TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

MACOS İŞLETİM SİSTEMİNE SAHİP BİLGİSAYARLAR ÜZERİNDE ADLİ BİLİŞİM AÇISINDAN ÖNEM ARZ EDEN KAYITLARIN İNCELENMESİ

Tümay KURTCA

DİSİPLİNLERARASI ADLİ BİLİMLER ANABİLİM DALI
ADLİ BİLİŞİM
YÜKSEK LİSANS TEZİ

DANIŞMAN
Prof. Dr. Refik SAMET

ANKARA
2021

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

MACOS İŞLETİM SİSTEMİNE SAHİP BİLGİSAYARLAR ÜZERİNDE ADLİ BİLİŞİM AÇISINDAN ÖNEM ARZ EDEN KAYITLARIN İNCELENMESİ

Tümay KURTCA

DİSİPLİNLERARASI ADLİ BİLİMLER ANABİLİM DALI
ADLİ BİLİŞİM
YÜKSEK LİSANS TEZİ

DANIŞMAN
Prof. Dr. Refik SAMET

ANKARA
2021

Ankara Üniversitesi
Sağlık Bilimleri Enstitüsü Müdürlüğü'ne,

Yüksek Lisans tezi olarak hazırlayıp sunduğum "MacOS İşletim Sistemine Sahip Bilgisayarlar Üzerinde Adli Bilişim Açısından Önem Arz Eden Kayıtların İncelenmesi" başlıklı tez; bilimsel ahlak ve değerlere uygun olarak tarafımdan yazılmıştır. Tezimin fikir/hipotezi tümüyle tez danışmanım ve bana aittir. Tezde yer alan deneysel çalışma/araştırma tarafımdan yapılmış olup, tüm cümleler, yorumlar bana aittir.
Yukarıda belirtilen hususların doğruluğunu beyan ederim.

Öğrencinin Adı Soyadı : Tümay KURTCA
Tarih : 26.01.2021
İmza:

İÇİNDEKİLER

Etik Beyan ii

Kabul ve Onay iii

İçindekiler iv

Önsöz vi

Simgeler ve Kısaltmalar vii

Şekiller viii

Çizelgeler xi

1. GİRİŞ 1

1.1. Kavram ve Tanımlar 5

1.2. Mac İşletim Sistemi ve Versiyonları 9

2. GEREÇ VE YÖNTEM 11

2.1. Çalışma Ortamının Hazırlanması ve Gereçler 11

2.2. Verilerin Toplanması 12

2.2.1. Mac İşletim Sistemine Sahip Sanal Makinenin Kurulması 13

2.2.2. Mac İşletim Sistemine Sahip Sanal Makine Üzerinde Kullanıcıların Oluşturulması ve Kullanıcı Silinmesi 14

2.2.3. Mac İşletim Sistemi Üzerinde Kullanıcıların Giriş-Çıkış İşlemleri 14

2.2.4. Mac İşletim Sistemine Sahip Bilgisayarın Açma ve Kapama İşlemleri 14

2.2.5. Mac İşletim Sistemi Üzerinde Kullanıcı Tarafından Yapılan Tarih ve Saat Değişikliği İşlemleri 15

2.2.6. Sistem Güncelleme Bilgilerinin Tespiti 15

2.2.7. Ağ Yapılandırması, Ağ Üzerinden Erişim, Kablosuz Erişim Noktalarına Yapılan Bağlantı İşlemleri 15

2.2.8. Yazıcıdan Çıktı Alındıktan Sonra Oluşan Kayıtların Tespiti 17

2.2.9. Bilgisayara Takılan Harici Veri Depolama Cihazlarına Ait Kayıtların Tespiti 17

2.2.10. Bilgisayara Programların Yüklenmesi 17

2.2.11. MacBook Pro Bilgisayarın Filevault2 Özelliğini Aktif Etme 18

2.2.12. MacBook Pro Bilgisayar Üzerinden Şifre Tespitleri 18

2.3. Verilerin Analizi ve Sonuçların Değerlendirilmesi 19

3. BULGULAR 21
3.1. Mac İşletim Sistemi İle İlgili Kayıtların Analizi 21
3.2. Mevcut Kullanıcıya Ait Kayıtların Analizi 22
3.3. Silinen Kullanıcıya Ait Kayıtların Analizi 27
3.4. Kullanıcıların Giriş-Çıkış İşlemleri Sonucunda Oluşan Kayıtların Analizi 30
3.5. Mac İşletim Sistemine Sahip Bilgisayarın Açma ve Kapama İşlemleri 32
3.6. Mac İşletim Sistemi Üzerinde Kullanıcı Tarafından Yapılan Tarih ve Saat Değişikliği İşlemleri 33
3.7. Sistem Güncelleme Bilgilerinin Tespiti 34
3.8. Ağ Yapılandırması, Ağ Üzerinden Erişim, Kablosuz Erişim Noktalarına Yapılan Bağlantı İşlemleri 36
3.8.1. iOS uygulama 1 36
3.8.2. iOS uygulama 2 38
3.8.3. iOS uygulama 3 39
3.8.4. iOS uygulama 4 40
3.8.5. iOS uygulama 5 41
3.8.6. Yazıcı ile Yapılan Uygulama 43
3.9. Yazıcıdan Çıktı Alınması 45
3.10. Bilgisayara Takılan Harici Veri Depolama Cihazlarına Ait Kayıtların Tespiti 48
3.11. Bilgisayara Programların Yüklenmesi 51
3.12. MacBook Pro Bilgisayarın FileVault2 Özelliğini Aktif Etme 52
3.13. MacBook Pro Bilgisayar Üzerinden Şifre Tespitleri 58

4. TARTIŞMA 62
5. SONUÇ VE ÖNERİLER 65
ÖZET 69
SUMMARY 70
KAYNAKLAR 71
ÖZGEÇMİŞ 74

ÖNSÖZ

İşletim sistemlerinin sürekli gelişimine karşın adli bilişim yazılımlarının ilerlemesi, Mac işletim sistemi açısından yeteriz kalmaktadır. Aynı zamanda Mac işletim sisteminin güvenlik kısıtlamaları ve kendine özgü yapısından dolayı diğer işletim sistemleri ile karşılaştırıldığında adli analizinin daha zor olduğu görülmüştür. Yapılan bu çalışma ile tespit edilen kayıtlar ve incelemeler sırasında karşılaşılan problemlere sunulan çözümler sonucunda, Mac işletim sisteminin adli bilişim açısından incelenmesi konusunda metodoloji oluşturması ve inceleme süresinin kısaltılması hedeflenmiştir.

Bilgisini ve azmini örnek aldığım danışman hocam, Prof. Dr. Refik SAMET'e, bu çalışmanın hazırlanması aşamasında her türlü desteğini benden esirgemeyen aileme teşekkür eder, bu alana yönelmeme sebep olan Jandarma Kriminal Daire Başkanlığı, Bilişim Teknolojileri İnceleme Şube Müdürlüğüne, bu tez çalışmasını atfederim.

SİMGELER VE KISALTMALAR

APFS	Apple Dosya Sistemi (Apple File System)
App Store	Apple Uygulama Marketi (Apple Store Market)
ASL	Apple Sistem Günlüğü (Apple System Log)
CUPS	Genel UNIX Yazdırma Sistemi (Common UNIX Printing System)
HFS/HFS+	Hiyerarşik Dosya Sistemi (Hierarchical File System)
IOS	iPhone İşletim Sistemi (iPhone Operating System)
MDS	Meta Veri Sunucusu(Meta Data Server)
MFS	Macintosh Dosya Sistemi (Machintosh File System)
PBKDF2	Parola Tabanlı Anahtar Türetme Fonksiyonu (Password Based Key Derivation Functions)
RAM	Rastgele Erişimli Hafıza (Random Access Memory)
SHA	Güvenlik Hashing Algortiması (Secure Hashing Algorithm)
UTC	Eşgüdümlü Evrensel Zaman (Coordinated Universal Time)
Wi-Fi	Kablosuz Bağlantı Alanı (Wireless Fidelity)
XTS-AES	"Tweakable narrow-block encryption" Modu Kullanan Gelişmiş Şifreleme Standardı

ŞEKİLLER

Şekil 1.1. FileVault ayarını etkinleştirme-1 7
Şekil 1.2. FileVault ayarını etkinleştirme-2 8
Şekil 1.3. FileVault ayarını etkinleştirme-3 8
Şekil 3.1. İşletim sistemi versiyon bilgileri 21
Şekil 3.2. Bilgisayar adı bilgisi 22
Şekil 3.3. "AppleSetupDone" dosyasının oluşma zamanı 22
Şekil 3.4. Ana kullanıcı klasörlerine ait görüntü 23
Şekil 3.5. Kullanıcılara ait ".plist" dosyaları 24
Şekil 3.6. Kullanıcıya ait ".plist" dosyasının incelenmesi 24
Şekil 3.7. AXIOM yazılımı "apple kişiler" görünümü 25
Şekil 3.8. Kullanıcı oluşturma tarihinin hesaplanması 26
Şekil 3.9. Kullanıcılara ait UUID adında oluşan klasörler 26
Şekil 3.10. Kullanıcı silindikten sonra kullanıcı ait ana dizin klasörleri 28
Şekil 3.11. "com.apple.preferences.accounts.plist" dosyasının oluşma tarihi 28
Şekil 3.12. Silinen kullanıcıya ait kayıtlar 29
Şekil 3.13. Kullanıcı silindikten sonra oluşan audit log dosyası 29
Şekil 3.14. Audit log dosyası içerisinde silinen kullanıcıya ait kayıtlar 29
Şekil 3.15. Yonetici isimli kullanıcının oturum açma-kapama zaman bilgileri 30
Şekil 3.16. Tespit edilen oturum açma-kapama zaman bilgileri 31
Şekil 3.17. Bilgisayarın açma ve kapama zaman bilgileri 32
Şekil 3.18. Tespit edilen bilgisayar açma-kapama zaman bilgileri 32
Şekil 3.19. Zaman değişikliği ile ilgili kayıtlar 34
Şekil 3.20. Yüklenecek olan "MacOS Mojave-10.14.3" sürümünün indirilme zaman bilgisi 35
Şekil 3.21. Güncelleme işleminin yapıldığı zaman bilgisi 35
Şekil 3.22. Güncelleme yapılmadan önceki versiyon sürümü ve güncelleme yapıldıktan sonraki versiyon sürümleri bilgisi 35
Şekil 3.23. "com.apple.airport.preferences.plist" dosyası-1 37
Şekil 3.24. "netusage.sqlite" dosyasının görünümü-1 37

Şekil 3.25. Ağ arayüzleri yapı görüntüsü-1 37
Şekil 3.26. Ağ arayüzleri yapı görüntüsü-2 38
Şekil 3.27. "NetworkInterfaces.plist" dosyası-1 39
Şekil 3.28. "netusage.sqlite" dosyasının görünümü-2 40
Şekil 3.29. Ağ arayüzleri yapı görüntüsü-3 41
Şekil 3.30. "NetworkInterfaces.plist" dosyası-2 42
Şekil 3.31." Wi-Fi ile bağlanılan yazıcı için elde edilen bilgiler 44
Şekil 3.32. "netusage.sqlite" dosyasının görünümü-3 45
Şekil 3.33. "c00001" kontrol dosyasından elde edilen bilgiler-1 46
Şekil 3.34. "c00001" kontrol dosyasından elde edilen bilgiler-2 47
Şekil 3.35. Mac_apt.exe yazılımının çalıştırılması 47
Şekil 3.36. Mac_apt.exe'nin çalıştırılması sonucu PRINTJOBS klasörü altında oluşan dosyalar ve yazdırılan dosyanın ham hali 48
Şekil 3.37. Toshiba marka USB'ye ait tespit edilen bilgiler 49
Şekil 3.38. İnternet isimli USB üzerinden erişilen dosya adı bilgisi 49
Şekil 3.39. Takılan USB belleklerin isim bilgileri 50
Şekil 3.40. Yazdırılan CD'nin isim bilgisi 50
Şekil 3.41. Uygulama mağazası üzerinden yüklenen programlara ait bilgiler 51
Şekil 3.42. Terminal üzerinden yüklenen programlara ait bilgiler 51
Şekil 3.43. FileVault 2 İle şifreleme olduğuna dair uyarı 52
Şekil 3.44. Apfs Container'a sahip mac bilgisayarın Blackbag Macquisition ile boot edildikten sonraki arayüz görünümü 53
Şekil 3.45. CoreStorage mantıksal birime sahip mac bilgisayar için kullanıcı şifresi girildikten sonraki macquisition arayüz görünümü 53
Şekil 3.46. AXIOM yazılımı tarafından FileVault şifreleme olduğuna dair görüntü 54
Şekil 3.47. AXIOM yazılımı tarafından FileVault şifrelemesine dair destek 54
Şekil 3.48. FileVault şifrelemesi olan disk imajının X-Ways yazılımı ile görüntüsü 55
Şekil 3.49. Passware Password Recovery Kit yazılımının full disk encrypytion desteği 55
Şekil 3.50. Passware Password Recovery Kit yazılımının FileVault/APFS desteği 56
Şekil 3.51. Passware Password Recovery Kit yazılımının FileVault şifrelemesi olan disk imajının eklenmesi 56

Şekil 3.52. Passware Password Recovery Kit yazılımı ile imajın çözümlenmesi 57
Şekil 3.53. Çözümlenen imajın X-Ways yazılımına eklenmiş hali 57
Şekil 3.54. Dumpkeychain.exe'nin çalıştırılması 59
Şekil 3.55. Dumpkeychain.exe'nin çalıştırılması sonucu oluşan .txt uzantılı dosyada iTunes şifresi 59
Şekil 3.56. Chainbreaker.exe'nin arayüzü 60
Şekil 3.57. SystemKey dosyasından elde edilen key (anahtarı) değeri 60
Şekil 3.58. Tespit edilen ağ parolaları 61

ÇİZELGELER

Çizelge 3.1. Yapılan uygulamaların, veri toplama aşamasında elde edilen veriler 36
Çizelge 4.1. İnceleme yazılımının verdiği sonuç ve önerilen analiz yöntemi sonrası tespit edilen sonuçlar 63
Çizelge 5.1. Tespit edilen veriler 65

1. GİRİŞ

Bilgisayarlar üzerinde bulunan işletim sistemleri sürekli güncellenmekte ve gelişmektedir. Bununla birlikte güncel işletim sistemlerinde kullanıcının gerçekleştirdiği işlemlere ve geride bıraktığı izlere ait tespit edilebilecek adli bilişim açısından önem arz eden kayıtlar da artış göstermektedir. Bilgisayar sistemleri üzerinde yapılan her işlem, işletim sistemleri üzerinde iz bırakmaktadır. Adli bilişim incelemelerinde işletim sistemi kayıtlarının analizi, tüm analiz işlemlerinin sonuçları arasındaki bağlantıyı oluşturması açısından önemlidir (Henkoğu, 2011). Kullanıcının yapmış olduğu işlemler, kurulan programlara ait bilgiler ve işletim sisteminin tutmuş olduğu kayıtlar arasındaki tutarlılık, disk/dosya analizinde ulaşılan sonucu destekler nitelikte olmalıdır.

İnceleme talepleri de son yıllarda daha ayrıntılı, nitelikli ve zorlayıcı olmakta, talep ile ilgili bulgu tespiti için örnek deneyler yapılması gerekmektedir. Dünyada en çok tercih edilen adli bilişim yazılımları da bu doğrultuda kendini geliştirmekte ve uzman personele söz konusu kayıtları tespit etmede ve analiz etmede kolaylık sağlamaktadır. Ancak söz konusu adli bilişim yazılımları bu gelişimi daha çok Windows işletim sistemine sahip bilgisayarlar için göstermekte (Martin, 2016), Mac ve Linux işletim sistemine sahip bilgisayarlar için çok yetersiz kalmaktadır (Rathod, 2017a). Aynı zamanda Mac ve Windows'un kullanılan dosya sistemi ve teknolojisi farklı olduğundan, Windows işletim sistemi için geçerli olan dijital adli teknikler MacOS için geçerli değildir (Rathod, 2017a). Bu nedenle bu projede platform olarak MacOS seçilmiştir.

