve anahtar kelimeler gibi özellikleri içerir.

Metadayı incelemek için ExifTool isimli araç kullanılmaktadır.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

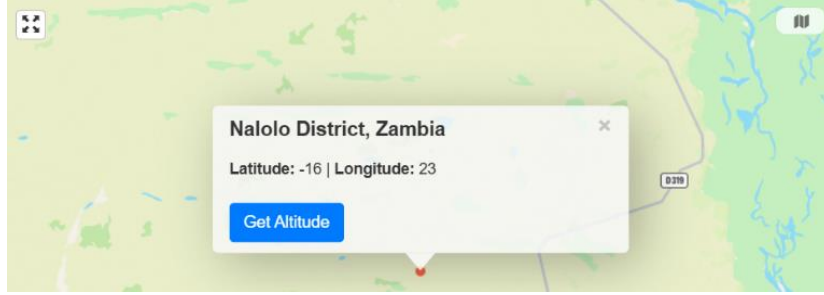
PS C:\Users\User\Desktop\toolbag\exiftool> .\exiftool.exe C:\Users\User\Desktop\20210429_152043.jpg
```

Şekil 8.1: exiftool sentaks yapısı

```
Windows PowerShell
Chromaticity Channels      : 3
Chromaticity Colorant     : Unknown (0)
Chromaticity Channel 1   : 0.64 0.33002
Chromaticity Channel 2   : 0.3 0.60001
Chromaticity Channel 3   : 0.15001 0.06
Device Mfg Desc          : GIMP
Device Model Desc        : sRGB
Comment                  : 0 AC original_brightness(123.3) bright_enhanced_level(0.0) brightness_shift(1.3) bri
ghtness_high_level(194), contrast_enhanced_level(14.8) isOutdoor(1) lux(145.9) FM0 CR0 Prmid2 mxDrkA0.03 mxBrA0.00 mxPk
NSat6.38 dr0.05 br6.82 wdr0.00 wbr16.44 sbr6.06 ldr0.25 lp51.0 [f0] 00000000bfalic 00000
Image Width              : 4160
Image Height             : 3120
Encoding Process         : Progressive DCT, Huffman coding
Bits Per Sample          : 8
Color Components         : 3
Y Cb Cr Sub Sampling     : YCbCr4:2:0 (2 2)
Aperture                 : 2.2
GPS Latitude              : 16 deg 0' 0.00" S
GPS Longitude            : 23 deg 0' 0.00" E
GPS Position             : 16 deg 0' 0.00" S, 23 deg 0' 0.00" E
Image Size               : 4160x3120
```

Şekil 8.2: Metada içerisinde elde edilen koordinat bilgileri

ExifTool ile elde ettiğimiz enlem ve boylam bilgilerini <https://www.gps-coordinates.net/> isimli site vasıtasıyla araştırıyoruz.



Şekil 8.3: Koordinatın gösterdiği lokasyon

Cevap: Zambiya

3.6 Soru 6

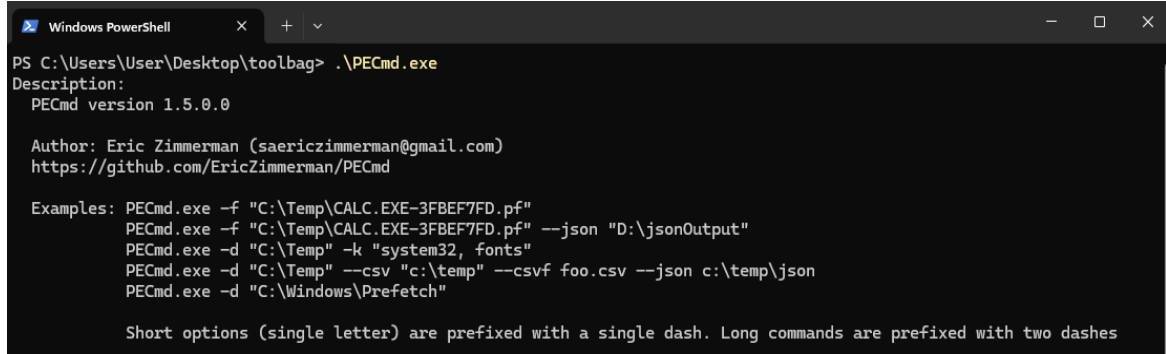
Şüpheli bilgisayarda Tor Browser kaç kez çalıştırıldı?

Bir programın kaç kez çalıştırıldığını öğrenmek için Prefetch artifactinden yararlanacağız. Prefetch artifactini incelemek için Eric Zimmerman'ın geliştirmiş olduğu PECmd.exe aracını kullanacağız. Çıktılarını ise yine Eric Zimmerman tarafından geliştirilen TimeExplorer uygulaması ile inceleyeceğiz.

3.6.1 Prefetch

Prefetch dosyası, Windows'ta bir uygulama açıldığında oluşturulan bir dosyadır. Bir uygulama belirli bir alandan ilk kez çalıştırıldığında, Windows bir prefetch (önceden getirme) kaydı yapar. Bu özellik sık kullanılan uygulamaların başlangıç sürelerini daha da kısaltmaktadır. Prefetch ile dosya adı, dosya konumu, dosya konumu hash değeri, dosyanın oluşturulma ve erişim zaman damgalarını, en son çalıştırılma zamanını, çalıştırılma sayısını ve uygulamanın talep ettiği DLL'leri tespit edebiliriz.

Prefetch dosyasını ayrıştırmak için Eric Zimmerman'ın geliştirdiği araçlardan biri olan PECmd.exe kullanılmaktadır.



```
Windows PowerShell
PS C:\Users\User\Desktop\toolbag> .\PECmd.exe
Description:
  PECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Examples: PECmd.exe -f "C:\Temp\CALC.EXE-3FBEF7FD.pf"
  PECmd.exe -f "C:\Temp\CALC.EXE-3FBEF7FD.pf" --json "D:\jsonOutput"
  PECmd.exe -d "C:\Temp" -k "system32, fonts"
  PECmd.exe -d "C:\Temp" --csv "c:\temp" --csvf foo.csv --json c:\temp\json
  PECmd.exe -d "C:\Windows\Prefetch"

Short options (single letter) are prefixed with a single dash. Long commands are prefixed with two dashes
```

Şekil 9.1: PECmd.exe komut sentaksı

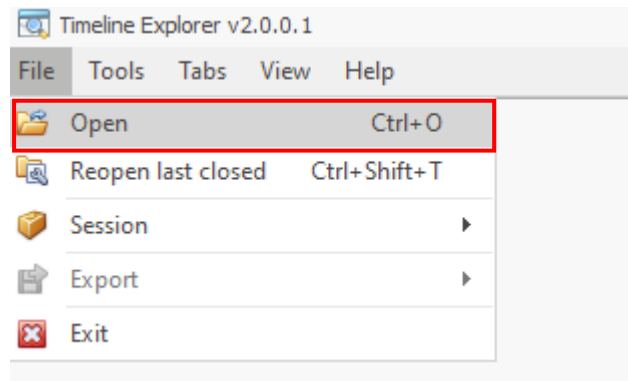
Prefetch dosyasını parse etmek için “*PECmd.exe -d C:\Users\User\Desktop\Prefetch — csv C:\Users\User\Desktop\Prefetch-Cikti*” komutunu kullanıyoruz.



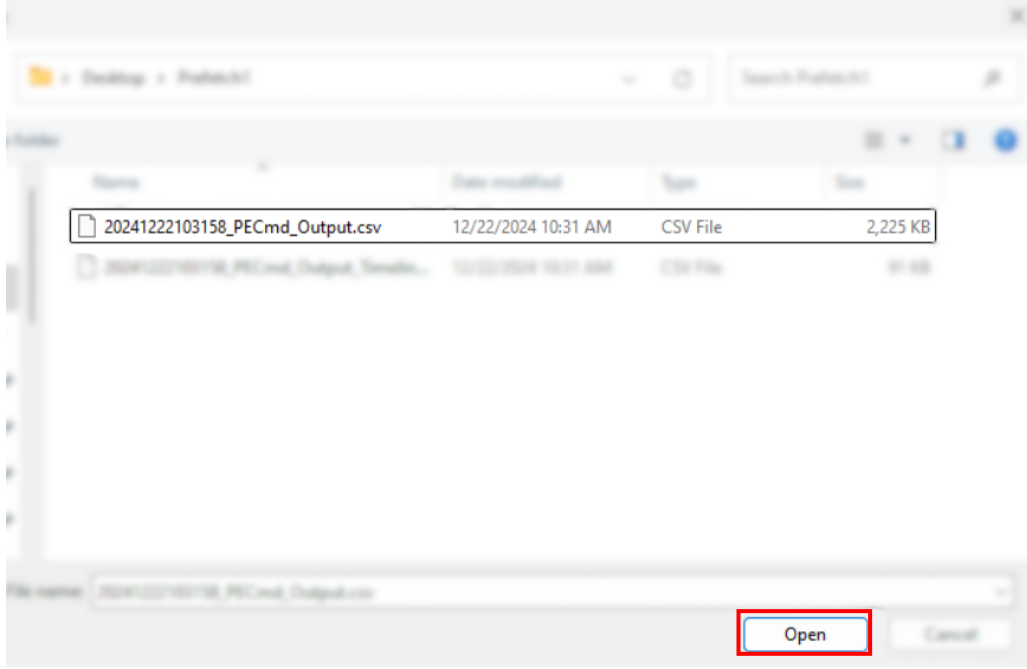
```
PS C:\Users\User\Desktop\toolbag> .\PECmd.exe -d C:\Users\User\Desktop\Prefetch --csv "C:\Users\User\Desktop\Prefetch -Cikti"
```

Şekil 9.2: Prefetch dosyasını parse etmek için kullanılan komut

Elde edilen çıktı .csv uzantılı bir dosya ve bu dosyayı analiz etmek için yine Eric Zimmerman'ın geliştirmiş olduğu bir araç olan Timeline Explorer kullanılmaktadır.



Şekil 9.3: Timeline Explorer csv dosyası açma



Şekil 9.4: .csv uzantılı Prefetch çıktısı seçimi

Timeline Explorer v2.0.0.1

File Tools Tabs View Help

20241222103158_PECmd_Output.csv

Drag a column header here to group by that column

	Source Filename	Volume1Seri...	Run Count
+	C:\Users\User\Desktop\Prefetch\SVCHOST.EXE-E45D8788.pf		1
	C:\Users\User\Desktop\Prefetch\SVCHOST.EXE-E8610451.pf		3
	C:\Users\User\Desktop\Prefetch\SVCHOST.EXE-EDE0F878.pf		6
	C:\Users\User\Desktop\Prefetch\SVCHOST.EXE-EE1C9ACA.pf		46
	C:\Users\User\Desktop\Prefetch\SYMENU.EXE-A56F0640.pf		1
	C:\Users\User\Desktop\Prefetch\SYSTEMSETTINGS.EXE-01D72268.pf		2
	C:\Users\User\Desktop\Prefetch\SYSTEMSETTINGSBROKER.EXE-CBC37DFF.pf		1
	C:\Users\User\Desktop\Prefetch\TASKHOSTW.EXE-3E0B74C8.pf		62
	C:\Users\User\Desktop\Prefetch\TEXTINPUTHOST.EXE-18B298A2.pf		2
	C:\Users\User\Desktop\Prefetch\TEXTINPUTHOST.EXE-1D9ED047.pf		2
	C:\Users\User\Desktop\Prefetch\TIWORKER.EXE-E317E7F1.pf		27
	C:\Users\User\Desktop\Prefetch\TORBROWSER-INSTALL-WIN64-10.0-F3C4DF19.pf		1

Şekil 9.5 : Prefetch çıktıları

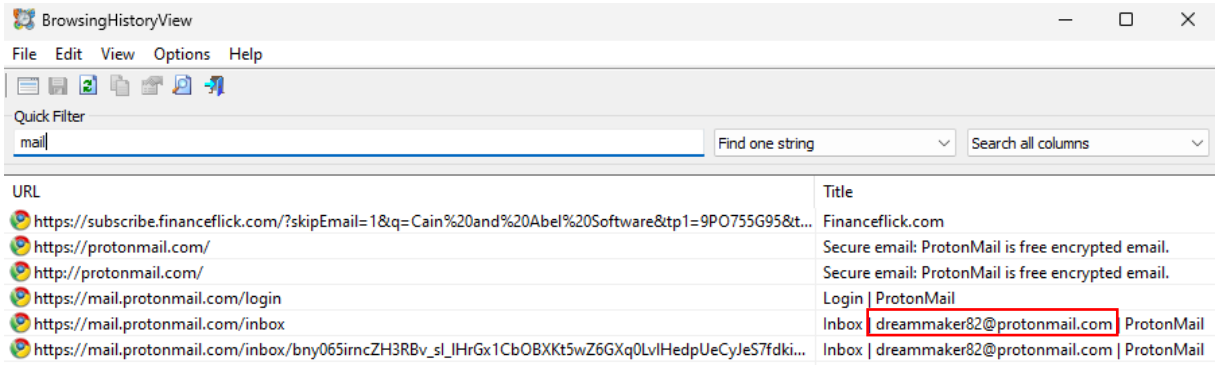
Ekrana gelen kayıtlarda “Run Count” sekmesinde uygulamanın kaç kez çalıştırıldığı görülmektedir. Şüpheli Tor Browser tarayıcısının kurulum exe dosyasını 1 kez çalıştırmıştır ancak kurulum sonrasında Tor Browser’ı hiç kullanmadığı için Prefetch kayıtlarında Tor Browser yer almamıştır.

Cevap: 0

3.7 Soru 7

Şüphelinin e-posta adresi nedir?

Şüphelinin e-posta adresini bulabilmek için tarayıcı geçmişini inceleyip e-posta hesabına giriş yapıp yapmadığını kontrol etmemiz gerekiyor. Yukarıda da belirtildiği gibi bir kullanıcının tarayıcı geçmişini History dosyası üzerinden inceleyebiliriz. Şüphelinin Chrome tarayıcı geçmişini incelediğimizde aradığımız sonuca ulaşıyoruz.