Çalışmanın ilk aşamasında yapılan literatür taraması sonucunda ise yapılan çalışmaların çoğunda adli bilişim ile ilgi bazı kayıtlar için sadece bu kayıtların dosya sistemindeki lokasyonlarına odaklandığı görülmüştür. Mac işletim sisteminin güvenlik kısıtlamaları ve kendine özgü yapısından dolayı diğer işletim sistemleri ile karşılaştırıldığında adli analizinin daha zor olduğu vurgulamıştır (Prasad ve ark, 2018). İncelemecilerin MacOS versiyonlarını anlaması ve kayıtların konumlarına

aşina olmalarının öneminden bahsetmişlerdir (Craiger ve Burke, 2006). HFS+ (Hiyerarşik Dosya Sistemi) dosyalama sisteminden (Burghardt ve Feldman, 2008), işletim sistemi üzerinde canlı olarak incelemelerden ve RAM (Rastgele erişimli hafıza) analizi ile elde edilebilecek verilerden bahsedilmiştir (Stamm, 2012). MacOS X için mevcut olan inceleme araçlarına alternatif olarak, MEGA isimli inceleme yazılımının geliştirildiği, sistem üzerinde canlı olarak da kullanılabileceği belirtilmiş, önceliklendirme (triyaj) metodunun hız kazandıracağından bahsedilmiş ve MEGA yazılımı ile önceliklendirme örneğine yer verilmiştir (Joyce ve ark., 2008). MacOS'un yeni dosyalama sistemi APFS'ye (Apple dosyalama sistemi) geçiş yapan güncel versiyonları üzerinde imaj üzerinden ve uygulamalı olarak bir çalışma yapılmadığı görülmüştür. MacOS'un El Capitan 10.11.2 ve Yosemite 10.10.5 versiyonlarında anımsatılan Wireless ağ geçmişi ile ilgili bilgilerin "com.apple.airport.preferences.plist" isimli dosyada bulunduğundan ve bu dosyanın lokasyonundan bahsedilmiştir (Cook ve Ark. 2015). Ağ trafiğinin incelenmesi için ağ arayüzleri ve MAC adreslerinin önemli olabileceği yine bu bilgilerin ise "NetworkInterfaces.plist" isimli dosyada tutulduğu belirtilmiştir (Reddy, 2019). "netusage.sqlite" isimli veritabanı dosyasında cihazın bağlandığı ağ ve zaman bilgileri bulunduğu ve bu veritabanın kaç tablodan oluştuğu gösterilmiştir (mac4n6, Erişim Tarihi:10.09.2019). "com.apple.network.identification.plist" isimli dosyada ise yine Wireless ağ geçmişini, servis seti tanımlayıcısını (service set identifier - SSID), zaman, güvenlik tipi gibi değerlerin kaydının tutulduğundan bahsedilmiştir (Rathod, 2017b). Ancak burada adı geçen "com.apple.network. identification.plist" dosyasının MacOS'un yeni sürümlerinden biri olan Mojave yüklü MacOS bilgisayar içerisinde olmadığı görülmüştür. Bluetooth üzerinden bağlanılan cihazlara ait kayıtların "com.apple.bluetooth.plist" isimli dosyada bulanabileceğinden bahsedilmiş (Maddu ve Rao, 2019) ancak kablosuz bağlantı alanı (Wireless Fidelity - Wi-Fi) ve USB üzerinden bağlanılan cihazlara ait kayıtlardan bahsedilmemiştir. "Mac Memorize" aracıyla rastgele erişilebilir bellek (random access memory –RAM) analizi gerçekleştirilen çalışmada bağlanılan Wi-Fi ağının parolası tespit edilmiş ve bu parolanın bir ağla ilişkili olduğunu gösteren ya da parola olduğuna dair bir ibare bulunamadığı belirtilmiştir (Catherine, 2012). MacOS ve diğer işletim sistemlerindeki ".bash history" dosyasının versiyonları karşılaştırılmış olup bu

dosyanın Windows ve Unix sistemlerde kullanıcıların girmiş olduğu komut geçmişini tuttuğu ancak MacOS sistemlerde kullanıcılara ait son girilen komutları tuttuğundan bahsedilmiştir (Mateljan ve ark., 2020). Mac işletim sisteminin bir özelliği olan Spotlight isimli arama motoru ile ilgili detaylı çalışmaların olduğu görülmüştür. Bu arama motoru mekanizmanın Spotlight Meta Veri Sunucusu (MDS) ve FSEvent'ler yardımıyla çalıştığından bahsedilmiştir (Atwal ve ark., 2019). FSEvent, dosya sistemi değişikliklerini tutan çekirdek içi bildirim sistemidir (Kaushik, 2007). Eğer bir dosya oluşturulmuş, değiştirilmiş veya silinmişse, bağlamsal metin ve gömülü meta veri dizine almak için, MDS'ye geri gönderilmeden önce uygun meta veri eklenerek indekslenir (Levin, 2012). MacOS'un 10.5 (Leopard) sürümü ile gelen, küçük resimler ve dosyaları ön izlemek için ayrı bir pencere açmaya yarayan QuickLook uygulması ele alınmış, bu küçük resimlerin tutulduğu veritabanı dosyasından bahsedilmiştir (Newcomer ve Martin, 2014). Parolaların adli bilişim incelemelerinde çok değerli olduğundan, incelemeleri engelleyebileceğinden bahsedilmiş olup depolanmış parolaların olası dosya konumları verilmiş bu dosyalardan şifre elde etmek için sosyal mühendislik yöntemi, şifre kırma ataklarının kullanabileceğinden bahsedilmiştir (Primeaux ve ark., 2011). Ancak söz konusu yöntemlerde şifrenin karmaşası arttıkça başarı oranının düştüğü ve çok uzun zamana ihtiyaç duyulduğu bilinmektedir. iTunes yedeklerinin MacOS üzerindeki dosya konumundan bahsedilmiş olup eğer şifreli ise şifresinin kırabilmesinin mümkün olduğundan ve Elcomsoft Phone Password Breaker isimli ücretli yazılımın kullanılabileceğinden bahsedilmiştir (Hoene ve Creutzburg, 2011). Ancak şifre ne kadar güçlü ise şifre kırma yazılımları kullanılarak şifre kırma işlemi bir o kadar zorlaşmaktadır.

MacOS bilgisayarların adli bilişim incelemesi ile ilgili yapılan literatür taraması sonucunda önceliklendirme (triyaj) metodunun yurt dışında yoğunlukla kullanıldığı görülmüştür. Önceliklendirme, depolama kapasiteleri artan sayısal delillerin elde edilmesinde hızlılık sağlanması için geliştirilen bir yöntemdir (Pearson ve Watson, 2010). Temel olarak adli bilişim sürecinin zaman alıcı bir süreç olmasına çözüm olarak sunulmaktadır (Hitchcock ve ark., 2016). Ancak önceliklendirme yöntemiyle yapılan incelemelerde delillerin bilimsel yöntemlerle elde edilmesi

konusunda şüpheler söz konusudur. Aynı zamanda bu yönteminin sadece teknik bir hızlandırma işlemi mi yoksa hukuksal süreçleri de kapsayan bir delil elde edilmesi yöntemi mi olduğu noktasında literatürde farklı görüşler bulunmaktadır (Değirmenci, 2020). Mahkeme veya savcılık, hangi sayısal delilin hangi veri taşıma aracında olduğunu, soruşturma veya kovuşturmanın verdiği bilgiler ışığında tayin ederek önceliklendirmeyi kararında göstermesi gerektiğinden ancak ülkemizde uygulamada buna çok dikkat edilmediğinden bahsedilmiştir (Değirmenci, 2020). Ülkemizde daha çok delilin kopyasının alınıp kopya üzerinden bir bütün olarak incelenmesi tercih edilmektedir. Bu sebeple yapılan araştırmaların çoğunda canlı inceleme yapılması, önceliklendirme yönteminin kullanılması ülkemiz açısından kaynakların yetersiz olduğunu göstermektedir. Yine yapılan çalışmaların çoğunun hiyerarşik dosya sistemi (hierarchical file system - HFS) ile ilgili olduğu, RAM analizi ile elde edilebilecek veriler olduğu görülmüştür. Adli bilişim ile ilgi bazı kayıtlar için sadece lokasyonlara odaklandığı görülmüştür. Söz konusu kayıtların, kopya üzerinden nasıl incelenmesi gerektiği açıklanmamıştır. MacOS'un HFS+'yi geride bırakarak yeni Apple dosya sistemine (apple file system - APFS) geçiş yapan güncel versiyonları üzerinde bir çalışma olmadığı tespit edilmiştir. İşletim sistemi üzerinden tespit edebileceğimiz parolalar incelemeleri kolaylaştırmaktadır. Literatürde belirtilen şifre kırma yöntemleri ve ücretli yazımlar yerine bu konuda ücretsiz yazılım kullanılarak şifre tespiti uygulamalarına yer verilmiştir. Yine yapılan çalışmalarda ağ ile ilgi bilgi elde edebileceğimiz dosyalar ve bu dosyaların yalnızca yolları gösterilmiştir. Ancak incelemeler sırasında söz konusu dosyalarda tutarsızlıklar görülmüş, yeni versiyon Mojave'de lireatürde belirtilen bazı dosyaların olmadığı görülmüştür. Ayrıca MacOS'un yeni versiyonlarında FileVault özelliği açık ise imaj alındıktan sonra inceleme yazılımları tarafından tanınmadığı görülmüş olup bu konu hakkında herhangi bir çalışma literatürde bulunamamıştır.

Bu çalışmada MacOS'un yeni dosyalama sistemi APFS'ye geçiş yapan versiyonları üzerinde çalışma olmadığı görüldüğü için platform olarak MacOS'un Mojave versiyonu seçilmiştir. Çalışmanın amacı, MacOS'e sahip bir bilgisayarda adli bilişim açısından önem arz edebilecek kayıtları analiz etmek, analiz sırasında karşılaşılan problemleri tespit etmek ve bu problemlere çözüm önerisi sunmaktır. Bu

amacı gerçekleştirmek için çalışma ortamının hazırlanması, verilerin toplanması, verilerin analizi ve sonuçların değerlendirilmesi aşamalarından oluşan bir metodoloji önerilmiştir. Bu metodolojiye uygun olarak çeşitli uygulamalar yapılmıştır. Uygulamaların ardından bilgisayarın imajı alınarak, tespit edilmek istenen kayıtlar incelenmiştir. İnceleme sonucunda; elde edebileceğimiz kayıtların doğruluğu, nasıl incelenmesi gerektiği, raporlama aşamasında yanıltıcı bir durum olup olmadığı belirtilmiştir. Ağ bağlantı türünün sonuçları etkilediği, MAC adresi kayıtlarının her seferinde doğru sonucu vermediği, doğru MAC adreslerinin ulaşılabilirliği, AXIOM yazılımı kullanıldığında raporlama aşamasında USB ile ağ bağlantısı sağlanan tüm iOS (iPhone İşletim Sistemi) sisteme sahip telefonları göstermediği, bu durumlarında dava sonucunu yanıltabileceği değerlendirilmiştir. Mojave versiyonu ile yapılan incelemelerde FileVault özelliği etkin ise kullanıcı şifresi bilinse dahi inceleme yazılımlarının disk imajını çözemediği görülmüştür. Bu konuda çözüm önerisi sunulmuştur. Wi-Fi parolalarının tespit edilmesi ve şifreli iTunes yedeklerinin şifre karmaşası dikkate alınmaksızın şifrelerinin tespit edilmesi konusunda ücretsiz yazılımlar kullanılarak çözüm önerisi sunulmuştur.

Yapılan incelemeler ve tespitlerin anlaşılırlığını kolaylaştırmak için kavramlar ve tanımlar, bu çalışmada kullanılacak olan ve Mac işletim sisteminin, Windows işletim sistemine göre aşina olmadığımız, adli bilişim açısından önem arz edebileceği değerlendirilen özellikleri anlatılmıştır. Çalışmanın diğer bölümleri şu şekilde organize edilmiştir; Bölüm 2'de MacOS üzerinde adli bilişim açısından önem arz edebileceği değerlendirilen kayıtlarının incelenmesi için metodoloji önerilmiştir. Bölüm 3'te önerilen metodolojinin uygulaması yapılmıştır. Sonraki bölümlerde ise tartışma ve sonuçlar sıralanmıştır.

1.1. Kavram ve Tanımlar

- **XTS-AES Blok Şifreleme Modu:** Orijinal olarak IEEE, NIST tarafından standartlaştırılmış şifreleme algoritmasıdır. LUKS, TrueCrypt, FileVault ve Microsoft dahil olmak üzere modern tam disk şifreleme sistemleri tarafından

kullanılır. CBC gibi diğer mevcut blok şifreleme modlarına daha güçlü bir alternatif olarak tasarlanmıştır. Diğer modlardaki yetersizlikten faydalanmak için kullanılabilen bazı daha karmaşık yan kanal saldırıları ile birlikte ortaya çıkan olası güvenlik zafiyetlerini ortadan kaldırır (Thompson, 2017).

- **APFS:** Apple dosyalama sistemi olarak adlandırılan bu sistem, depolama alanının desteğini artırmak, şifreleme ve veri bütünlüğünü korumak üzere tasarlanan ve macOS High Sierra ile gelen yeni dosya sistemidir (Reddy, 2019).

- **ASL:** Apple sistem günlüğü, uygulamalar tarafından sağlanan günlük bilgilerini yöneten ve depolayan bir servistir. Bilgiler, uygulama adı, işlem tanımlaması ve kullanıcı gibi farklı kriterler kullanılarak saklanır. Binary formatta depolanırlar. Zaman bilgileri ise Epoch formattadır. Her ASL dosyasında bir başlık ve bir veya daha fazla giriş vardır. Başlığın, başlangıç girişini ve son girişi belirten iki önemli alanı vardır. Girişler ardışık olarak kaydedilir (Garijo ve Cavallaro, 2015).

- **Audit:** Mac işletim sistemlerde meydana gelen olayların tutulduğu günlük binary dosyalarıdır. Sonu crash_recovery olarak biten audit günlük dosyaları, sistemin crash olması sonrasında kurtarılan audit dosyalarıdır. İsim bilgisi tarih formatında olan dosyalar ise audit işlemi tarafından normal şekilde sonlandırılmış audit dosyalarıdır. Bu dosyaların isim formatları "log_dosyasının_ baslangıc_zamanı.log_dosyasının_bitis_zamanı" şeklindedir (Maddu ve Rao, 2019).

- **Core Storage:** MacOS'ta Apple tarafından Mac OS X Lion'a tanıtılan bir mantıksal birim yönetim sistemidir. Filevault ve Fusion Drive dahil olmak üzere OSX'te bir çok özelliğin uygulanmasını sağlar (Faronics, 2017)

- **Fusion Drive,** HDD sürücü ile SSD sürücüyü birleştiren bir depolama birimidir. Sistem performansını en üst düzeye çıkarmak için veriler, otomatik olarak HDD sürücüden SSD sürücüye taşır. Bu teknoloji ile başlatma süreleri kısalır ve sistem sizin nasıl çalıştığınızı öğrendiği için uygulamalar daha hızlı açılır (Gupta ve Rogers, 2014).

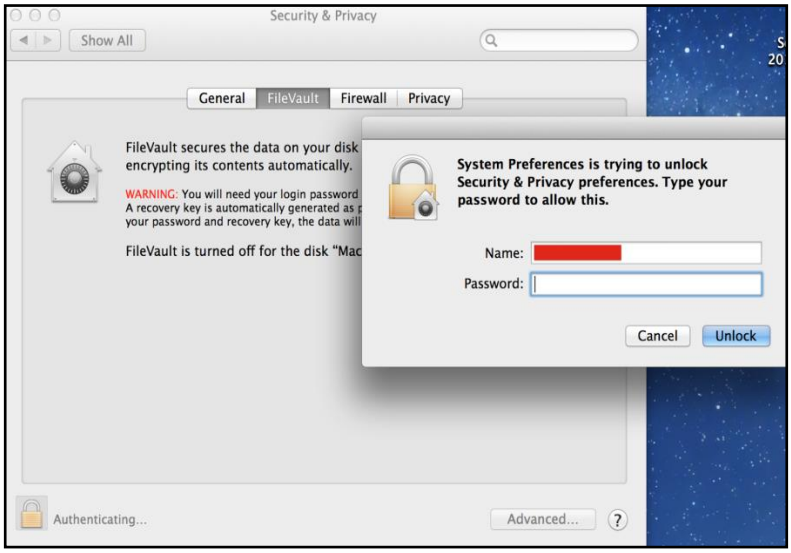
- **Plist:** Mac OS X ve harici uygulamalar tarafından kullanılan dosyalardır. Uygulama ve sistem yapılandırmalarını saklamak için kullanılır. İki farklı formatta depolanabilirler. Bunlar XML ve BPlist olarak adlandırılan binary formattır. (Garijo ve Cavallaro, 2015).

• **Unix:** Bell Laboratuvarlarında geliştirilmiş, çok kullanıcılı, çok görevli yapıyı destekleyen bilgisayar işletim sistemidir (Eteng ve ark., 2007).

• **FileVault:** Mac OS X Lion'dan önce FileVault sadece kullanıcı ana dizinini şifreliyordu. Kullanıcı çıkış yaptığında ya da bilgisayarı kapattığında şifreli durumda kalıyor. Lion ve sonrasında FileVault 2, diskin tümünü, hatta çıkarılabilir diskleri de şifrelemektedir. FileVault, 256 bitlik anahtarla XTS-AES 128 ile şifreleme algoritmasını kullanır. Her kullanıcı şifresi veya kurtarma anahtarı ile bu şifrelemeyi çözebilir (SWGDE, Erişim Tarihi:30.07.2019).

FileVault'u aktif hale getirip diski şifrelemek için; öncelikle Spotlight (Command+Space) üzerinden sistem tercihlerine erişilir, ardından güvenlik ve gizliliğe (Security&Privacy) gelerek aşağıdaki şekilde gösterildiği gibi FileVault sekmesine tıklanır (Şekil 1.1). Daha sonra ekrana kullanıcı adı ve şifre girilir (Şekil 1.2).

Şekil 1.1. FileVault ayarını etkinleştirme-1.



Şekil 1.2. FileVault ayarını etkinleştirme-2.