The screenshot shows a window titled 'BrowsingHistoryView' with a menu bar (File, Edit, View, Options, Help) and a toolbar. A 'Quick Filter' box contains the text 'mail'. Below the filter, there are two dropdown menus: 'Find one string' and 'Search all columns'. The main area displays a table of search results with two columns: 'URL' and 'Title'.

URL	Title
https://subscribe.financeflick.com/?skipEmail=1&q=Cain%20and%20Abel%20Software&tp1=9PO755G95&t...	Financeflick.com
https://protonmail.com/	Secure email: ProtonMail is free encrypted email.
http://protonmail.com/	Secure email: ProtonMail is free encrypted email.
https://mail.protonmail.com/login	Login ProtonMail
https://mail.protonmail.com/inbox	Inbox dreammaker82@protonmail.com ProtonMail
https://mail.protonmail.com/inbox/bny065irncZH3RBv_sl_IHrGx1CbOBXKt5wZ6GXq0LvlHedpUeCyJeS7fdki...	Inbox dreammaker82@protonmail.com ProtonMail

Şekil 10.1 : Şüphelinin ziyaret ettiği mail servisi

Cevap: dreammaker82@protonmail.com

3.8 Soru 8

Şüpheli port taraması hangi web sitesinde yapıldı?

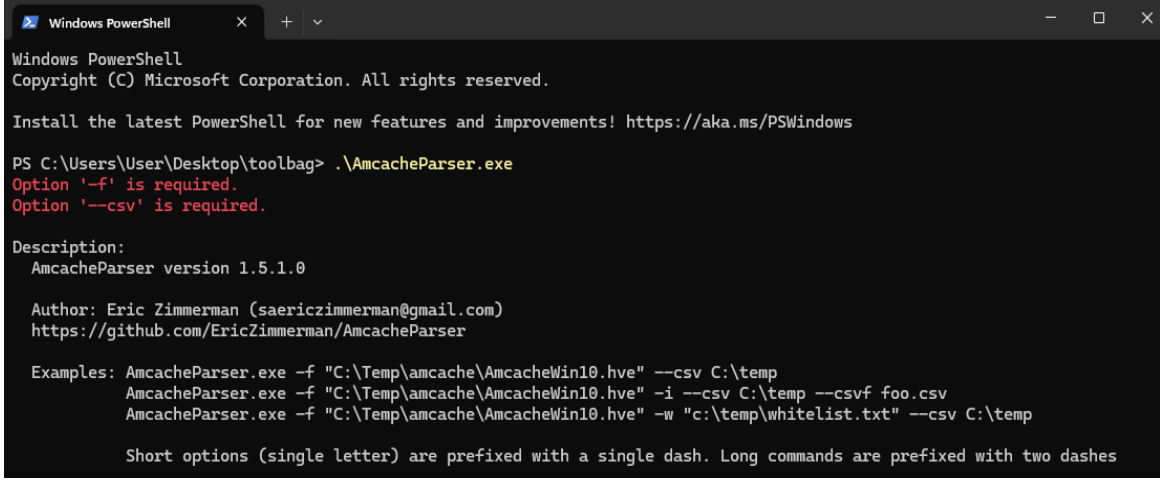
Port taraması yapmak için kullanılacak araçların sistemde yüklü olup olmadığını kontrol etmemiz gerekiyor. Daha önce SOFTWARE registry kaydını inceleyerek yüklü programları incelemiştik. Bu soruda farklı bir artifact üzerinden ilerleyeceğiz. Değineceğimiz artifact Amcache. “Amcache nedir, nasıl analiz edilir?” sorularına açıklama getirelim.

3.8.1 Amcache

Amcache.hve dosyası windows işletim sistemleri arasındaki program uyumsuzluğunu ortadan kaldırmak amaçlı oluşturulmuş bir dosyadır. Windows işletim sisteminin sistem dosyası olan Amcache.hve dosyaları registry kayıt dosyasıdır.

İşletim sistemine yüklenen herhangi bir program için, bu programın hash değeri, programın çalıştığı yol ve program hakkındaki zaman damgaları (programın yüklenmesi ve silinmesi) hakkında bilgi verir.

Amcache.hve dosyası “C:\Windows\AppCompat\Programs\Amcache.hve” konumunda bulunmaktadır. Amcache.hve, başka bir Eric Zimmerman aracı olan AmcacheParser.exe ile parse edilir.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\User\Desktop\toolbag> .\AmcacheParser.exe
Option '-f' is required.
Option '--csv' is required.

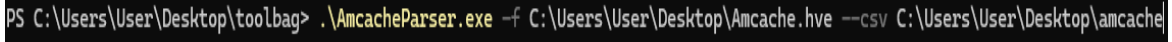
Description:
  AmcacheParser version 1.5.1.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/AmcacheParser

Examples: AmcacheParser.exe -f "C:\Temp\amcache\AmcacheWin10.hve" --csv C:\temp
          AmcacheParser.exe -f "C:\Temp\amcache\AmcacheWin10.hve" -i --csv C:\temp --csvf foo.csv
          AmcacheParser.exe -f "C:\Temp\amcache\AmcacheWin10.hve" -w "c:\temp\whitelist.txt" --csv C:\temp

Short options (single letter) are prefixed with a single dash. Long commands are prefixed with two dashes
```