FileVault'u aktif etmek için "FileVault'u aç (Turn On FileVault)" sekmesine tıklanır (Şekil 1.3). Bu işlemin ardından, 24 haneden oluşan "kurtarma anahtarı (recovery key)" gelecektir. Bu anahtar, FileVault şifresinin unutulması halinde diske tekrar erişim sağlanmasını sağlar.

Şekil 1.3. FileVault ayarını etkinleştirme-3.

FileVault özeliği “sudo fdesetup enable” komutu ile ya da sadece belirtilen kullanıcı için “sudo fdesetup enable –user” komutu ile kullanıcı adını ve şifresini girerek aktif edilebilir. FileVault için önemli noktalar ise ;

- Mutlaka kullanıcınıza şifre verilmesi gerekmektedir.
- Şifrenin ve kurtarma anahtarının unutulması halinde tüm veriler ve ayarlar silinir.
- Birden fazla kullanıcı varsa FileVault ayarı aktif olan kullanıcı giriş yapabilir, diğer kullanıcılar ise yetkili kullanıcı girişi ardından giriş yapabilirler.
- Birden fazla kullanıcı varsa FileVault özelliği her kullanıcı için ayrı ayrı aktif edilir. Ayrıca tüm kullanıcılar için FileVault’u aktif edilebilir (Boursalian ve Stamp, 2019).

1.2. Mac İşletim Sistemi ve Versiyonları

Mac İşletim Sistemi 1984 yılındaki ilk Macintosh bilgisayarın işletim sistemidir. Mac İşletim Sistemi monolitik bir çekirdeğe sahipti ve eskiden MFS (Macintosh dosya sistemi) isimli bir dosya sistemi kullanıyordu. 1985 yılında Macintosh dosya sistemi HFS (Hierarchical File System) olarak değiştirildi. Mac işletim sistemi 2001 senesinde OS X olarak adlandırıldı. Burada OS'un yanında ki X romen rakamı olarak 10'u temsil etmektedir. (Summers ve ark., 2001) 2001'de tanıtılan Mac OS X'in sürümü 10.1’dir. Daha sonraki Mac işletim sistemlerinin versiyonları, tanıtılma tarihleri şunlardır:

- OS X 10.0: Cheetah - 24 Mart 2001
- OS X 10.1: Puma - 25 Eylül 2001
- OS X 10.2: Jaguar - 24 Ağustos 2002
- OS X 10.3 Panther (Pinot) - 24 Ekim 2003
- OS X 10.4 Tiger (Merlot) - 29 Nisan 2005
- OS X 10.5 Leopard (Chablis) - 26 Ekim 2007
- OS X 10.6 Snow Leopard - 28 Ağustos 2009
- OS X 10.7 Lion (Barolo) - 20 Temmuz 2011

- OS X 10.8 Mountain Lion (Zinfandel) - 25 Temmuz 2012
- OS X 10.9 Mavericks (Cabernet) - 22 Ekim 2013
- OS X 10.10: Yosemite (Syrah) - 16 Ekim 2014
- OS X 10.11: El Capitan (Gala) - 30 Eylül 2015
- macOS 10.12: Sierra (Fuji) - 20 Eylül 2016
- macOS 10.13: High Sierra (Lobo) - 25 Eylül 2017
- macOS 10.14: Mojave (Liberty) - 24 Eylül 2018
- macOS 10.15: Catalina - 7 Ekim 2019

Görüldüğü üzere MacOS sürekli gelişim göstermektedir. Son yıllarda bu gelişim sadece işletim sistemi versiyonu değil aynı zamanda dosyalama sisteminde de köklü değişiklikleri kapsamaktadır. MacOS uzun yıllardır kullandığı HFS+ dosyalama sistemini geride bırakarak APFS dosyalama sistemine geçiş yapmıştır. Adli bilişim yazılımları ise MacOS'un bu köklü gelişimini aynı hızda takip edememektedir. Literatür taramasına baktığımızda yapılan çalışmaların eski dosyalama sistemi olan HFS+ üzerinde olduğu görülmüştür. Yeni dosyalama sistemi olan APFS üzerinde adli bilişim açısından önem arz edebileceği değerlendirilen, tespit edilmesi hedeflenen kayıtları incelemek ve inceleme sırasında herhangi bir problemle karşılaşıp karşılaşılmadığının tespiti için bu çalışmada diğerlerinden farklı olarak çalışma platformu MacOS Mojave seçilmiştir.

2. GEREÇ VE YÖNTEM

Tez çalışmasında Mac işletim sistemi üzerinde adli bilişim incelemelerini yürütmek için üç aşamalı metodoloji önerilmektedir:

1) Çalışma Ortamının Hazırlanması ve Gereçler,
2) Verilerin Toplanması,
3) Verilerin Analizi ve Sonuçların Değerlendirilmesi.

2.1. Çalışma Ortamının Hazırlanması ve Gereçler

Bu çalışmanın amacı, APFS dosyalama sistemine sahip Mac işletim sistemi üzerinde adli bilişim açısından önem arz edebileceği değerlendirilen kayıtları analiz etmek ve analiz sırasında karşılaşılan problemlere çözüm önerisi sunmaktır. Dolayısı ile incelemecinin elinde sadece delil olarak bilgisayar olduğu düşünülmelidir. Bilgisayar adli bilişim prensiplerine uygun olarak delil kabul edilmeli ve imajı alınmalıdır.

- Çalışma ortamı için APFS dosyalama sistemine sahip Macbook bilgisayar temin edilmeli ve yine APFS dosyalama sistemine sahip MacOS sanal bilgisayar oluşturulmalı,
- Bilgisayar ile bağlantı kurulan telefonların MAC adresinin tespit edilebilmesi ve MAC adresinin doğruluğunu kanıtlamak için MAC adresleri bilinen akıllı telefonlar temin edilmeli,
- Bilgisayar ile bağlantı kurulan yazıcıya ait kayıtların tespit edilebilmesi için kablosuz bağlanma özelliği olan yazıcı temin edilmeli,
- Bilgisayara takılan harici belleklere ait kayıtların tespit edilebilmesi için USB bellek ve CD temin edilmeli,
- Yukarıdaki adımları gerçekleştirebilmek için yine imaj alma yazılımı ve inceleme yazılımları temin edilmelidir.
- Bu çalışma için temin edilen yazılımlar aşağıda belirtilmiştir.

- VMware® Workstation 15 Player
- BlackBag MacQuisition (Version 2019 SR-2) Yazılımı
- BlackBag BlackLight 2019 Yazılımı
- X-Ways Forensics (Version 19.7 SR6) Yazılımı
- Magnet Axiom Examine&Proces (Version 3.6.0.15906) Yazılımı
- Passware Forensic Kit (Version 2018 v5) Yazılımı
- Dcode.v4.01b
- plist Editor Pro
- HXD editör
- Mac_Apt.exe
- Chainbreaker.exe
- Dumpkeychain.exe

Mac işletim sistemi incelemelerinde kullanılabilecek yazılımlar Windows işletim sistemine göre çok azdır. Bu durum APFS dosyalama sistemi olduğunda daha da zorlaşmaktadır. Çalışma sırasında bazı yazılımların APFS dosyalama sistemini desteklediğini iddia etse de imajların yazılımlar tarafından çözümlenmediği görülmüştür. Bu sebeple yukarıda belirtilen yazımlara alternatif olarak kullanılabilecek yazımların APFS dosyalama sistemine sahip imaj ile denenmesi gerekmektedir.

2.2. Verilerin Toplanması

Veri toplama aşamasında adli bilişim incelemeleri sürecini ilgilendiren aşağıda listelenen veriler toplanmalı ve tespitler yapılmalı;

- İşletim sistemi versiyonu ve kurulma tarihi tespiti,
- Oluşturulan ve silinen kullanıcıların tespiti,
- Kullanıcının oturum açma ve kapatma bilgilerine ait tespitler,
- Bilgisayarın başlatma ve kapatma tarihi tespiti,
- Tarih-saat değişikliğinin tespiti,
- Sistem güncelleme bilgilerinin tespiti,

- Ağ üzerinden erişim, MAC adresleri, kablosuz erişim noktalarına yapılan bağlantıların tespiti,

- Yazıcıdan çıktı alındıktan sonra oluşan kayıtların tespiti,

- Bilgisayara takılan harici veri depolama cihazlarına ait kayıtlar,

- Yüklenen programların tespiti,

- FileVault2 özelliği aktif olan disklerde alınan imajların kullanıcı verisine nasıl erişilebileceğine dair tespitler,

- Mac bilgisayara bağlanılan ağların ve bilgisayara alınan şifreli iTunes backupların şifrelerinin tespiti.

2.2.1. Mac İşletim Sistemine Sahip Sanal Makinenin Kurulması

- İşletim sistemine ait bilgilerin tespiti amacıyla, sanal makine kurulmalı, işletim sistemi kurulurken bilgisayar adı, tarih ve saat not alınmalı,

- Sanal makineler ile birden fazla uygulama gerçekleştirilip veri analiz aşaması hızlı bir şekilde uygulanabilir. Sanal makineler ile birbirinden farklı MacOS versiyonu kurup inceleme bu sanal makineler üzerinden gerçekleştirilebilir. Ancak macOS sanal makine kurulumun yapılabilmesi için yama aracının yüklemesi gerekmektedir. Yama aracı internetten ücretsiz olarak sağlanmaktadır. Sanal makine kurulumunda performans sistem kaynaklarına bağlı olduğundan bu işlemin yapılacağı bilgisayar ona göre seçilmelidir. Windows işletim sistemi üzerinde MacOS sanal makine kurmak yerine MacOS işletim sistemine sahip bir bilgisayarda sanal makine kurulumu daha kolay sağlanabilir. Sanal makineye alternatif olarak bilgisayarın mevcut işletim sistemi versiyon bilgisi not edilebilir. Bu durumda tespit edilmek istenen veri, bilgisayarın alınan imajı üzerinden yapılabilir. Ancak bu şekilde sadece mevcut olan versiyonun tespiti yapılmış olacaktır.

2.2.2. Mac İşletim Sistemine Sahip Sanal Makine Üzerinde Kullanıcıların Oluşturulması ve Kullanıcı Silinmesi

- Mevcut kullanıcı ve silinen kullanıcılara ait kayıtların tespit edilebilmesi için ilk aşamada birden fazla kullanıcının oluşturulması önerilir. Yönetici hakkına sahip kullanıcı, standart kullanıcılardan birini sildiğinde kayıt oluşması için ve veri toplama işlemini gerçekleştirilebilmesi için en az bir yönetici ve en az iki standart yetki ile kullanıcı tanımlanmalı,

- Kullanıcılar oluşturulurken ve silinirken bu işlemlere ait kullanıcı adları, bu işlemleri hangi kullanıcı tarafından yapıldığı varsa kullanıcı parola ipuçları, kullanıcıların yetkileri ayrı ayrı not alınmalı.

2.2.3. Mac İşletim Sistemi Üzerinde Kullanıcıların Giriş-Çıkış İşlemleri

- Bu aşamada kullanıcının giriş-çıkış zaman bilgisinin tespiti için belirlenen bir kullanıcı ile oturum açmalı ve bir süre sonra oturum kapatılmalı,

- Oturum açma ve kapama işlemini yapan kullanıcı adı ve bu işlemlerin tarih-saati not alınmalı.

2.2.4. Mac İşletim Sistemine Sahip Bilgisayarın Açma ve Kapama İşlemleri

- Bilgisayarın açma ve kapama bilgilerinin tespiti için bilgisayar kullanılarak açma ve kapama işlemleri gerçekleştirilmeli,

- Bilgisayarın açma ve kapama işlemlerinin tarih ve saat bilgileri not alınmalı.

2.2.5. Mac İşletim Sistemi Üzerinde Kullanıcı Tarafından Yapılan Tarih ve Saat Değişikliği İşlemleri

- Kullanıcı tarafından değiştirilen tarih ve saat ayarlarına ilişkin kayıtların tespit edilebilmesi için bilgisayarın gerçek sistem saati not edilmeli,
- Kullanıcı tarafından sistem saati değiştirilmeli ve değiştirilen sistem saati not edilmeli.

2.2.6. Sistem Güncelleme Bilgilerinin Tespiti

- Sistem güncelleme bilgilerinin tespiti için mevcut sistem versiyonu not edilmeli,
- Bilgisayarın sistem güncellemesi yapılarak versiyonu yükseltilmeli, yükseltilen versiyon bilgisi not edilmeli,
- Ardından güncelleme tarihi bilgisi ve işletim sistemi yükleme tarihi geçmişi not edilmelidir.
- Bazı işletim sistemi versiyonlarında, işletim sistemi güncellendikten sonra işletim sisteminin kurulum tarihi, güncelleme tarihi olarak gözükmektedir. Bu da yanlış sonuçlar doğurmaktadır.

2.2.7. Ağ Yapılandırması, Ağ Üzerinden Erişim, Kablosuz Erişim Noktalarına Yapılan Bağlantı İşlemleri

- İnternet'e bağlanma özelliğine sahip bir cihazın ethernet kartına, üretici tarafından verilen harf ve sayılardan oluşan fiziksel adrese, ortam erişim kontrolü (media access control-MAC) adresi adı verilir (Garg ve ark., 2012). İnternet'e bağlı olan her cihazın farklı bir MAC adresi bulunur ve ethernet kartı değişmediği sürece MAC adresi de değişmemektedir. Kırk sekiz bitten oluşan MAC adresleri, onaltılı (hexadecimal) sayı sisteminde on iki karakter ile ifade edilir. En baştaki altı karakter, cihaz üreticisini (organizasyona ait eşsiz kimlik/OUI) tanıtır (Martin ve ark., 2016).

Geriye kalan son altı karakter ise cihazın benzersiz adresi olarak tanımlanır. Bu benzersizlikten ötürü adli içerik incelemelerinde kişiye ait bilgisayar, cep telefonu gibi elektronik cihazların MAC adreslerinin tespitiyle desteklenmesi önemlidir (Gedik, 2019). Akıllı telefonlar hücresel ağlar üzerinden veri kullanımı gerçekleştirebilmektedirler (Sarwar ve Soomro, 2013), dolayısı ile internet'e her zaman ve her yerden erişebilme yeteneğine sahiplerdir (Kim ve ark., 2011). İnternet'in bulunmadığı ortamlarda kullanıcılar çoğunlukla telefondaki bu hücresel ağ bağlantısını kullanarak bilgisayar üzerinden internet'e erişim sağlarlar. İnternetin yaşamımızın her alanında olması karşısında sanal ortamda işlenen suçlar ve kötücül yazımlarının kullanımında da artışlar olmuştur (Aslan ve Samet, 2020). Sanal ortamda işlenen suçlar dışında kurulan basit bir ağ bağlantısı ile bir çok olay çözüme kavuşturulmuştur. Avustralya Kriminoloji Enstitüsü tarafından yapılan bir araştırmada, 2010-2012 arasında Avustralya'daki 479 cinayetin % 75'inde, olay sırasında suçlunun ağ bağlantısı gerçekleştirdiği gösterilmiştir (Cussen ve Bryant, 2015). Mobil cihazlar ile bilgisayar arasında ağ bağlantısı kurulduğu anda işletim sistemine düşen kayıtlardan tespit edilen MAC adresleri sayesinde kullanılan cihazı kimin satın aldığına ve cihazın nerede satıldığına dair bilgilere ulaşılabilir (Blackman ve Szewczyk, 2015).

- Bu aşamada bağlanılan ağ isimleri ve MAC adreslerini tespit etmek amacıyla; bilgisayar ile cep telefonları ve yazıcı arasında bağlantı kurulmalı,

- iOS işletim sistemine sahip telefonlar MacOS bilgisayar ile direkt olarak USB, Wi-Fi üzerinden ve çoğu zaman iki seçenekte aktif iken ağ bağlantısı gerçekleştirebilmektedir. Uygulamalarda kullanılan bağlantı türleri bu doğrultuda seçilmeli,

- Uygulamalarda ortaya çıkan farklılıkları görmek amacıyla "Wi-Fi Ağını Anımsa" seçeneği aktif ve pasif iken bağlantı kurulmalı,

- Bağlantı kurulan cihazlara ait MAC adresleri, marka/model bilgisi, cihaz adı, her cihazın ayarlar bölümünden elde edilmeli,

- Oluşturulan bağlantı türleri, ağ isimleri not edilmeli.

2.2.8. Yazıcıdan Çıktı Alındıktan Sonra Oluşan Kayıtların Tespiti

- Yazıcıdan çıktı alındıktan sonra oluşan kayıtların tespiti için bilgisayar ile yazıcı arasında bağlantı kurulmalı, yazıcının marka/model bilgisi not edilmeli, çıktı alma işlemi gerçekleştirilmeli,
- Çıktı alınacak dosyanın ham hali saklanmalı, dosyanın ismi ve yazdırma işlemine ait tarih-saat bilgisi not edilmeli.

2.2.9. Bilgisayara Takılan Harici Veri Depolama Cihazlarına Ait Kayıtların Tespiti

- Bilgisayara takılan harici veri depolama cihazlarına ait kayıtların tespiti için harici veri depolama cihazları bilgisayara takılmalı, bu cihazlar üzerinden dosya erişimi sağlanmalı,
- Harici veri depolama cihazlarına ait birim etiketleri ile seri numaraları, bu cihazlar üzerinden erişilen dosya isimleri not edilmeli.