Şekil 11.1 : AmcacheParser.exe örnek sentaks yapısı



```
PS C:\Users\User\Desktop\toolbag> .\AmcacheParser.exe -f C:\Users\User\Desktop\Amcache.hve --csv C:\Users\User\Desktop\amcache
```

Şekil 11.2 : Amcache.hve dosyasını parse etme işlemi

Elde edilen sonuç bir .csv dosyası olduğu için analiz aşamasında Timeline Explorer aracına başvurulur.

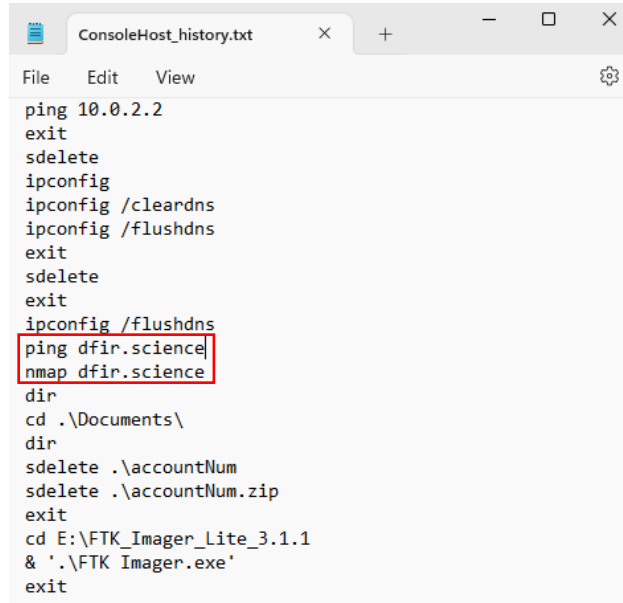
Timeline Explorer v2.0.0.1	
File Tools Tabs View Help	
20241207045636_Amcache_UnassociatedFileEntries.csv	
Drag a column header here to group by that column	
Enter text to search... Find	
	Name
files (x86)\google\update\1.3.36.82\googleupdatebroker.exe	GoogleUpdateBroker.exe
files (x86)\google\update\1.3.36.82\googleupdatecomregistershell64.exe	GoogleUpdateComRegisterShell6...
files (x86)\google\update\1.3.36.82\googleupdatecore.exe	GoogleUpdateCore.exe
files (x86)\google\update\1.3.36.82\googleupdateondemand.exe	GoogleUpdateOnDemand.exe
files (x86)\google\update\1.3.36.82\googleupdatesetup.exe	GoogleUpdateSetup.exe
hn doe\downloads\ipscan-3.7.6-setup.exe	ipscan-3.7.6-setup.exe
files (x86)\microsoft\edgeupdate\1.3.143.45\microsoftedgeupdatecomregistershellarm64.exe	MicrosoftEdgeComRegisterShell...
files (x86)\microsoft\edgeupdate\1.3.143.45\microsoftedgeupdateondemand.exe	MicrosoftEdgeUpdateOnDemand.e...
files (x86)\microsoft\edgeupdate\1.3.143.45\microsoftedgeupdatesetup.exe	MicrosoftEdgeUpdateSetup.exe
files (x86)\microsoft\edgeupdate\1.3.143.45\microsoftedgeupdatecore.exe	MicrosoftEdgeUpdateCore.exe
files (x86)\microsoft\edgeupdate\1.3.143.45\microsoftedgeupdatecomregistershell64.exe	MicrosoftEdgeUpdateComRegiste...
files (x86)\microsoft\edgeupdate\download\{f3c4fe00-efd5-403b-9569-398a20f1ba4a}\1.3.143.45\microsofte...	MicrosoftEdgeUpdateSetup_X86_...
files (x86)\microsoft\edgeupdate\1.3.143.45\microsoftedgeupdate.exe	MicrosoftEdgeUpdate.exe
files (x86)\microsoft\edgeupdate\microsoftedgeupdate.exe	MicrosoftEdgeUpdate.exe
files (x86)\microsoft\edgeupdate\1.3.143.45\microsoftedgeupdatebroker.exe	MicrosoftEdgeUpdateBroker.exe
files (x86)\microsoft\edgeupdate\download\{56eb18f8-b008-4cbd-b6d2-8c97fe7e9062}\85.0.564.67\microsofte...	MicrosoftEdge_X64_85.0.564.67...
ata\microsoft\windows defender\platform\4.18.2103.7-0\msmpeng.exe	MsMpEng.exe
ata\microsoft\windows defender\platform\4.18.2103.7-0\nissrv.exe	NisSrv.exe
hn doe\downloads\nmap-7.91-setup.exe	nmap-7.91-setup.exe

Şekil 11.3 : Amcache.hve dosyası çıktıları

Port taraması yapabilecek olan 2 uygulama göze çarpıyor. ipscan-3.7.6-setup.exe'nin, Angry IP Scanner programının kurulum dosyası olduğu görünüyor. Sistemde Angry IP Scanner ile ilgili herhangi bir log olmadığı için şüpheli diğer exe'yi inceliyoruz.

nmap-7.91-setup.exe'nin Nmap programına ait bir kurulum dosyası olduğunu anlıyoruz. Nmap, ağ tarama ve zafiyet tespiti için kullanılan açık kaynaklı bir araçtır. Nmap üzerinde bulunan modüller sayesinde port taraması, servis keşfi, versiyon ve işletim sistemi tespiti gerçekleştirilebilir.

Nmap, cmd/PowerShell vasıtasıyla kullanılan bir araç olduğu için şüphelinin sistemindeki konsol geçmişi bilgilerini “\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline” dizininde yer alan ConsoleHost_history.txt dosyasından elde ediyoruz.



```
ping 10.0.2.2
exit
sdelete
ipconfig
ipconfig /cleardns
ipconfig /flushdns
exit
sdelete
exit
ipconfig /flushdns
ping dfir.science
nmap dfir.science
dir
cd .\Documents\
dir
sdelete .\accountNum
sdelete .\accountNum.zip
exit
cd E:\FTK_Imager_Lite_3.1.1
& '.\FTK Imager.exe'
exit
```

Şekil 11.4 : Konsolda çalıştırılan komutlar

ConsoleHost_history.txt dosyasını incelediğimizde şüphelinin dfir.science sitesine Nmap aracılığıyla port taraması yapıldığını görüyoruz.

Cevap: dfir.science

3.9 Soru 9

20210429_151535.jpg” resmi, onu oluşturan orijinal cihazda hangi klasördeydi?

.jpg uzantılı resim dosyasının, oluşturulduğu yani fotoğrafın çekildiği zamanı bulmamız gerekiyor. Fotoğrafın çekildiği cihaz sisteme USB disk veya sürücüler gibi çıkarılabilir aygıtlarla bağlandıysa dosya izinleri hakkındaki bilgiler kaydedilir. Bu kayıtları tutan ise Shellbag artifactidir. Shellbag’i incelemeden önce UsrClass registry dosyasını açıklamakta fayda var.