2.2.10. Bilgisayara Programların Yüklenmesi

- Mac bilgisayara programlar Apple Uygulama Mağazası üzerinden veya terminal üzerinden kurulabilir, bu sebeple yüklü programların tespiti amacıyla her iki yöntemle program yükleme işlemi gerçekleştirilmeli,
- Bilgisayara yüklenen programların ismi ve bu işleme ait tarih-saat bilgisi not edilmeli.

2.2.11. MacBook Pro Bilgisayarın Filevault2 Özelliğini Aktif Etme

- İmaj alma ve inceleme sırasında Filevault2 özelliğinden kaynaklı karşılaşılabilecek problemlere ve bu problemlere çözüm önerisi sunmak amacıyla Bölüm 1.1'de anlatıldığı gibi bilgisayarın FileVault özelliği aktif edilmeli,
- FileVault özelliğini aktifleştirme işlemini yapan kullanıcının oturum şifresi not edilmelidir.

2.2.12. MacBook Pro Bilgisayar Üzerinden Şifre Tespitleri

- İnceleme sırasında bağlanılan ağların şifrelerini tespit etmek ve şifresi bilinmeyen iTunes yedek dosyalarına karşı çözüm önerisi sunmak amacıyla iTunes yazılımı ile iOS işletim sistemine sahip cep telefonun bilgisayara yedeği şifrelenerek alınmalı, yedeğe verilen şifre not edilmeli,
- Bilgisayarın kablosuz ağlarla bağlantısı kurulmalı, bağlantı kurulan ağların parolaları not edilmeli.

Bu çalışmada önerilen metodolojinin ikinci aşaması olan verilerin toplanması adımı, inceleme sonuçlarının doğruluğunun kanıtlanabilmesi için önemlidir. Bu adımda yukarıda belirtilen uygulamaların ayrı ayrı gerçekleştirilmesi önerilir. Gerçekleştirilen her uygulamadan sonra bilgisayar adli bilişim prensiplerine uygun olarak delil olarak kabul edilmeli ve imajı (kopyası) alınmalıdır. Bilgisayar imajının incelemesinin yanında sanal makine incelemesi de adli bilişim açısından önemli olabilmektedir. Uygulamalar sanal makine üzerinden de gerçekleştirilebilir. Eğer uygulama sanal makine üzerinde gerçekleştirildiyse sanal makine kurulumu ile oluşan dosya incelemek üzere saklanmalıdır. Verilerin analizi ve sonuçların değerlendirilmesi aşamasında alınan kopyalar veya sanal makine kurulumu ile oluşan dosyalar verilerin analizi ve sonuçların değerlendirilmesi aşamasında incelenebilir.

2.3. Verilerin Analizi ve Sonuçların Değerlendirilmesi

Veri toplama aşamasında alınan her imaj veya sanal makine kurulumu ile oluşan dosyalar, incelemek için kullanılabilecek yazılımla incelenmelidir. İnceleme sonucunda tespit edilen kayıtlar ile veri toplama aşamasında belirlenen karşılaştırılıp kayıtlar arasında farklılık varsa bu farklılığın tekrar eden bir yapıda olup olmadığına bakılabilir. Tespit edilemeyen veriler, imaj içerisinde anahtar kelime olarak aratılmalı tespit edilebilirliğine dair değerlendirme yapılmalıdır.

Bu aşamada elde edilen bilgilere bakılarak; tespit edilebilen kayıtların doğruluğu veri toplama aşamasında elde edilen bilgilerle karşılaştırılarak gösterilmiştir. Adli bilişim yazılımlarınca desteklenmeyen kayıtlar için anahtar kelimeler oluşturulmuştur. Bu yöntem ile erişilen kayıtlar için anahtar kelimeler belirtilmiştir. Mac işletim sisteminde çoğu veri binary formatta tutulmaktadır bu dosyaların nasıl okunabilir hale getirildiği, nasıl incelenmesi gerektiği gösterilmiştir. Tarih saat bilgileri UTC (Eşgüdümlü evrensel zaman) formatı dikkate alınarak tespit edilmiştir. Yazdırılan belgeler ve tarih bilgileri soruşturma aşamasında önemli olabilmektedir. Bu tarih bilgilerinin binary format içerisinde bulunduğu ancak adli bilişim yazılımlarınca çözümlenmediği görülmüştür. Tarih bilgisinin nasıl tespit edilip okunabilir formata çevrileceği gösterilmiştir. Yine yazdırılan belgenin ham halinin nasıl bulunabileceği gösterilmiştir. Farklı marka\model telefonlar ile yapılan uygulamalar sayesinde, MAC adreslerinin tespit edilebilirliğine dair değerlendirmeler yapılmış ve nihayetinde sadece inceleme yazılımına bağlı kalınarak raporlama yapılmaması gerektiği önerilmiştir. İnceleme yazılımlarının MAC adresi kayıtlarını her seferinde doğru sonucu vermediği gösterilmiştir. MAC adres tespitinde ağ bağlantı türünün sonuçları etkilediği, iOS cihazlar için Wi-Fi ile bağlantı sağlandığı zaman işletim sistemine düşen MAC adresi kayıtlarının tamamen farklı olabileceği ve bu durumun göz önüne alınması gerektiği önerilmiştir. iOS cihazlarda USB ile bağlantı sağlandığı zaman işletim sistemine düşen MAC adresi kaydının doğrusunun nasıl bulunabileceği, AXIOM yazılımı kullanıldığında raporlama aşamasında bağlanılan USB ile ağ bağlantısı sağlanan tüm iOS işletim sistemine sahip telefonları göstermediği, bu durumlarında dava sonucunu

yanıltabileceği uyarısında bulunulmuştur. Mojave versiyonu ile yapılan incelemelerde FileVault özelliği etkin ise inceleme aşamasında problemlerle karşılaşılmıştır. Filevault özelliği etkin olan bilgisayarın imajı alınırken kullanıcı şifresinin girilmesi gerekmektedir. Bu şekilde imaj Filevault şifresi çözümlenerek alınacaktır. Ancak yeni versiyonla beraber imaj alınırken kullanıcı şifresi girilse dahi inceleme yazılımlarının disk imajını çözemediği görülmüştür. FileVault özelliği etkin olan bilgisayarın imajı içerisinden kullanıcı verilere nasıl erişilebileceğine dair çözüm önerisi sunulmuştur. Parola tespiti, adli bilişim incelemelerinde önemli bir yere sahiptir. Wi-Fi parolalarının tespit edilmesi ve şifreli iTunes yedeklerinin şifre karmaşası dikkate alınmaksızın şifrelerinin tespit edilmesi konusunda ücretsiz yazılımlar kullanılarak çözüm önerisi sunulmuştur. Mac işletim sistemi sürekli gelişme göstermekte adli bilişim yazılımları aynı hızda takip edememektedir. Bu sebeple imaj alma işlemi düzgün gerçekleştirilse dahi bazı durumlarda adli bilişim yazılımları imajı tam olarak çözümleyememektedir. Bu durumlarda tespit edilmesi gereken kayıtlar imaj içerisinden bulunup manuel olarak incelemesinin yapılması gerekebilir. Bu çalışma sonunda Mac işletim sisteminde adli bilişim açısından önemli olabileceği değerlendirilen kayıtlara ait izlerin nerede bulunduğunu gösteren bir tablo oluşturulmuştur.

3. BULGULAR

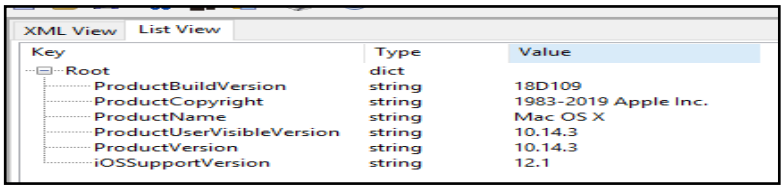
Bu bölümde, önerilen metodolojinin uygulaması yapılmıştır. Metodolojinin ilk aşamasında belirtildiği gibi; işletim sistemi kayıtlarını incelemek üzere Macbook Pro (A1707) bilgisayar, iOS işletim sistemine sahip iPhone telefonlar, kablosuz bağlanma özelliği olan yazıcı, harici depolama cihazları, gereç bölümünde belirtilen imaj alma ve inceleme yazılımları temin edilmiştir. Çalışma ortamının hazırlanmasının ardından, aşağıdaki her bir başlık altında; veri toplama aşaması gerçekleştirilmiş alınan imajlar ve sanal makine kurulumu ile oluşan dosyalar incelenerek önerilen metodolojinin son aşaması olan verilerin analizi ve sonuçların değerlendirilmesi aşaması tamamlanmıştır.

3.1. Mac İşletim Sistemi İle İlgili Kayıtların Analizi

İşletim sistemi sanal makineye kurulmuştur. Veri toplama aşamasında elde ettiğimiz veriler şunlardır:

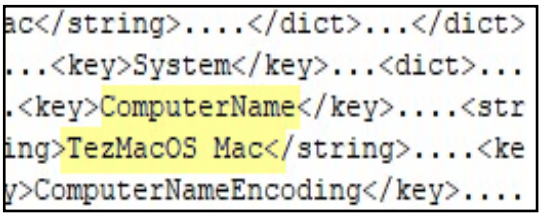
- Kurulan işletim sistemi versiyon bilgisi: MacOS 10.14.3 (Mojave),
- Bilgisayar adı: "TezMacOS" olarak belirlenmiştir.
- İşletim sistemi kurulum tarih-saat bilgisi: Tarih 10.08.2019 saat 09:47 (UTC+3).

MacOS 10.14.3 (Mojave) işletim sistemi kurulmasından sonra, sanal disk dosyalarının yapılan analizinde; "…\System\Library\CoreServices\" konumu altında bulunan "SystemVersion.plist" isimli dosyanın, plist Editör ile açılarak incelenmesi sonucu, içerisinde işletim sistemi versiyon bilgilerinin olduğu görülmüştür (Şekil 3.1).



Şekil 3.1. İşletim sistemi versiyon bilgileri.

"…\Library\Preferences\SystemConfiguration\" konumu altında "preferences.plist" isimli dosya içerisinde ise bilgisayar adına ait kayıt tespit edilmiştir (Şekil 3.2).



Şekil 3.2. Bilgisayar adı bilgisi.

İşletim sistemi kurulduğu anda "…\private\var\db\" konumu altında ".AppleSetupDone" isimli dosya oluşmaktadır. Söz konusu dosyanın X-Ways yazılımı ile yapılan analizinde oluşma tarihi UTC+4'e göre 10.08.2019 saat 10:47 olarak gözükmektedir. İşletim sistemi ise UTC+3'e göre 10.08.2019 saat 09:47'de kurulmuştur (Şekil 3.3).

Şekil 3.3. "AppleSetupDone" dosyasının oluşma zamanı.

Tespit edilmesi hedeflenen işletim sistemi versiyon bilgisi, kurulma tarihi ve bilgisayar adı kaydına ulaşılmıştır. Veri toplama aşamasında elde ettiğimiz veriler ile tespit edilen kayıtların doğruluğu görülmüştür. X-Ways yazılımı ile kurulum tarihinin UTC+4'e göre gösterdiği görülmüştür.

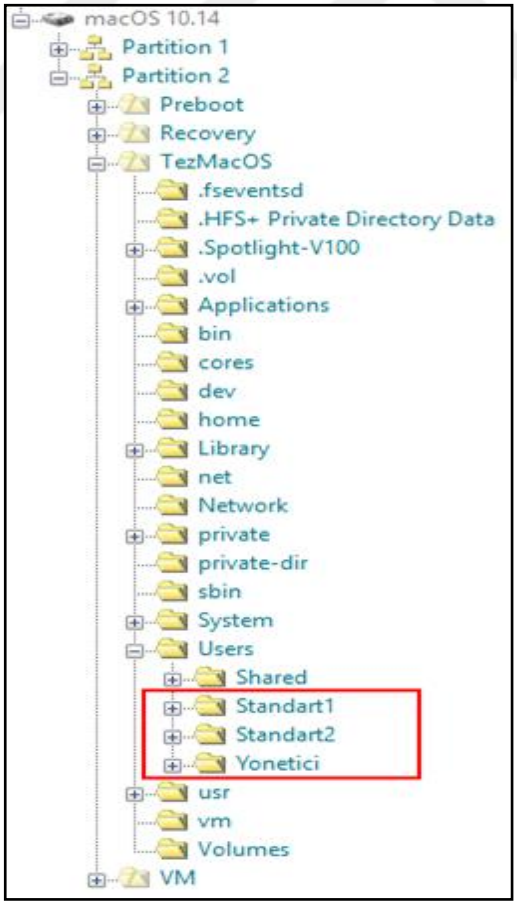
3.2. Mevcut Kullanıcıya Ait Kayıtların Analizi

Mac bilgisayarda üç adet kullanıcı oluşturulmuştur. Oluşturulan ilk kullanıcı yönetici yetkisindedir ve bu kullanıcının şifresi olmak zorundadır. Veri toplama aşamasında elde ettiğimiz veriler şunlardır:

Oluşturulan kullanıcılar;

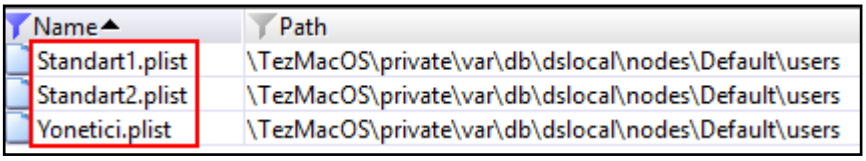
- Yönetici yetkisine sahip “Yonetici” isimli kullanıcı, tarih 11.08.2019, saat 15:35’de (UTC+3) oluşturulmuştur. Kullanıcıya ait parola “JKDB” olarak belirlenmiştir.
- Yonetici kullanıcısı tarafından standart yetkiye sahip “Standart1” isimli kullanıcı tarih 11.08.2019, saat 15:50’de (UTC+3) oluşturulmuştur. Kullanıcıya ait parola “9876” ve parola ipucu “okul numarası” olarak belirlenmiştir.
- Yonetici kullanıcısı tarafından standart yetkiye sahip “Standart2” isimli kullanıcı tarih 11.08.2019, saat 16:04’de (UTC+3) oluşturulmuştur. Kullanıcıya ait parola “Jdeneme06” olarak belirlenmiş parola ipucu tanımlanmamıştır.

Biri yönetici yetkisine sahip, diğer ikisi standart yetkiye sahip olmak üzere 3 adet kullanıcı oluşturulduktan sonra sanal disk dosyasının “X-Ways” yazılımı ile yapılan incelemesinde mevcut kullanıcılara ait ana kullanıcı klasörlerinin oluştuğu görülmüştür (Şekil 3.4).



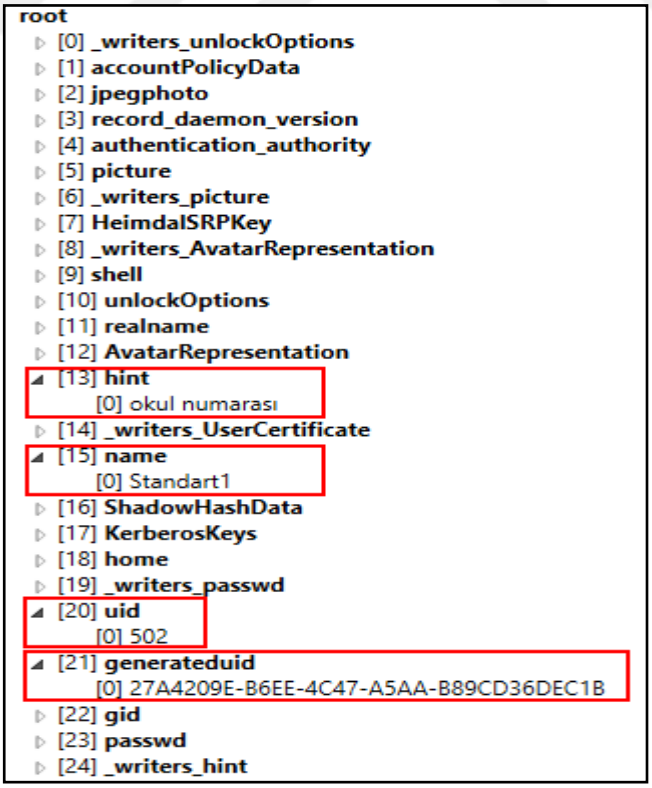
Şekil 3.4. Ana kullanıcı klasörlerine ait görüntü.

Kullanıcılar oluşturulduğunda "…\private\var\db\dslocal\nodes\Default\users" konumu altında her kullanıcıya ait, kullanıcı adında .plist uzantılı dosyanın oluştuğu görülmüştür (Şekil 3.5). Bu .plist dosyaları içerisinde MacOS 10.8'den sonraki versiyonlarda kullanıcı şifresinin PBKDF2-SHA512 (Parola Tabanlı Anahtar Türetme Fonksiyonu-Güvenlik Hashing Algoritması) ile hesaplanan hash değeri tutulmaktadır (Garijo, 2015).



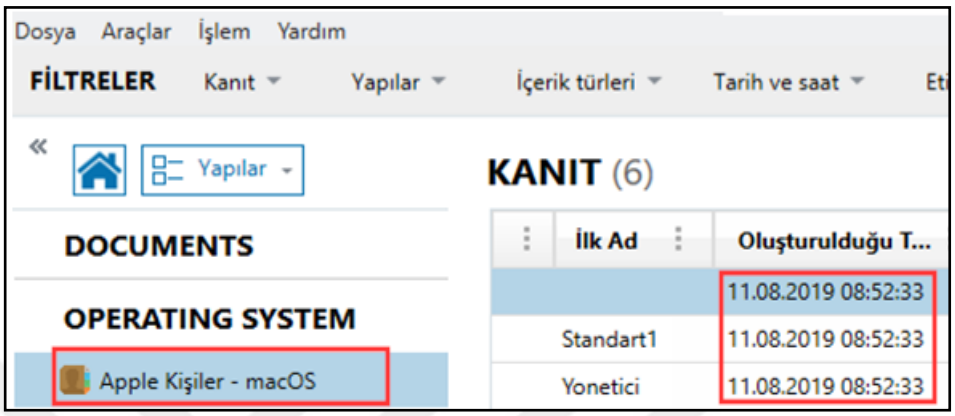
Şekil 3.5. Kullanıcılara ait ".plist" dosyaları.

Kullanıcıya ait .plist dosyasının, AXIOM yazılımının plist görüntüleyicisi ile yapılan incelemesinde kullanıcı adı, kullanıcıya özgü ID (uid), UUID (generateduid) ve parola ipucu verilerinin olduğu görülmüştür (Şekil 3.6). Örnek olarak kullanıcılardan sadece bir tanesi gösterilmiştir.



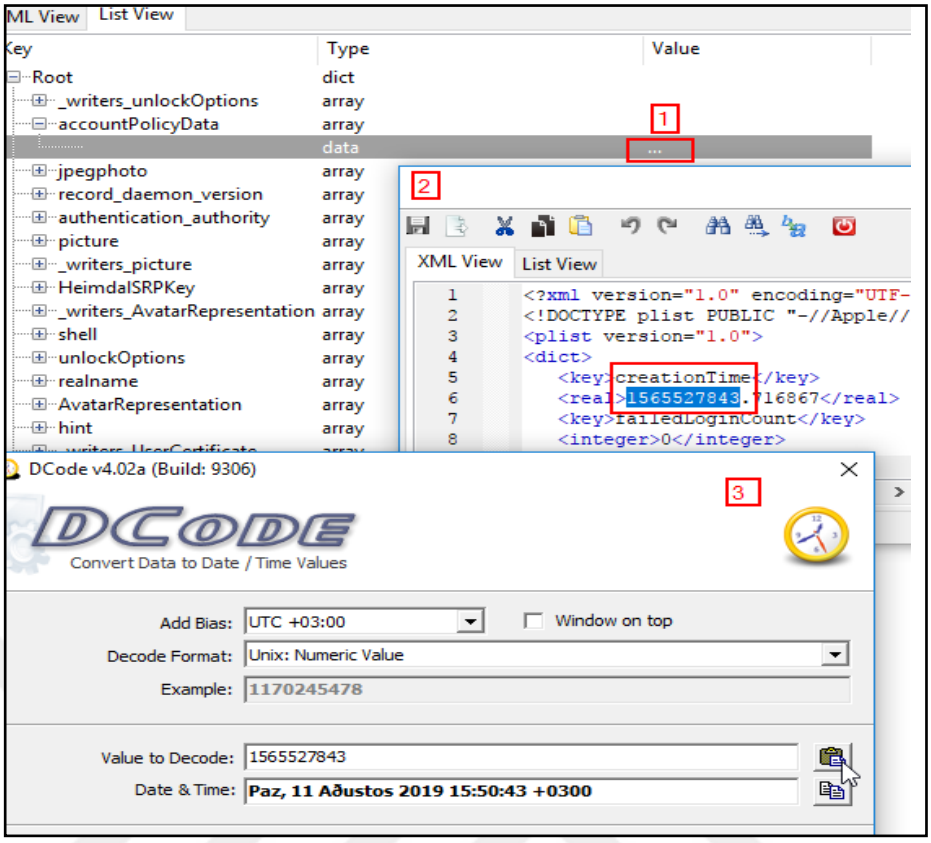
Şekil 3.6. Kullanıcıya ait ".plist" dosyasının incelenmesi.

Sanal disk dosyasının AXIOM yazılımı ile yapılan incelemesinde “Apple kişiler” bölümümde, kullanıcıların oluşturulma tarihlerinin yanlış olduğu, tüm kullanıcıları göstermediği ve gösterdiği her kullanıcı için aynı oluşturma tarihlerinin olduğu görülmüştür (Şekil 3.7).



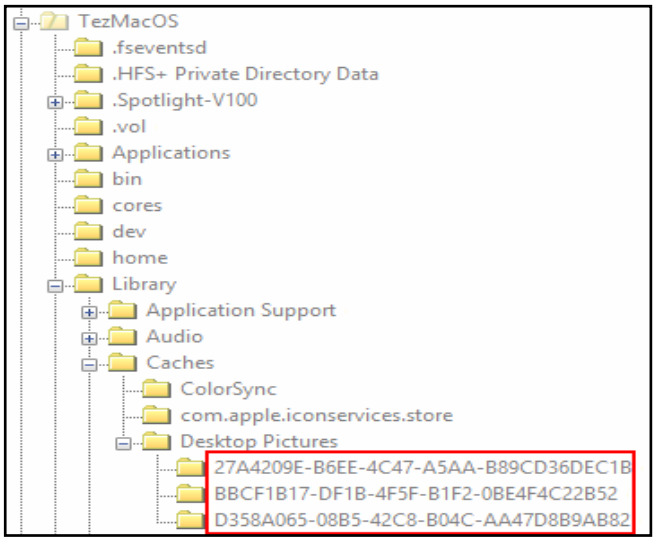
Şekil 3.7. AXIOM yazılımı “apple kişiler” görünümü.

Kullanıcıya ait .plist dosyası, plist Editör Pro ile incelendiğinde Şekil 3.8’de görüldüğü gibi “accountPolicyData” sekmesine tıklandığında üç nokta gözükmektedir. Burada üç noktaya çift tıklandığında karşımıza 2 numaralı pencere gelecektir. Burada ise kullanıcının oluşturma tarihinin epoch formatta olduğu görülmüştür. Söz konusu tarih 3 numaralı pencerede görüldüğü gibi Unix numeric okunabilir formata çevrilmiştir. (Şekil 3.8). Örnek olarak kullanıcılardan sadece bir tanesi gösterilmiştir.



Şekil 3.8. Kullanıcı oluşturma tarihinin hesaplanması.

Ayrıca kullanıcılar oluşturulduğunda "…\Library\Caches\Desktop Pictures\" konumu altında her kullanıcıya ait kullanıcı UUID adında klasörler oluştuğu görülmüştür (Şekil 3.9).



Şekil 3.9. Kullanıcılara ait UUID adında oluşan klasörler.

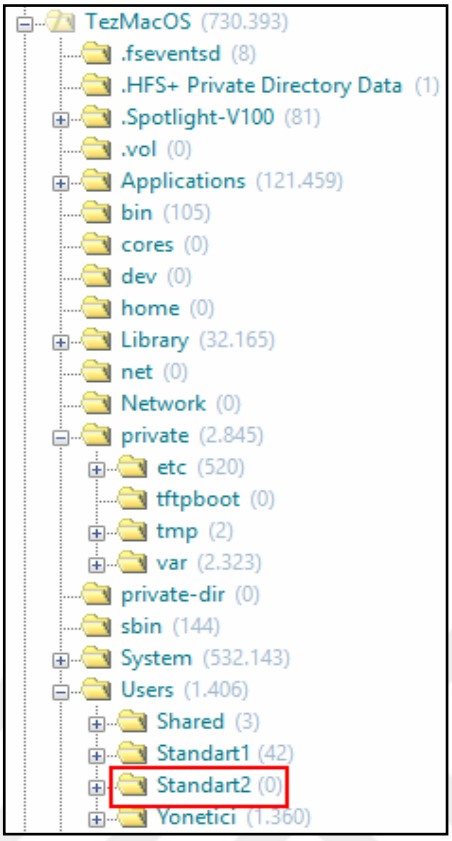
Tespit edilmesi hedeflenen mevcut kullanıcı isimleri, kullanıcılara ait parola ipuçları ve kullanıcıların oluşturulma tarihlerine ait kayıtlara ulaşılmıştır. Veri toplama aşamasında elde ettiğimiz veriler ile tespit edilen kayıtların doğruluğu görülmüştür. AXIOM yazılımı ile tespit edilen kullanıcı oluşturma tarihine ait kayıtlarının yanlış ve eksik olabileceği görülmüştür. Ek olarak her kullanıcıya ait kullanıcı UUID numarası tespit edilmiştir. Ancak oluşturulan kullanıcıların, hangi kullanıcı tarafından oluşturulduğu bilgisi tespit edilememiştir.

3.3. Silinen Kullanıcıya Ait Kayıtların Analizi

Üç adet kullanıcı oluşturulduktan sonra yönetici yetkisine sahip kullanıcı tarafından standart yetkiye sahip bir kullanıcı silinmiştir. Veri toplama aşamasında elde ettiğimiz veriler şunlardır:

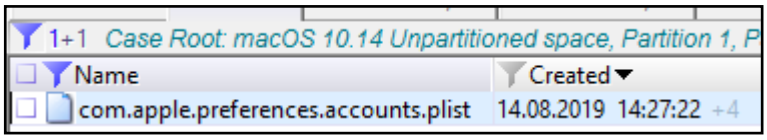
- "Standart2" isimli standart kullanıcı, "Yonetici" isimli yönetici tarafından tarih 14.08.2019 saat 13:27'de (UTC+3) silinmiştir.

İşlem sonrası sanal disk dosyasının "X-Ways" yazılımı ile yapılan incelemesinde mevcut kullanıcılara ait ana klasörlerin olduğu dizindeki Standart2 isimli klasörün kaldığı fakat içinin boş olduğu görülmüştür (Şekil 3.10).



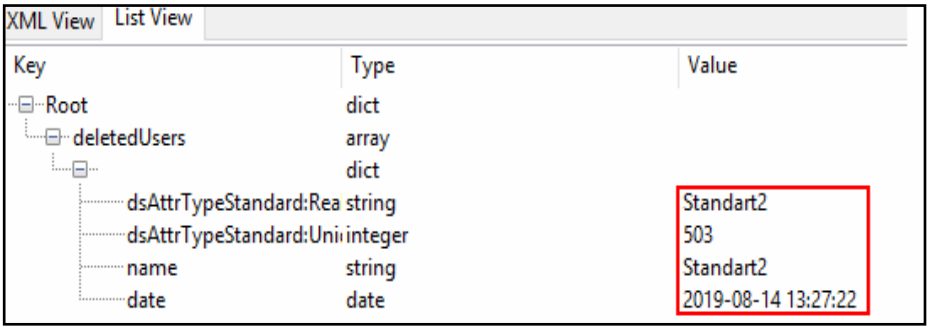
Şekil 3.10. Kullanıcı silindikten sonra kullanıcı ait ana dizin klasörleri.

Ayrıca kullanıcı silindikten sonra "…\Library\Preferences\" konumu altında oluşma tarihi UTC+4'e göre 14.08.2019 saat 14:27 olan "com.apple.preferences.accounts.plist" isimli dosyanın oluştuğu tespit edilmiştir (Şekil 3.11).



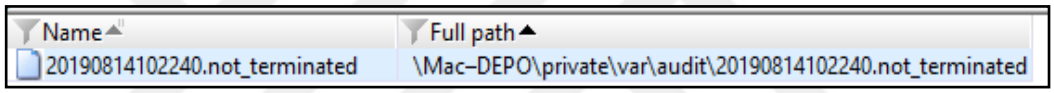
Şekil 3.11. "com.apple.preferences.accounts.plist" dosyasının oluşma tarihi.

Söz konusu dosyanın plist Editör Pro görüntüleyicisi ile yapılan analizinde silinen kullanıcıya ait kayıtlar tespit edilmiştir (Şekil 3.12). Kullanıcının silinme tarihi 14.08.2019 saat 13:27:22 olarak gözükmektedir.

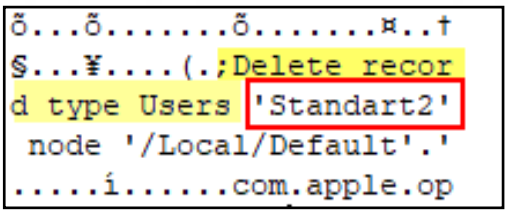


Şekil 3.12. Silinen kullanıcıya ait kayıtlar.

Yapılan kullanıcı silme işlemleri başka sanal makinelerde denenmiş ve her seferinde audit loglarının tutulduğu "…\private\var\audit" dizini altında silinme tarihi ile başlayan ve sonlandırılmamış log kaydının oluştuğu görülmüştür (Şekil 3.13). Söz konusu kayıtlar HXD hexeditör ile incelendiğinde "Delete record type Users" ile başlayan yapı tespit edilmiştir (Şekil 3.14).



Şekil 3.13. Kullanıcı silindikten sonra oluşan audit log dosyası.



Şekil 3.14. Audit log dosyası içerisinde silinen kullanıcıya ait kayıtlar.

Tespit edilmesi hedeflenen silinen kullanıcı ismi ve silme işlemine ait tarih-saat kayıtlarına ulaşılmıştır. Veri toplama aşamasında elde ettiğimiz veriler ile tespit edilen kayıtların doğruluğu görülmüştür. Silme işlemine ait tarih bilgisinin, tespit edilen .plist uzantılı dosya içerisinde UTC+3'e göre tutulduğu, aynı dosyanın X-Ways yazılımı ile incelendiğinde ise UTC+4'e göre gösterdiği görülmüştür. Ek olarak her silme işlemi gerçekleştirildiğinde log kaydı oluştuğu ve bu log kaydının binary formatta olduğu görülmüştür. Log kaydı HEX editör yardımıyla açılarak incelendiğinde tekrarlanan yapı tespit edilmiştir. Tekrarlanan bu yapıya göre anahtar kelime oluşturularak anahtar kelime araması ile silinen kullanıcılara ait kayıtların

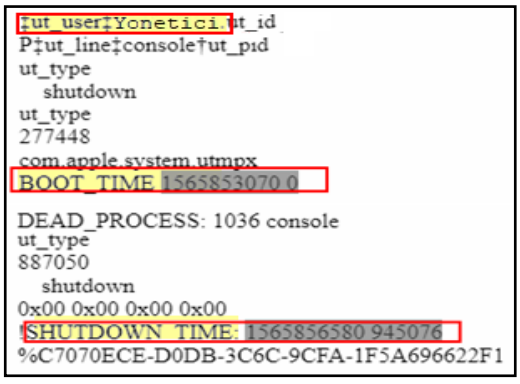
tespiti yapılabilir. Aynı zamanda log kaydı adının da silme işlemine ait tarih ile başladığı yani "20190814102240.not_terminated" olduğu gözükmektedir. Ancak silme işlemine ait saat bilgisi 13:27 olduğu için log kaydı adının "201908141327" ile başlaması beklenirken "201908141022" ile başladığı görülmüştür. Log kaydı adında bulunan tarih-saat, silime işlemine ait tam saati gösteremeyebilir. Silinen kullanıcıların, hangi kullanıcı tarafından silindiği bilgisi tespit edilememiştir.

3.4. Kullanıcıların Giriş-Çıkış İşlemleri Sonucunda Oluşan Kayıtların Analizi

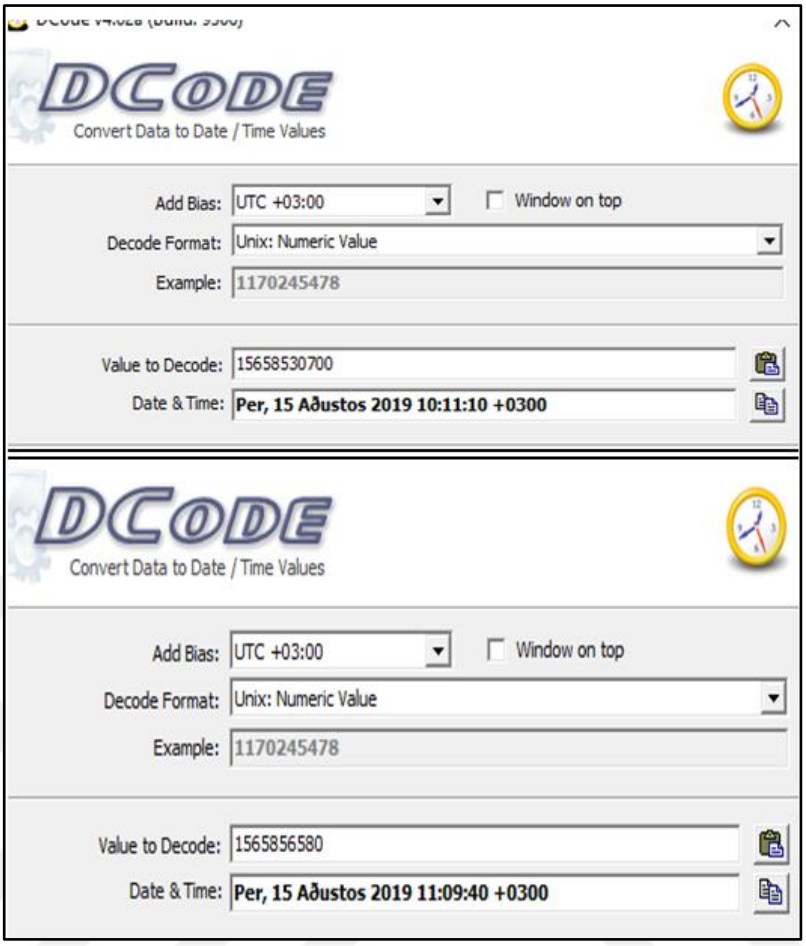
Kullanıcı ile oturum açılmış ve bir süre sonra oturum kapatılıştır. Veri toplama aşamasında elde ettiğimiz veriler şunlardır:

- "Yonetici" isimli kullanıcının oturumu, tarih 15.08.2019, saat 10:11'de (UTC+3) açılmıştır
- "Yonetici" isimli kullanıcının oturumu, tarih 15.08.2019 saat 11:09'da (UTC+3) kapatılmıştır.