3.9.1 UsrClass

UsrClass.dat, Microsoft Windows işletim sistemlerinde bulunan bir kayıt defteri (registry) dosyasıdır ve her kullanıcı için bireysel olarak saklanır. Kullanıcı profiline özgü bazı uygulama ve sistem yapılandırma bilgilerini depolar. Özellikle, Windows Shell ve Kullanıcı Arabirimi ile ilgili ayarları içerir.

UsrClass.dat dosyası, kullanıcının masaüstü görünümü, Dosya Gezgini (File Explorer) ayarları, ShellBag bilgileri ve uygulama ilişkilendirmeleri gibi kullanıcıya özel yapılandırma verilerini içerir

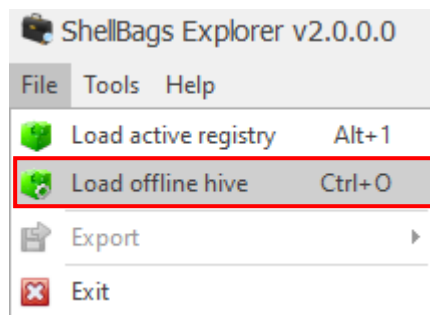
UsrClass.dat dosyası, her kullanıcının profil dizininde aşağıdaki konumda bulunur:

- C:\Users\<KullanıcıAdı>\AppData\Local\Microsoft\Windows\UsrClass.dat

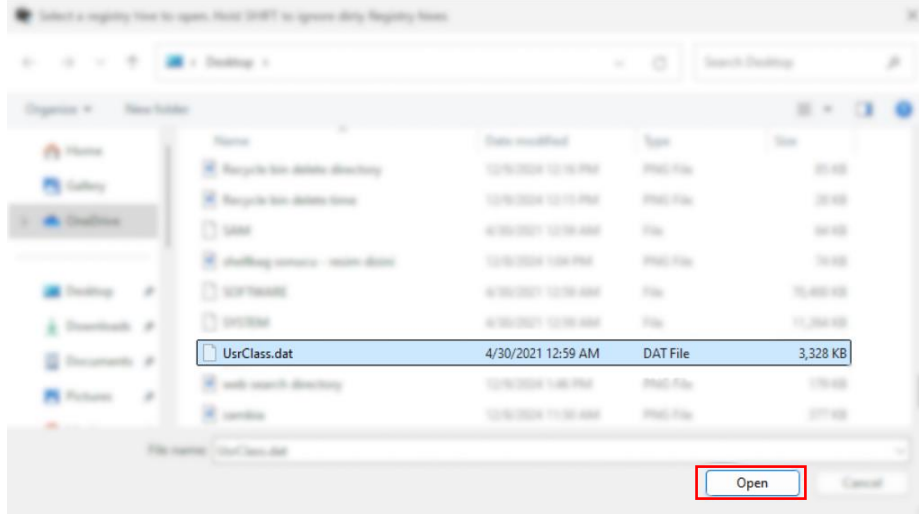
Gizli bir sistem dosyası olduğundan, görünür yapmak için "Gizli dosyaları göster" ayarı etkinleştirilmelidir.

3.9.2 Shellbag

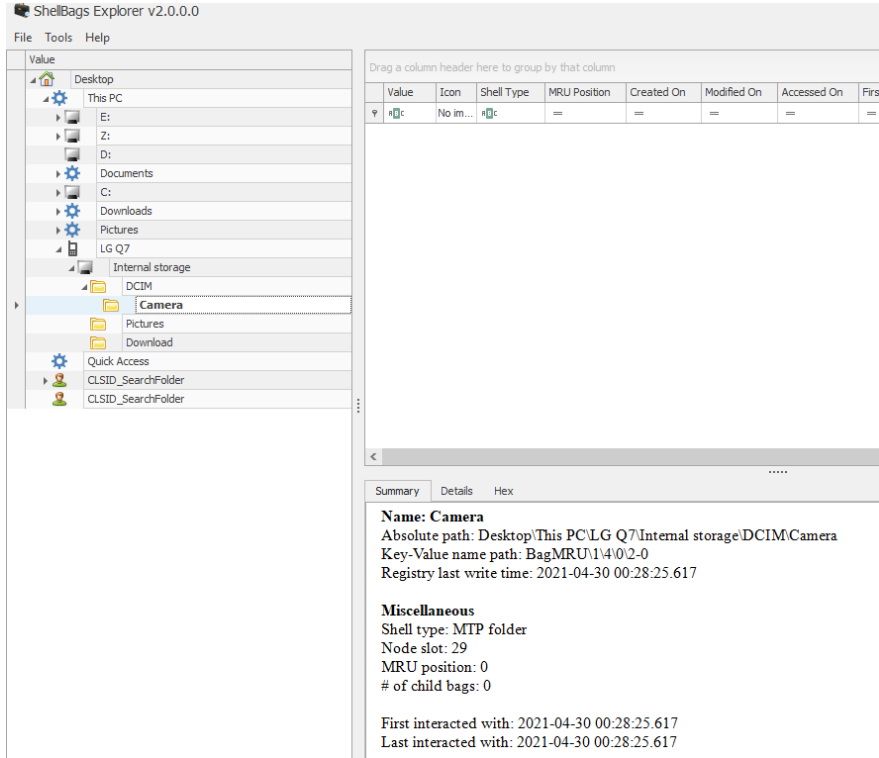
Microsoft Windows Explorer aracılığıyla, görüntülediğinde bir klasör penceresinin görünümünü, boyutlarını ve konumlarını izlemeye yardımcı olur buna ağ klasörleri ve çıkarılabilir cihazlar dahildir. Yani Windows ekranını başka bir yere taşıdığımızda, boyutunu değiştirdiğimizde, içindeki dosya sıralamasını yaptıktan sonra bir daha hatırlamasında Shellbag yardımcı olur. Shellbag analizi sayesinde, silinmiş klasörlerin bilgisini bulabiliriz. Kullanıcının hangi klasörle eriştiği bilgisine ve klasörlere ait zaman damgalarının bilgisine ulaşabiliriz. Shellbag analizi için Eric Zimmerman aracı ShellBags Explorer kullanılmaktadır.



Şekil 12.1 : Registry kaydı seçimi



Şekil 12.2 : UsrClass.dat dosyası seçimi



Şekil 12.3 : Mobil cihaza ait Shellbag bilgileri

Shellbag artifactini incelerken sisteme daha önce bağlanmış olan bir mobil cihaz görüyoruz. Cihazın depolama bilgilerini incelediğimizde fotoğrafın çekildiğinde oluşan asıl dizinin “LG Q7\Internal storage\DCIM\Camera” olduğunu görüyoruz.