İşlem sonrası yapılan analizde "…\private\var\log\asl\" konumu altında bulunan apple sistem günlüğünün oluştuğu görülmüştür. Söz konusu log kaydı HxD editör yardımıyla açıldığında tarih bilgilerinin Epoch format olarak tutulduğu tespit edilmiştir. (Şekil 3.15). Tespit edilen zaman bilgileri DCode yazılımı ile Unix numeric formata çevrilmiştir (Şekil 3.16).



Şekil 3.15. Yonetici isimli kullanıcının oturum açma-kapama zaman bilgileri.



Şekil 3.16. Tespit edilen oturum açma-kapama zaman bilgileri.

Tespit edilmesi hedeflenen kullanıcı oturum açama ve kapama işlemlerine ait tarih-saat kayıtlarına ulaşılmıştır. Veri toplama aşamasında elde ettiğimiz veriler ile tespit edilen kayıtların doğruluğu görülmüştür. Kullanıcı oturum açama ve kapama işlemleri başka sanal makinelerde denenmiş ve her seferinde log kayıtlarının oluştuğu görülmüştür. Birden fazla log kaydı oluşması durumunda tekrar eden yapı olan "BOOT_TIME" ve "SHUTDOWN_TIME" yapısına dikkat edilmesi gerekmektedir. Yine bu yapılar tekrar ettiği için anahtar kelime oluşturulup kolayca oturum açama ve kapama işlemlerine ait tarih-saat kayıtlarına erişilebilir. Log kayıtlarının HEX editör yardımıyla açılması ve tarih bilgilerinin okunabilir hale getirilmesi için Numeric formata çevrilmesi gerekmektedir.

3.5. Mac İşletim Sistemine Sahip Bilgisayarın Açma ve Kapama İşlemleri

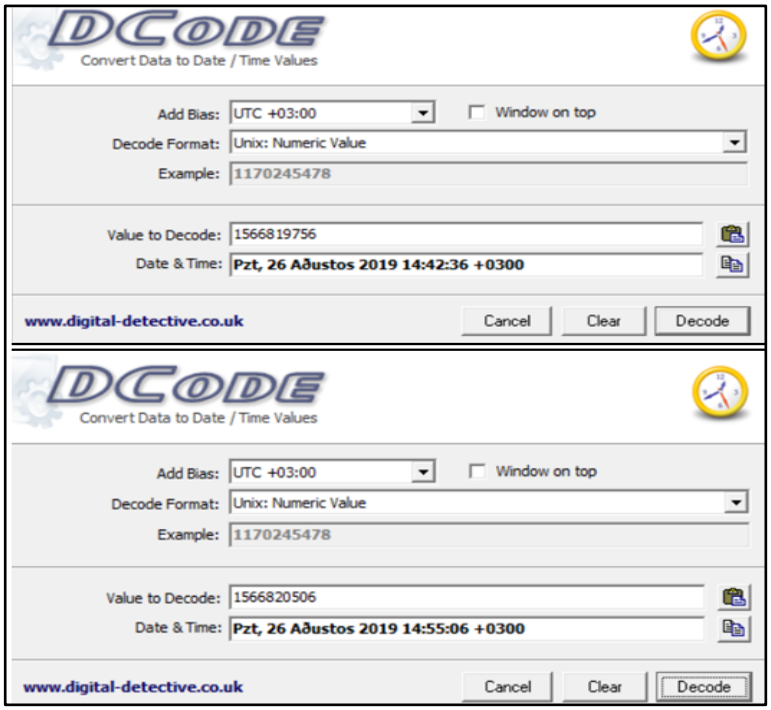
Bilgisayarın açma ve kapama bilgilerinin tespiti için MacOS işletim sistemine Macbook Pro bilgisayar ile açma ve kapama işlemleri gerçekleştirilmiştir. Veri toplama aşamasında elde ettiğimiz veriler şunlardır:

- Macbook Pro bilgisayar, tarih 26.08.2019, saat 14:42'de (UTC+3) açılmış ve 14:55'de (UTC+3) kapatılmıştır.
- Ardından BlackBag MacQuisition ile bilgisayarın imajı alınmıştır.

Alınan imajın yapılan analizinde "…\private\var\log\" konumu altında bulunan "system.log" isimli dosya HxD editör yardımıyla açıldığında içerisinde açma tarihi ve kapama tarih bilgilerinin Epoch format olarak tutulduğu tespit edilmiştir (Şekil 3.17). Tespit edilen zaman bilgileri DCode yazılımı ile Unix numeric formata çevrilmiştir (Şekil 3.18).

```
BOOT_TIME 1566819756 0Aug 26 14:42:44 localhost syslogd[36]:
consoleAug 26 14:55:06 TEZMACOS Mac shutdown[346]: SHUTDOWN_TIME: 1566820506 91561
```

Şekil 3.17. Bilgisayarın açma ve kapama zaman bilgileri.



Şekil 3.18. Tespit edilen bilgisayar açma-kapama zaman bilgileri.

Tespit edilmesi hedeflenen bilgisayarın açama ve kapama işlemlerine ait tarih-saat kayıtlarına ulaşılmıştır. Veri toplama aşamasında elde ettiğimiz veriler ile tespit edilen kayıtların doğruluğu görülmüştür. Uygulama sanal makineler ile de gerçekleştirildiğinde aynı sonucu vermektedir. Oturum açma ve kapamada olduğu gibi log kaydında tekrar eden yapı olan "BOOT_TIME" ve "SHUTDOWN_TIME" yapısı olduğu görülmektedir. Yine bu yapılar tekrar ettiği için anahtar kelime oluşturulup kolayca bilgisayar açama ve kapama işlemlerine ait tarih-saat kayıtlarına erişilebilir. Burada dikkat edilmesi gereken oturum açma-kapama tarihine ait bilgilerin "…\private\var\log\asl\" konumu altında, bilgisayar açma kapama-tarihine ait bilgilerin ise system.log içerisinde tutulduğudur. Log kayıtlarının HEX editör yardımıyla açılması ve tarih bilgilerinin okunabilir hale getirilmesi için Numeric formata çevrilmesi gerekmektedir.

3.6. Mac İşletim Sistemi Üzerinde Kullanıcı Tarafından Yapılan Tarih ve Saat Değişikliği İşlemleri

Kullanıcı tarafından gerçek sistem tarih ve saat ayarları değiştirilmiştir. Veri toplama aşamasında elde ettiğimiz veriler şunlardır:

- Macbook Pro bilgisayarın gerçek sistem tarih-saati 12.11.2019 10:45 (UTC+3),
- Kullanıcı tarafından sistem tarih-saati 14.08.2019 11:13 (UTC+3) olarak değiştirilmiştir.
- Ardından BlackBag MacQuisition ile bilgisayarın imajı alınmıştır.

Alınan imajın yapılan analizinde, "private/var/db/timed" altındaki "com.apple.timed.plist" yapılandırma dosyasında gerçek sistem zaman bilgisinin bulunduğu görülmüştür. Fakat sistem tarihi geriye alındığında "…/private/var/db/timed/Library/Preferences" konumu altında bir tane daha "com.apple.timed.plist" dosyası oluştuğu, bu dosya da değiştirilen zaman ve tarih bilgisini gösterdiği görülmüştür. Söz konusu 2 dosyanın AXIOM yazılımı ile yapılan incelemesinde asıl sistem saati ve geriye alınan sistem saati tespit edilmiştir (Şekil 3.19).

Şekil 3.19. Zaman değişikliği ile ilgili kayıtlar.

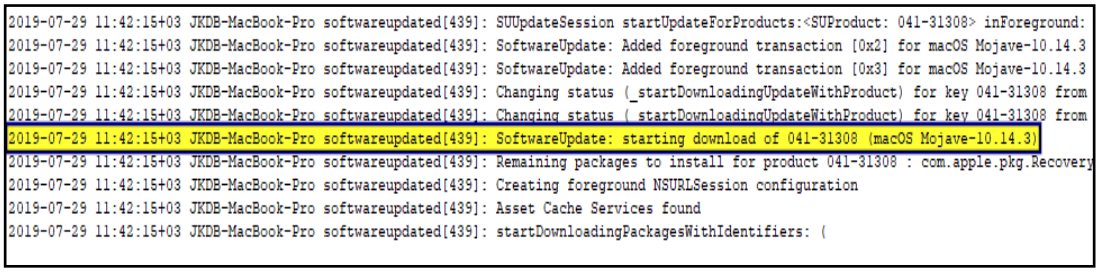
Tespit edilmesi hedeflenen bilgisayarın sistem tarih-saati değişikliğine ait kayıtlara ulaşılmıştır. Veri toplama aşamasında elde ettiğimiz veriler ile tespit edilen kayıtların doğruluğu görülmüştür. Burada dikkat edilmesi gereken iki dosyanın da aynı isimli olduğu fakat bulunduğu dosya konumlarının farklı olduğudur.

3.7. Sistem Güncelleme Bilgilerinin Tespiti

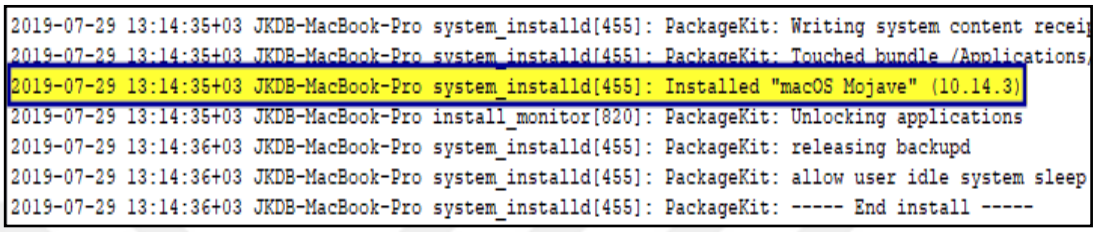
Macbook Pro bilgisayar sürümü güncelleştirilmiştir. Veri toplama aşamasında elde ettiğimiz veriler şunlardır:

- Macbook Pro bilgisayarın mevcut sürümü MacOS 10.13 iken tarih 29.07.2019 saat 11:42'de (UTC+3) güncelleme yapılarak MacOS 10.14'e yükseltilmiştir.
- Ardından BlackBag MacQuisition ile bilgisayarın imajı alınmıştır.

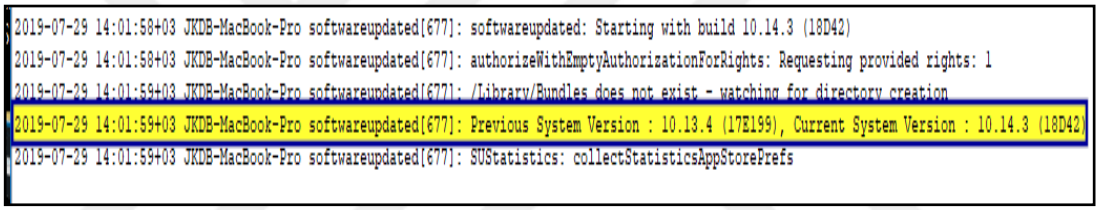
Alınan imajın yapılan incelemesinde; "…\var\log" konumu altında bulunan "install.log" isimli dosya içerisinde yüklenecek olan yeni sürümün indirilme zamanı bilgisi, güncelleme işleminin yapıldığı zaman bilgisi ve güncelleme yapılmadan önceki işletim sistemi versiyon sürümü ile güncelleme yapıldıktan sonraki versiyon sürümleri bilgisi tespit edilmiştir (Şekil 3.20, Şekil 3.21, Şekil 3.22).



Şekil 3.20. Yüklenecek olan "MacOS Mojave-10.14.3" sürümünün indirilme zaman bilgisi.



Şekil 3.21. Güncelleme işleminin yapıldığı zaman bilgisi.



Şekil 3.22. Güncelleme yapılmadan önceki versiyon sürümü ve güncelleme yapıldıktan sonraki versiyon sürümleri bilgisi.

Tespit edilmesi hedeflenen bilgisayarın yeni sürümün indirilme zamanı, güncelleme işleminin yapıldığı zaman bilgisi ve güncelleme yapılmadan önceki işletim sistemi versiyon sürümü ile güncelleme yapıldıktan sonraki versiyon bilgilerine ait kayıtlara ulaşılmıştır. Veri toplama aşamasında elde ettiğimiz veriler ile tespit edilen kayıtların doğruluğu görülmüştür. Log kaydında paketlerin yüklenmesi gibi her adımda kayıt tutulduğu görülmüştür. Fazla bilgilerin içerisinden tespit edilmesi hedeflenen kayıtlara, aşağıda belirlenen yapılar aratılarak kolayca ulaşılabilir.

- SoftwareUpdate: starting download of + Güncellenen versiyon bilgisi
- Installed "güncellenen versiyon bilgisi"
- Previous System Version: Eski versiyon bilgisi, Current System Version Güncellenen versiyon bilgisi

3.8. Ağ Yapılandırması, Ağ Üzerinden Erişim, Kablosuz Erişim Noktalarına Yapılan Bağlantı İşlemleri

iOS işletim sistemine sahip telefonlar ile toplam 5 adet uygulama, yazıcı ile de bir adet uygulama gerçekleştirilmiştir. Veri toplama aşamasında elde ettiğimiz veriler Çizelge 3.1.'de verilmiştir.

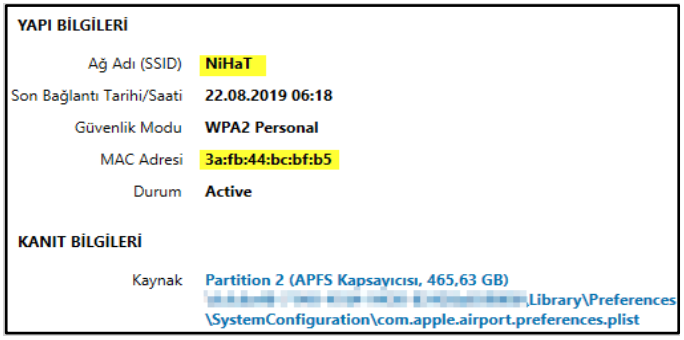
Çizelge 3.1. Yapılan uygulamaların, veri toplama aşamasında elde edilen verileri.

	Sıra No	Marka Model	Cihaz Adı	Bağlantı Türü	MAC Adresi	Açıklama
iOS Uygulama1	I1	iPhone A1778	Nihat	USB & Wi-Fi	98:00:C6: 42:A5:03	"Wi-Fi Ağını Anımsa" seçeneği aktif edilmiştir.
iOS Uygulama2	I2	iPhone A1688	Mürsel	USB & Wi-Fi	B4:9C:DF:01: B3:DD	"Wi-Fi Ağını Anımsa" seçeneği aktif edilmiştir
iOS Uygulama3	I3	iPhone A1688	Salih İphone'u	Wi-Fi	58:E2:8F:CB: 87:D4	"Wi-Fi Ağını Anımsa" seçeneği pasif edilmiştir
iOS Uygulama4	I4	iPhone A1786	Yiphone	Wi-Fi	78:4F:43: 28:B3:7F	"Wi-Fi Ağını Anımsa" seçeneği pasif edilmiştir
iOS Uygulama5	I5	iPhone A1901	Ömer	USB	3C:2E:FF:41: 60:A0	Sadece USB üzerinden bağlantı sağlanmıştır.
Yazıcı Uygulama	-	HP LaserJet MFP M22fdw	DIRECT -e4-HP M227f LaserJet	Wi-Fi	B0:52:16:A1: 88:E4	"Wi-Fi Ağını Anımsa" seçeneği pasif edilmiştir

Kurulan her bağlantıların ardından BlackBag MacQuisition ile bilgisayarın imajı alınmıştır. Alınan imajların yapılan incelemesinde;

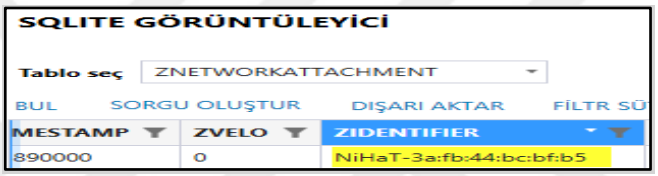
3.8.1. iOS uygulama 1

Çizelge 3.1'in iOS Uygulama 1 satırında belirtildiği gibi cep telefonu ile bağlantı kurulmuştur. Ardından bilgisayarın imajı alınmış ve alınan imajın AXIOM yazılımı ile analizi sonucu; "com.apple.airport.preferences.plist" dosyasında; cihaz adı, bağlantı tarihi ve MAC adresi bulunduğu görülmüştür. Ancak buradaki MAC adresi, telefonun kendi MAC adresinden tamamen farklı olduğu görülmüştür (Şekil 3.23).



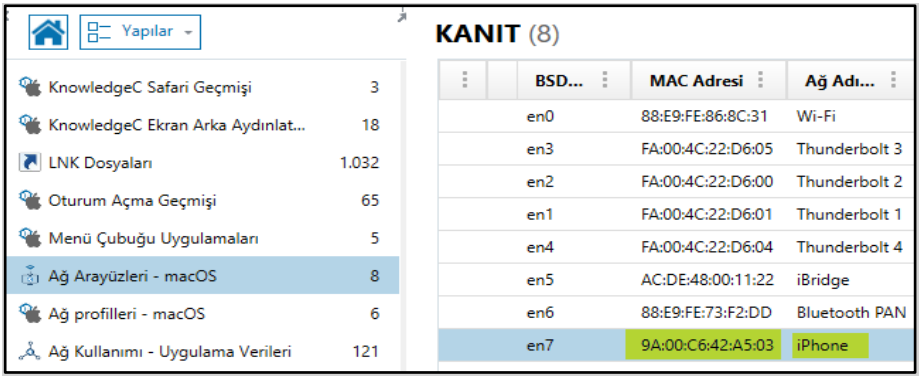
Şekil 3.23. "com.apple.airport.preferences.plist" dosyası-1.

İmaj içerisinde yer alan "netusage.sqlite" dosyasının AXIOM yazılımı ile yapılan analizinde ise yine MAC adresinin kullanılan telefonun kendi MAC adresinden tamamen farklı olduğu görülmüştür (Şekil 3.24).



Şekil 3.24. "netusage.sqlite" dosyasının görünümü-1.

İmajın AXIOM yazılımı ile ağ arayüzleri yapı görüntüsüne *(kaynak dosyası NetworkInterfaces.plist)* bakıldığında ise 8 adet ağ arayüz kaydı görülmüştür. "en7" numaralı kaydın analizinde ürün adı iPhone olan cihazın MAC adresi 98:00:C6:42:A5:03 olması gerekirken 9A:00:C6:42:A5:03 olduğu görülmüştür (Şekil 3.25).

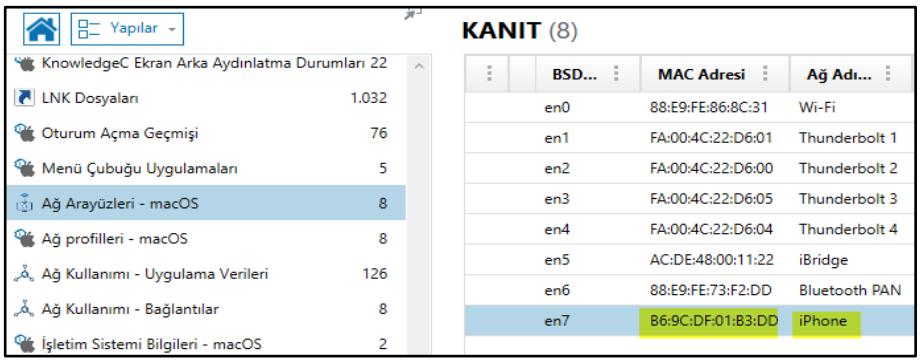


Şekil 3.25. Ağ arayüzleri yapı görüntüsü-1.

iOS uygulama 1 sonucunda; “com.apple.airport.preferences.plist” ve “netusage.sqlite” dosyalarında tespit edilen MAC adresinin, kullanılan telefonun MAC adresinden **tamamen farklı** olabileceği görülmüştür. “NetworkInterfaces.plist” dosyasında ise kullanılan iPhone marka telefonun ağ isim bilgisinin olmadığı ve MAC adresinin ilk byte değeri veri toplama adımında görüldüğü üzere “98” olması gerekirken, tespit edilen değerin 98’in iki byte fazlası “9A” olduğu görülmüştür.

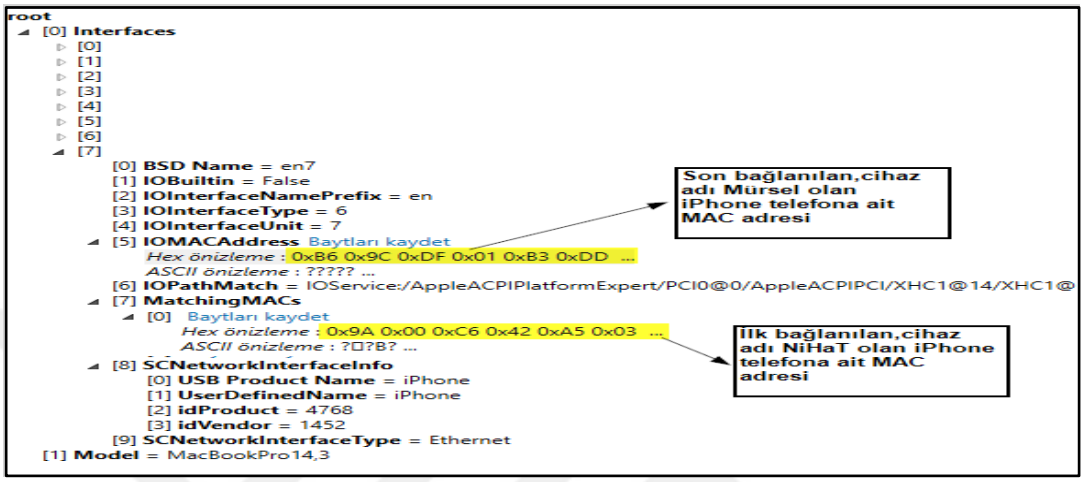
3.8.2. iOS uygulama 2

iOS Uygulama 1 sonucunda elde edilen bilgilerin teyit edilmesi amacıyla Çizelge 3.1’in iOS Uygulama 2 satırında belirtildiği gibi cep telefonu ile bağlantı kurulmuştur. Ardından bilgisayarın imajı alınmış ve alınan imajın incelenmesi sonucu; I2 numaralı telefon için; “com.apple.airport.preferences.plist”, “netusage.sqlite” dosyalarında yer alan MAC adresinin yine kullanılan telefonun MAC adresinden tamamen **farklı** olduğu görülmüştür. I2 numaralı telefon USB ile de bağlandığı için “NetworkInterfaces.plist” dosyasındaki kayıt sayısının artması beklenirken, imajın AXIOM yazılımı ile incelenmesi sonucu Ağ arayüzleri yapı görünümünde kayıt sayısının değişmediği ve yine 8 adet olduğu görülmüştür. “en7” numaralı iPhone marka telefona ait kayda bakıldığında MAC adresinin B4:9C:DF:01:B3:DD olması gerekirken B6:9C:DF:01:B3:DD olduğu görülmektedir (Şekil 3.26). **iOS Uygulama** 1’de bağlanılan telefona ait herhangi bilgi **bulunmamaktadır.**



Şekil 3.26. Ağ arayüzleri yapı görüntüsü-2.

"NetworkInterfaces.plist" dosyasının Plist görüntüleyicisi ile manuel olarak yapılan analizinde ise; "en7" numaralı kaydın "MatchingMACs" kısmında daha önce bağlanılan I1 numaralı telefona ait MAC adresi olduğu tespit edilmiştir. Burada da MAC adresinin ilk byte değeri 2 fazla olarak gösterilmektedir (Şekil 3.27).



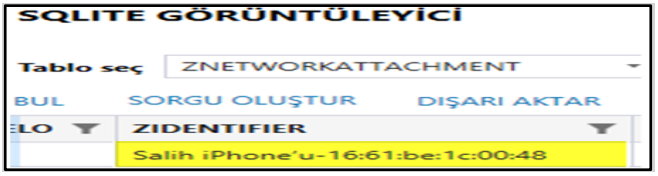
Şekil 3.27. "NetworkInterfaces.plist" dosyası-1.

iOS uygulama 2 sonucunda; "com.apple.airport.preferences.plist", "netusage.sqlite" ve "NetworkInterfaces.plist" dosyalarındaki kayıtlar incelendiğinde iOS Uygulama 1 sonucunda elde edilen bilgiler teyit edilmiştir. AXIOM yazılımı ile ağ arayüzleri yapı görüntüsüne bakıldığında, daha önce USB ile ağ bağlantısı sağlanan iPhone marka telefona ait herhangi bir kayıt olmadığı, sadece bağlanılan son iPhone telefona ait kayıt olduğu görülmüştür. Ancak ağ arayüzleri kaynak dosyası yani "NetworkInterfaces.plist" dosyasının Plist görüntüleyicisi ile manuel olarak yapılan analizinde bilgisayara USB ile ağ bağlantısı sağlanan tüm iPhone marka telefonlara ait MAC adresi bilgisinin bulunabileceği görülmüştür.

3.8.3. iOS uygulama 3

Bir iOS işletim sistemine sahip cep telefonun **sadece** Wi-Fi üzerinden, "Wi-Fi Ağını Anımsa" seçeneği **pasif** edilerek bilgisayar ile bağlantı kurulmasının, sonuçları nasıl etkilediğini görmek amacıyla Çizelge 3.1'in iOS Uygulama 3 satırında belirtildiği gibi cep telefonu ile bağlantı kurulmuştur. Ardından bilgisayarın imajı

alınmış ve alınan imajın incelenmesi sonucu; “com.apple.airport.preferences.plist” ve “NetworkInterfaces.plist” isimli dosyalarda I3 numaralı telefona ait kayıt tespit edilememiştir. “netusage.sqlite” dosyasının yapılan analizinde ise; I3 numaralı telefona ait MAC adresi kaydı incelendiğinde telefonun kendi MAC adreslerinden tamamen **farklı** olduğu görülmüştür (Şekil 3.28).



Şekil 3.28. “netusage.sqlite” dosyasının görünümü-2.

iOS Uygulama 3 Sonucunda; “com.apple.airport.preferences.plist” dosyasında ağ anımsatılmadığı için ve **“**NetworkInterfaces.plist” isimli dosyada USB ile bağlantı kurulmadığı için I3 numaralı telefona ait kayıt tespit edilememiştir. “Wi-Fi Ağını Anımsa” seçeneği **aktif** ya da **pasif** edilse de “netusage.sqlite” dosyasında yer alan MAC adresi kaydının kullanılan telefonun MAC adresi kaydından tamamen **farklı** olabileceği görülmüştür.

3.8.4**. iOS uygulama 4**

iOS Uygulama 3 sonucunda elde edilen bilgilerin teyit edilmesi amacıyla **sadece** Wi-Fi üzerinden, “Wi-Fi ağını anımsa” seçeneği pasif edilerek Çizelge 3.1’in iOS Uygulama 4 satırında belirtildiği gibi cep telefonu ile bağlantı kurulmuş ardından bilgisayarın imajı alınmıştır. Alınan imajın incelenmesi sonucu; “netusage.sqlite” dosyasında yer alan MAC adresi kaydı kullanılan telefonun MAC adresi kaydından tamamen **farklı** olduğu görülmüş ve iOS Uygulama 3 sonucunda elde edilen tüm sonuçlar teyit edilmiştir.

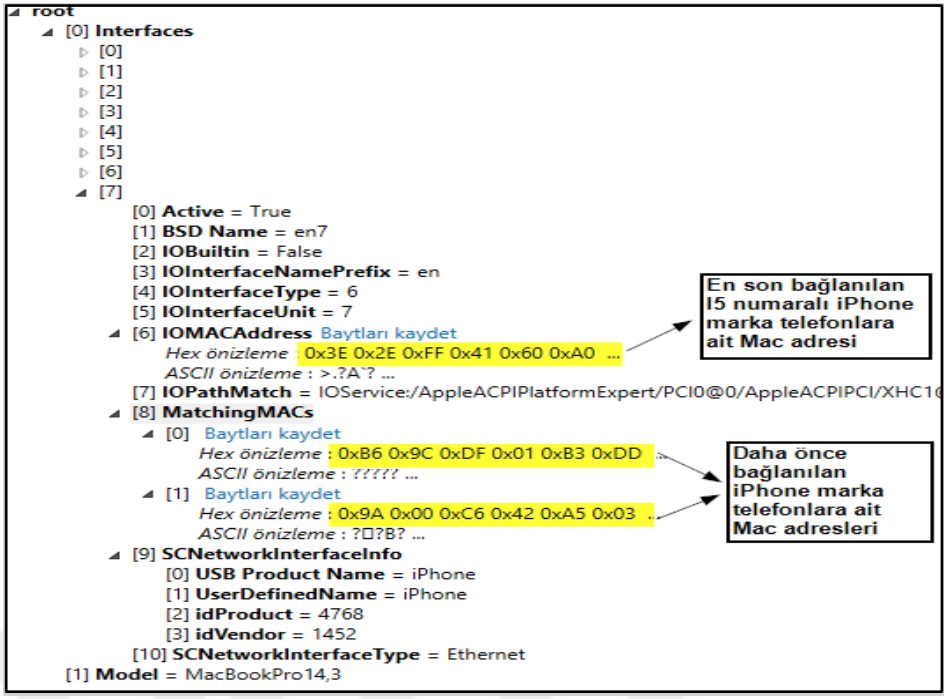
3.8.5. iOS uygulama 5

MAC bilgisayara iOS işletim sistemine sahip cep telefonu **sadece** USB ile bağlanıldığında "NetworkInterfaces.plist" dosyasında iOS Uygulama 1 ve iOS Uygulama 2'ye göre herhangi bir değişiklik olup olmayacağının tespiti için Çizelge 3.1'in iOS Uygulama 5 satırında belirtildiği gibi cep telefonu ile bağlantı kurularak internet'e erişim sağlanmıştır. Ardından bilgisayarın imajı alınmış ve alınan imajın AXIOM yazılımı ile incelenmesi sonucu Ağ arayüzleri kayıt sayısının yani "NetworkInterfaces.plist" dosyasının kayıt sayısının değişmediği ve yine 8 adet olduğu görülmüştür. iOS Uygulama 1 ve iOS Uygulama 2'de bağlanılan önceki iPhone marka telefonlara ait kayıt **gözükmemektedir** (Şekil 3.29).

BSD...	MAC Adresi	Ağ T...	Ağ Adı...
en0	88:E9:FE:86:8C:31	IEEE80211	Wi-Fi
en1	FA:00:4C:22:D6:01	Ethernet	Thunderbolt 1
en2	FA:00:4C:22:D6:00	Ethernet	Thunderbolt 2
en3	FA:00:4C:22:D6:05	Ethernet	Thunderbolt 3
en4	FA:00:4C:22:D6:04	Ethernet	Thunderbolt 4
en5	AC:DE:48:00:11:22	Ethernet	iBridge
en6	88:E9:FE:73:F2:DD	Ethernet	Bluetooth PAN
en7	3E:2E:FF:41:60:A0	Ethernet	iPhone

Şekil 3.29. Ağ arayüzleri yapı görüntüsü-3.

"NetworkInterfaces.plist" dosyasının Plist görüntüleyicisi ile manuel olarak yapılan analizinde ise USB ile ağ bağlantısı sağlanan tüm iPhone marka telefonlara ait MAC adresi bilgilerine ulaşılmıştır (Şekil 3.30).



Şekil 3.30. "NetworkInterfaces.plist" dosyası-2.

iOS uygulama 5 sonucunda; telefonun sadece USB ile bağlanılsa da bilgisayarın imajı AXIOM yazılımı ile incelenmesi sonucu Ağ arayüzleri yapı görüntüsünde daha önce USB ile bağlanılan iPhone marka telefolara ait herhangi bir kayıt olmadığı, **sadece** USB ile ağ bağlantısı sağlanan son iPhone telefona ait kayıt olduğu görülmüş olup NetworkInterfaces.plist dosyası için **iOS Uygulama 2**'de elde edilen bilgiler teyit edilmiştir.

iOS işletim sistemine sahip cep telefonları ile yapılan uygulamalar sonucunda;

- USB ile bağlanılan iOS işletim sistemine sahip telefonlar için; "NetworkInterfaces.plist" dosyasında yer alan MAC adresinin ilk byte değeri, telefonun kendi Wi-Fi MAC adresinin ilk byte değerinden 2 fazla olabileceği görülmüştür.
- "NetworkInterfaces.plist" dosyasında yer alan, ürün adı iPhone olan cihazlara ait MAC adresi kayıtlarının ilk byte değerinden 2 çıkartıldığında, telefonun kendi MAC adresi tespit edilmiş olur. Burada elde edilen MAC adresinin ilk üç byte'ı, internet ortamında "MAC adresi-üretici firma" eşleştiren veri tabanı ile sorgulatıldığında, Apple üretici firması ile eşleşme olup olmadığı teyit edilmesi önerilir.