Cevap: LG Q7\Internal storage\DCIM\Camera

3.10 Soru 10

Şüpheli hesap için Windows parola hashleri aşağıdadır. Kullanıcının parolası nedir?

John Doe

1001:aad3b435b51404eeaad3b435b51404ee:3DE1A36F6DDB8E036DFD75E8E20C4AF4 :::

Araştırmalar bu verinin bir NTLM hashi olduğu bilgisini veriyor. NTLM bir kimlik doğrulama protokölüdür ve yetkili kullanıcıların kaynağa erişmesini sağlar. NTLM hakkında kısa bir açıklama yapalım.

3.10.1 NTLM

NTLM (New Technology LAN Manager), sınaama-yanıt (challenge-response) yapısını kullanarak şifrelenmemiş kullanıcı adı parola bilgisi yerine Windows kimlik bilgileri ile doğrulamayı gerçekleştirir. Etki alanı adı, kullanıcı adı ve kullanıcının parolasının tek yönlü bir özeti NTLM kimlik bilgilerini oluşturur.

- LM hashi küçük/büyük harfe duyarlı değildir, NT hashi ise küçük/büyük harfe duyarlıdır.
- NT hashi, hashi kullanıcının girdiği tüm parolaya göre hesaplar. LM hashi, parolayı gerektiği gibi doldurarak iki 7 karakterlik parçaya böler.

Soruda yer alan NTLM hashine bakarsak:

- John Doe kullanıcı adını,
- 1001 göreceli tanımlayıcıyı,
- aad3b435b51404eeaad3b435b51404ee LM hashini,
- 3DE1A36F6DDB8E036DFD75E8E20C4AF4 NT hashini ifade etmektedir.

NT hashi kullanıcının girdiği tüm parolaya göre hesaplama yaptığı için NT hashi üzerinden ilerleyeceğiz. NTLM hashini “hashcat” isimli parola kırma aracı ile işleyeceğiz.

Hashcat kullanarak bir parolayı kırmak için genel sentaks yapısı şöyledir:

- `$ hashcat -m <değer> -a <değer> <veri> <kelime listesi> -r <kural dosyası>`

-m parametresi hash türünü belirtmek için kullanılır, -a parametresi saldırı modunu belirtmek içindir, -r parametresi kelime listelerindeki her kelimeye birden fazla kural uygulanacağını belirtir. -a (atak modu) parametresinin alabileceği değerler aşağıdaki gibidir:

- 0 | Straight | Düz
- 1 | Combination | Kombinasyon
- 3 | Brute-force | Kaba kuvvet
- 6 | Hybrid Wordlist + Mask | Hibrit Kelime Listesi + Maske
- 7 | Hybrid Mask + Wordlist | Hibrit Maske + Kelime Listesi
- 9 | Association | Birleşik

<https://hashcat.net/wiki/doku.php?id=hashcat> sitesi üzerinden NTLM hash türü değerini 1000 olarak bulduk. Hash türünü (-m) 1000 olarak giriyoruz. Atak modunu (-a) 0 yani Straight olarak ayarlıyoruz. Kullanacağımız veri ise NTLM hashinin NT kısmı olacak. Bu değeri de 3DE1A36F6DDB8E036DFD75E8E20C4AF4 olarak giriyoruz. Kullanılacak kelime listesini rockyou.txt olarak seçiyoruz. Kural dosyasını (-r) OneRuleToRuleThemAll olarak ayarlıyoruz.

12800		MS-AzureSync PBKDF2-HMAC-SHA256
12400		BSDi Crypt, Extended DES
1000		NTLM
9900		Radmin2
5800		Samsung Android Password/PIN

Şekil 13.1: Hashcat hash tipleri kodları

```
$ hashcat -m 1000 -a 0 3De1A36F6DDB8E036DFD75E8E20C4AF4 /usr/share/wordlists/rockyou.txt -r OneRuleToRuleThemAll.rule
hashcat (v6.1.1) starting...
```

Şekil 13.2 : Hashcat için kullanılan komut

```
3de1a36f6ddb8e036dfd75e8e20c4af4 AFR1CA!  
Session.....: hashcat  
Status.....: Cracked  
Hash.Name.....: NTLM  
Hash.Target.....: 3de1a36f6ddb8e036dfd75e8e20c4af4
```

Şekil 13.3: Hash kırma işlemi sonucu

Cevap: AFR1CA!

3.11 Soru 11

"John Doe" adlı kullanıcının Windows oturum açma şifresi nedir?

Kullanıcının oturum açma şifresini elde etmek için önce local kullanıcı bilgilerini elde etmemiz gerekiyor. Bunun için de Kali Linux üzerinden creddump7 isimli aracı kullanacağız. creddump, Windows registry kayıtlarından çeşitli kimlik bilgilerini çıkarmak için kullanılan bir Python aracıdır.

Local parola hashlerinin dökümünü elde etmek için:

- ./pwdump.py <SYSTEM registry> <SAM registry> komutunu kullanıyoruz.

SYSTEM ve SAM registry kayıtları ne amaçla kullanılır kısa bir inceleme yapalım.

3.11.1 SYSTEM

Windows işletim sisteminde SYSTEM registry kaydı, sistemin donanım ve yazılım yapılandırmalarıyla ilgili kritik bilgileri depolayan bir bölümdür. Bu kayıt, özellikle sistem başlatma işlemleri sırasında kullanılan ayarları içerir ve işletim sisteminin stabil çalışması için hayati öneme sahiptir.

- Aktif olarak kullanılan yapılandırma ayarlarını içerir.
- Yüklü hizmetler ve sürücülerle ilgili bilgileri barındırır.
- Farklı donanım profillerinin ayarlarını içerir.

- Takılı sürücülerin ve depolama cihazlarının bilgilerini içerir; sürücü harfleri ve bu sürücülerin fiziksel adresleri gibi.

3.11.2 SAM

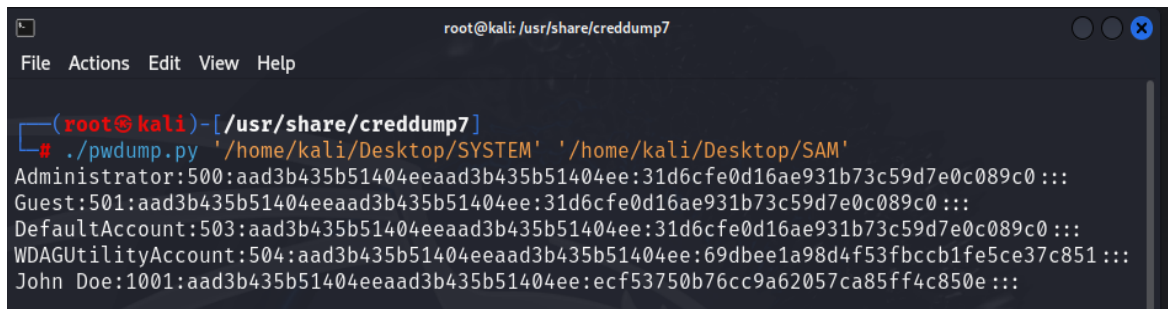
SAM (Security Account Manager) registry girdisi, Windows işletim sisteminde kullanıcı hesapları ve kimlik doğrulama bilgilerini depolayan kritik bir bileşendir. Bu kayıt, kullanıcı adları, parola özetleri ve kullanıcıların benzersiz Güvenlik Tanımlayıcıları (Security Identifier - SID) gibi bilgileri içerir.

SAM registry kaydı içeriği:

- Kullanıcı Hesapları: Sistemdeki tüm kullanıcıların hesap bilgileri, kullanıcı adları ve ilişkili SID'leriyle birlikte burada saklanır.
- Parola Özetleri: Kullanıcıların şifreleri, doğrudan düz metin olarak değil, özetlenmiş (hashlenmiş) biçimde depolanır. Bu, şifrelerin güvenliğini artırmak için kullanılan bir yöntemdir.
- Grup Bilgileri: Kullanıcıların ait olduğu gruplar ve bu grupların izinleri gibi bilgiler de SAM kaydında bulunur.

Kullanıcıların kimlik bilgilerini NTLM hash formatında bize çıktı olarak sunuyor:

- John Doe:
- 1001:
- aad3b435b51404eeaad3b435b51404ee:ecf53750b76cc9a62057ca85ff4c850e:::



```

root@kali: /usr/share/creddump7
File Actions Edit View Help

(root@kali)-[/usr/share/creddump7]
# ./pwdump.py '/home/kali/Desktop/SYSTEM' '/home/kali/Desktop/SAM'
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:69dbee1a98d4f53fbccb1fe5ce37c851:::
John Doe:1001:aad3b435b51404eeaad3b435b51404ee:ecf53750b76cc9a62057ca85ff4c850e:::

```

Şekil 14.1: SYSTEM ve SAM kayıtlarının işlenmesi

Hash türünü NTLM olarak bulmuştuk. NTLM için hash türü (-m) 1000 ile ifade edilir. Atak modunu (-a) 0 yani Straight olarak ayarlıyoruz. Kullanacağımız veri ise NTLM hashinin NT kısmı olacak. Bu değeri de ecf53750b76cc9a62057ca85ff4c850e olarak giriyoruz. Kullanılacak kelime listesini rockyou.txt olarak seçiyoruz. Kural dosyasını (-r) OneRuleToRuleThemAll olarak ayarlıyoruz.

```
hashcat -m 1000 -a 0 ecf53750b76cc9a62057ca85ff4c850e /usr/share/wordlists/rockyou.txt -r OneRuleToRuleThemAll.rule
hashcat (v6.1.1) starting...
```

Şekil 14.2: NT hashinin girilmesi

```
ecf53750b76cc9a62057ca85ff4c850e ctf2021
Session.....: hashcat
Status.....: Cracked
Hash.Name.....: NTLM
Hash.Target.....: ecf53750b76cc9a62057ca85ff4c850e
```

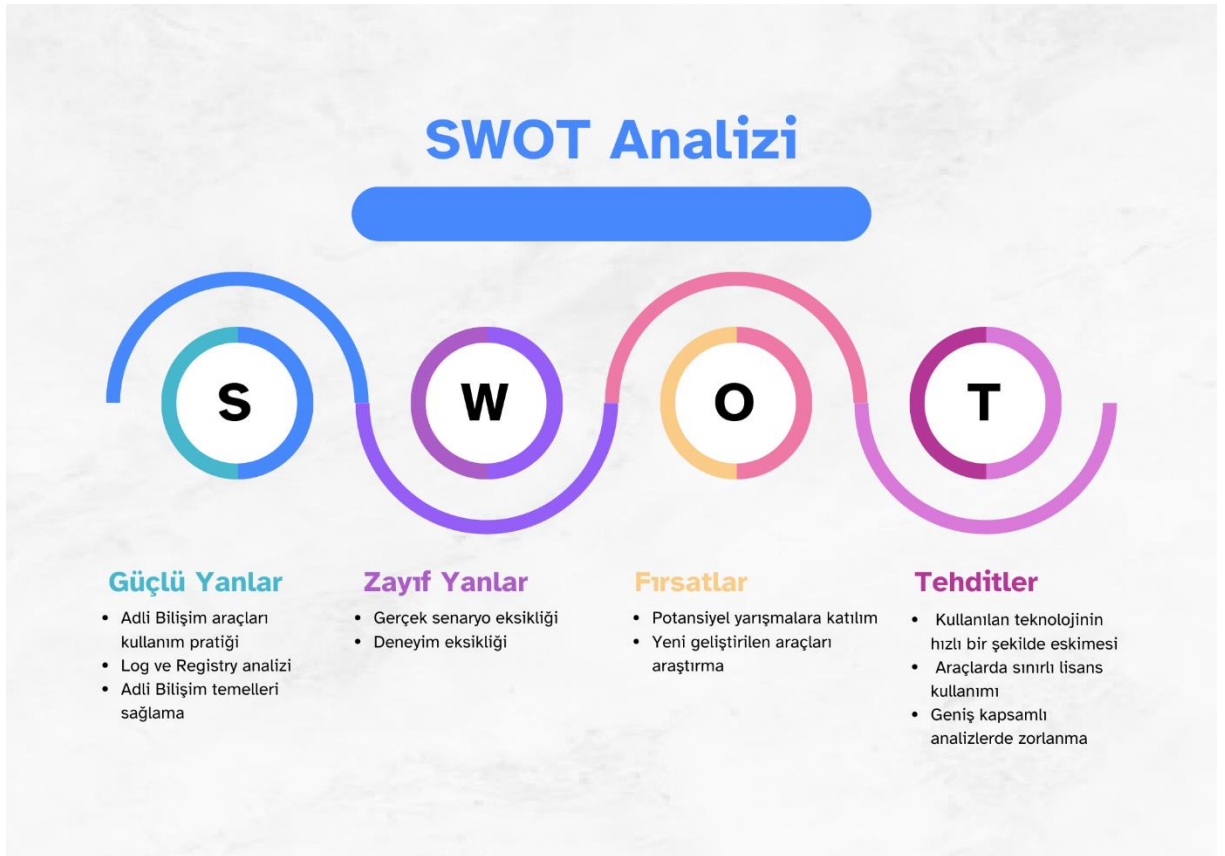
Şekil 14.3: NT hashi çıktısı

Parola kırma işlemi sonucunda çıktıyı elde ediyoruz.

Cevap: ctf2021

4. DEĞERLENDİRME

Bu çalışma Adli Bilişim alanındaki teknik becerilerinizi geliştirmek adına oldukça faydalı bir deneyim sunmaktadır. Bir CTF yarışması kapsamında değerlendirilen vaka gerçek hayat senaryosuna yakın olmasa da kullanılan araçlar, dijital suçun izlerini sürme ve dijital kanıtları inceleme konusunda derinlemesine bilgi edinmeye olanak sağlar. Bu çalışma, Adli Bilişim araçlarını kullanarak dijital kanıtları elde etme ve olayları analiz etme yetenekleri geliştirmektedir. Ayrıca, her bir aracın sağladığı veri türlerini ve analiz yöntemlerini öğrenerek, dijital dünyadaki potansiyel suç unsurlarını tespit etme ve izleme konusunda şüpheli bir anlayış kazandırmaktadır. Adli Bilişim alanındaki bu pratik, bu alandaki profesyonel yetkinliği artırarak, gerçek vaka analizlerinde daha hızlı ve etkin olmayı sağlayacaktır.



Şekil 15.1: SWOT Analizi

Soruları ve elde edilen cevapları Siber Güvenlik açısından değerlendirecek olursak dijital sistemlerde, ağ güvenliği ve kullanıcı kimlik doğrulama mekanizmalarının iyileştirilmesi gerektiğini göstermektedir. Şüphelinin Nmap gibi araçlarla ağdaki güvenlik açıklarını taraması, NTLM hash'leri gibi eski ve zayıf güvenlik protokollerinin kullanılması, sistemlerin güvenliğini büyük ölçüde tehdit etmektedir. Güvenliği artırmak için, daha güçlü şifreleme algoritmalarına, güvenli parolalara ve modern doğrulama yöntemlerine geçilmesi gerekmektedir. Ayrıca, ağda tespit edilen açıklar derhal kapatılmalı ve şüpheli aktiviteler izlenmelidir.

KAYNAKLAR

- [1]. **AdShotGyan.** (2012, Şubat). LM hash and NT hash. AdShotGyan.<http://www.adshotgyan.com/2012/02/lm-hash-and-nt-hash.html>
- [2]. **Allianz Sigorta.** (n.d.). SWOT analizi nedir? Allianz Sigorta. Erişim adresi: https://www.allianz.com.tr/tr_TR/seninle-guzel/swot-analizi-nedir.html?
- [3]. **Aygün, M.** (2022, Temmuz 13). Shellbag analizi. Muhammed Aygün. <https://www.muhammedaygun.com/2022/07/13/shellbag-analizi/>
- [4]. **Bircan, M.** (n.d.). Amcache.hve dosyası nedir? Nasıl analiz edilir?. LinkedIn. <https://www.linkedin.com/pulse/amcachehve-dosyas%C4%B1-nedir-nas%C4%B1-analiz-edilir-mustafa-bircan/>
- [5]. **BeyazNet.** (n.d.). Nmap nedir ve nasıl kullanılır?. BeyazNet. https://www.beyaz.net/tr/guvenlik/makaleler/nmap_nedir_ve_nasil_kullanilir.html
- [6]. **Canva.** (n.d.). Gantt şeması oluşturma aracı: Online ve ücretsiz. Canva. Erişim adresi: https://www.canva.com/tr_tr/sema/gantt-semasi/
- [7]. **Cloudyflex.** (n.d.). Gantt şeması nedir, nasıl oluşturulur? Cloudyflex. Erişim adresi: <https://www.cloudyflex.com/blogs/post/gantt-semasi-nedir-nasil-olusturulur>
- [8]. **CyberArtsPro.** (n.d.). Adli bilişim açısından en önemli Windows kayıt dosyaları. CyberArtsPro. <https://cyberartspro.com/adli-bilisim-acisindan-en-onemli-windows-kayit-dosyalari/>
- [9]. **DarkCybe.** (n.d.). DFIR tools execution: PECmd. GitHub Pages. https://darkcybe.github.io/posts/DFIR_Tools_Execution_PeCmd/
- [10]. **ExifTool.** (n.d.). ExifTool. Wikipedia. <https://en.wikipedia.org/wiki/ExifTool>
- [11]. **FileZilla Project.** (n.d.). Logs. FileZilla Wiki. <https://wiki.filezilla-project.org/Logs>
- [12]. **Forensafe.** (n.d.). Installed programs in Windows forensics. Forensafe Blog. <https://www.forensafe.com/blogs/installedprograms.html>
- [13]. **FreeCodeCamp.** (n.d.). Hacking with Hashcat: A practical guide. FreeCodeCamp. <https://www.freecodecamp.org/news/hacking-with-hashcat-a-practical-guide/>
- [14]. **Henkoğlu, T.** (2020). *Adli bilişim: Dijital delillerin elde edilmesi ve analizi*. Pusula.
- [15]. **Mandine, L.** (2021, Temmuz 15). Browser forensics. Medium. <https://medium.com/@laurent.mandine/browser-forensics-89429fe0749f>

- [16]. **Microsoft.** (n.d.). Windows registry. Microsoft Learn. <https://learn.microsoft.com/en-us/windows/win32/sysinfo/registry>
- [17]. **Microsoft.** (n.d.). Windows registry for advanced users. Microsoft Learn. <https://learn.microsoft.com/tr-tr/troubleshoot/windows-server/performance/windows-registry-advanced-users?>
- [18]. **Mochatouch.** (n.d.). SWOT analizi nedir? Mochatouch. Erişim adresi: <https://mochatouch.com.tr/blog/swot-analizi/>
- [19]. **Mynl, N.** (2021, Ocak 13). Prefetch analysis. Medium. <https://nursevimynl.medium.com/prefetch-analysis-bf54cd0c021b>
- [20]. **Stack Exchange.** (n.d.). Understanding Windows local password hashes (NTLM). Security Stack Exchange. <https://security.stackexchange.com/questions/161889/understanding-windows-local-password-hashes-ntlm>
- [21]. **Thismanera.** (2021, Aralık 12). Windows Recycle Bin forensics. Medium. <https://medium.com/@thismanera/windows-recycle-bin-forensics-a2998c9a4d3e>
- [22]. **Ünal, O.** (2021, Şubat 10). Registry forensics – Bölüm 1: Registry yapısı. Medium. <https://medium.com/@ozan.unal/registry-forensics-b%C3%B6l%C3%BCm-1-registry-yap%C4%B1s%C4%B1-24d609eff1f3>