- NetworkInterfaces.plist" dosyasının AXIOM yazılımı ile ağ arayüzleri yapı görüntüsüne bakıldığında, **sadece** en son bağlanılan iOS işletim sistemine sahip telefona ait kaydı tuttuğu, her yeni bağlantıda kayıt sayısının **değişmediği** görülmüştür. Bu dosyanın ayrıca manuel olarak incelenmesi önerilir.
- Wi-Fi ile bağlanılma durumunda; "com.apple.airport.preferences.plist" ve **"**netusage.sqlite" dosyasında yer alan tüm iOS işletim sistemine sahip telefonlara ait MAC adresi kayıtlarının, telefonun kendi MAC adresinden tamamen farklı olabildiği görülmüştür. Raporlama aşamasında bu durum belirtilebilir. MAC adresi tespit edilemeyen bu telefonların MAC adresleri imaj içerisinde anahtar kelime olarak aratılmış ancak bulunamamıştır.

3.8.6. Yazıcı ile Yapılan Uygulama

Macbook Pro bilgisayar ile Wi-Fi üzerinden HP marka LaserJet MFP M22fdw model yazıcıya "DIRECT-e4-HP M227f LaserJet" ağ adı ile bağlantı kurulmuştur. Ardından yazdırma işlemi gerçekleştirilmiştir. İşlemlerin arkasından, BlackBag MacQuisition ile bilgisayarın imajı alınmıştır. Alınan imajın yapılan incelemesinde;

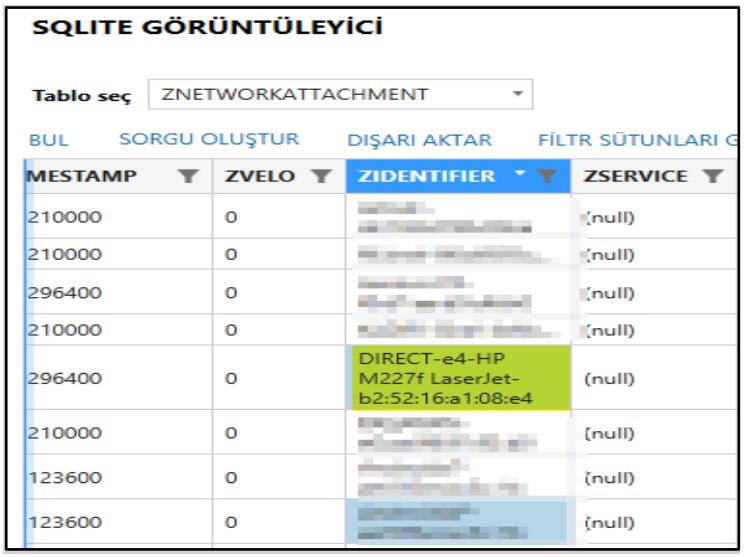
"…\Library\Preferences\" konumu altında "org.cups.printers.plist" dosyası içerisinde kullanılan yazıcıya ait bilgiler tespit edilmiştir. İsim ve model dışında "device-uri" kısmında yazıcının Mac adresi tespit edilmiştir (Şekil 3.31).

Şekil 3.31.“ Wi-Fi ile bağlanılan yazıcı için elde edilen bilgiler.

Ancak Şekil 3.31’de tespit edilen MAC adresinin, yazıcıya ait **kablolu bağlantı** MAC adresi olduğu görülmüştür.

Kablosuz MAC adresinin tespiti amacıyla .“…\Library\Preferences\SystemConfiguration” konumu altında “com.apple.airport.preferences.plist” dosyası incelendiğinde ise bu yazıcıya ait herhangi bir veri tespit edilememiştir.

“…\private\var\networkd\” konumu altında bulunan “netusage.sqlite” dosyasının yapılan analizinde Wi-Fi üzerinden bağlantı kurulan HP marka yazıcıya ait bilgiler olduğu görülmüştür. Yazıcının kablosuz bağlantı MAC adresi gerçekte “**b0**:52:16:a1:**88**:e4” iken, bu dosyada **b2**:52:16:a1:**08**:e4 olarak gözükmektedir. (Şekil 3.32).



Şekil 3.32. "netusage.sqlite" dosyasının görünümü-3.

Yazıcı ile yapılan uygulama sonucunda; "com.apple.airport.preferences.plist" dosyasında ağ anımsatılmadığı için yazıcıya ait Mac adresi bilgisinin bulunmadığı görülmüştür. "netusage.sqlite" dosyasında bulunan Mac adresi bilgisinin ise ilk hanesi ve dördüncü hanesinin yanlış olabileceği görülmüştür. İmaj içerisinde doğru Mac adresi anahtar kelime olarak aratılmış ancak bulunamamıştır.

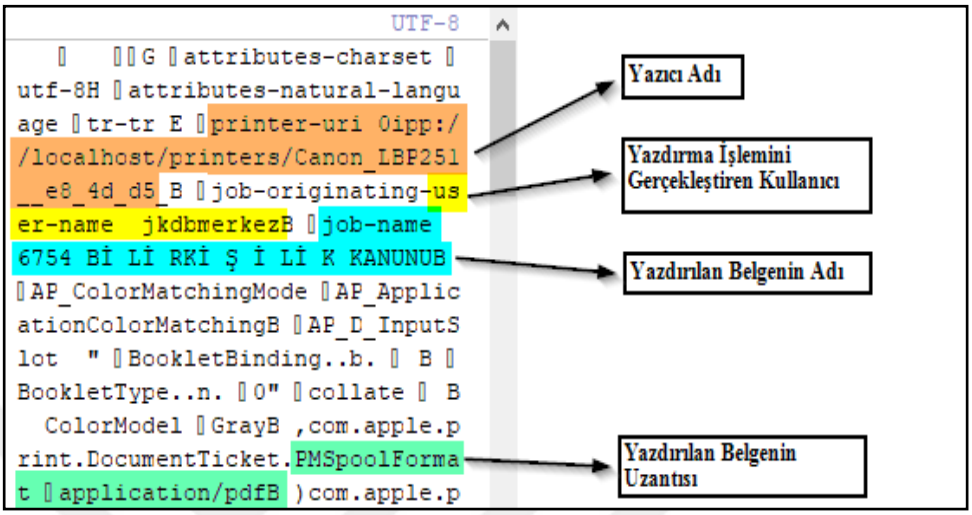
3.9. Yazıcıdan Çıktı Alınması

Macbook Pro bilgisayar ile Wi-Fi üzerinden yazıcıya bağlanılarak bir dosya yazdırılmıştır. Veri toplama aşamasında elde ettiğimiz veriler;

- Canon marka LBP251 model yazıcı ile bağlantı kurularak "Bilirkişilik Kanunu.pdf" dosyası 30.10.2019 tarihinde saat 16:45'de (UTC+3) yazdırılmıştır.
- Ardından BlackBag MacQuisition ile bilgisayarın imajı alınmıştır.

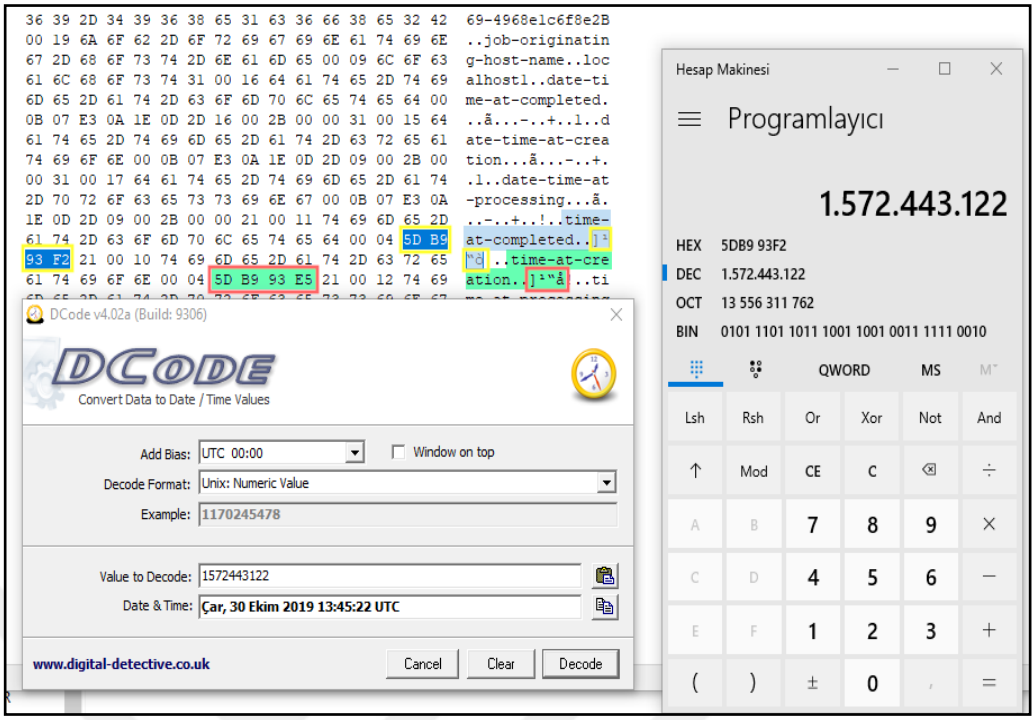
Alınan imajın yapılan incelemesinde; Mac işletim sistemi CUPS (Genel UNIX yazdırma sistemi) olarak adlandırdığı dosyaları kullanılır. CUPS, yazdırdığı her iş için tam sayı değerine göre sıralayarak işleri "…\private\var\spool\cups\" dizinine kaydeder. Bu dizin altında yazdırılan işin tamsayı değerini temsil ettiği "cXXXXX" sözdizimini kullanan kontrol dosyaları vardır. Burada söz dizimindeki 00001 ibaresinin ilk işi temsil ettiği görülmüştür.

Kontrol dosyalarının yapılan analizinde; dosyanın ne zaman yazdırıldığı, dokümanın tipi, yazıcı adı ve yazdırma işini yapan kullanıcı adı bilgileri tespit edilmiştir (Şekil 3.33).



Şekil 3.33. "c00001" kontrol dosyasından elde edilen bilgiler-1.

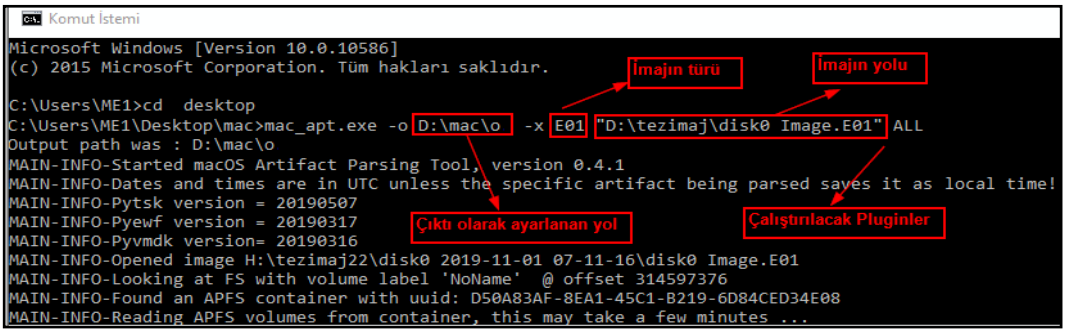
Aynı zamanda bu kontrol dosyalarının yapılan analizinde; "time-at-completed" ibaresinden sonraki ilk iki byte boş bırakıldıktan sonra gelen 4 byte'ın tarih saat bilgisini tuttuğu tespit edilmiştir. HEX değerleri aşağıdaki resimde gösterildiği gibi hesap makinesi aracılığı ile Decimal değerine dönüştürülmüştür. Böylece zaman bilgisi epoch formata dönüştürülmüştür. Elde edilen Decimal değeri ise DCode programı ile Unix numeric tarih saat formatı UTC+0'a dönüştürülerek yazıcıdan çıktı alınma zamanı tespit edilmiştir (Şekil 3.34).



Şekil 3.34. "c00001" kontrol dosyasından elde edilen bilgiler-2.

Yapılan literatür taramasında, yazdırılan belge eğer PostScript sürücüsü kullanılarak basılmış ise belgenin aynı kontrol numarasını kullanan ancak "c" harfi yerine "d" harfi ile başlayan kontrol dosyasını "…\private\var\spool\cups\" dizinine kaydettiğinden ve bu dosyanın yazdırılan belgenin bir kopyası olduğundan bahsedilmiştir (Garijo, 2015).

Alınan imaj, "mac_apt.exe" ile çalıştırıldığında çıktılar arasında yukarıda bahsedilen "d" harfi ile başlayan dosyaya yani yazdırılan belgenin kendisine ulaşılmıştır. Mac_apt.exe aşağıdaki gibi çalıştırılmıştır (Şekil 3.35).



Şekil 3.35. Mac_apt.exe yazılımının çalıştırılması

"Mac_apt.exe" programının çalıştırılması sonucu "…\Export\PRINTJOBS" konumu altında yazdırılan dosyaya yani "d00001-001" dosyasına erişilmiştir (Şekil 3.36).

Şekil 3.36. Mac_apt.exe'nin çalıştırılması sonucu PRINTJOBS klasörü altında oluşan dosyalar ve yazdırılan dosyanın ham hali.

Tespit edilmesi hedeflenen, çıktı alma işlemi gerçekleştirilen yazıcı marka-modeli, yazdırılan belgenin ham hali ve ismi, yazdırma işlemi tarih-saat bilgisine ait kayıtlara ulaşılmıştır. Veri toplama aşamasında elde ettiğimiz veriler ile tespit edilen kayıtların doğruluğu görülmüştür. Burada "cXXXXX" kontrol dosyası binary formatta olduğu görülmüş olup bu dosya HEX editör yardımıyla açılabilir. Bu dosyadaki tarih-saat bilgisinin byte değerinden epoch zaman formatına, epoch zaman formatından da okunabilir Unix numeric formata nasıl dönüştürüleceği gösterilmiştir.

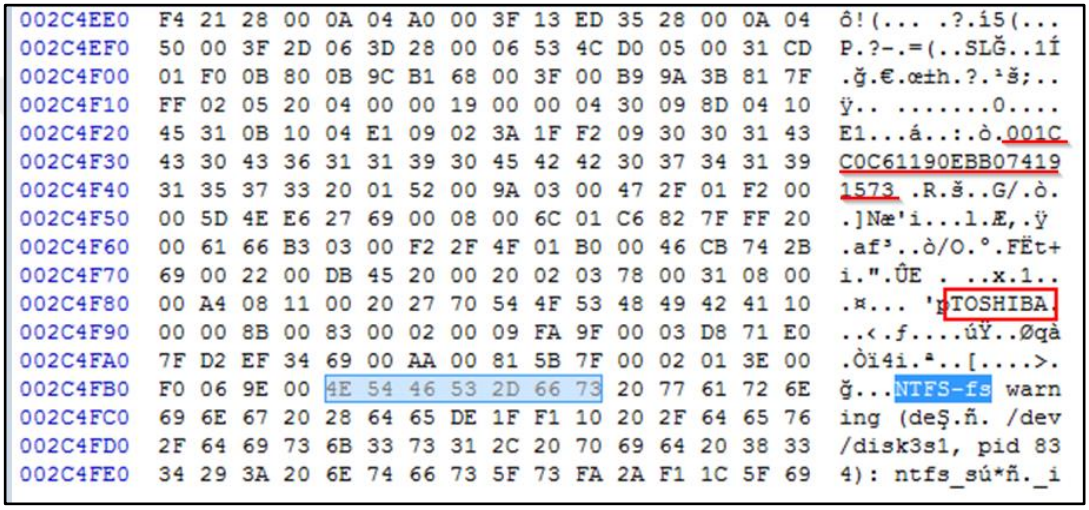
3.10. Bilgisayara Takılan Harici Veri Depolama Cihazlarına Ait Kayıtların Tespiti

Bilgisayara harici veri depolama cihazları takılarak bu cihazlar üzerinden dosya erişimi sağlanmıştır. Veri toplama aşamasında elde ettiğimiz veriler;

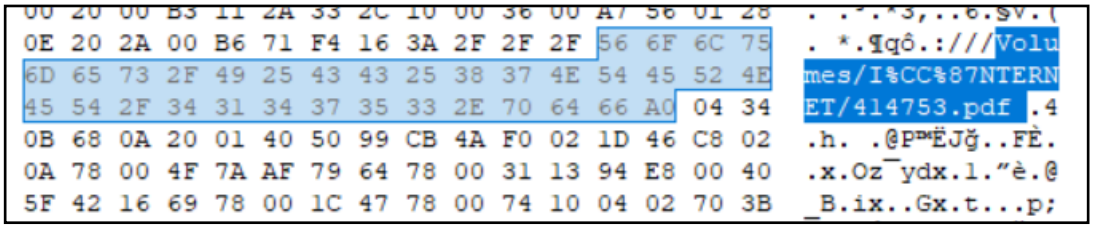
- "Yonetici" isimli kullanıcı ile oturum açılarak, Toshiba marka "001CC0C61190EBB0 74191573" yazılımsal seri numaralı USB bellek ve seri numarası atanmamış İnternet isimli USB bellek takılmıştır.
- İnternet isimli USB bellek üzerinden "414753.pdf" isimli dosyaya erişilmiştir.

- Boş CD takılarak içerisine dosya yazdırılmış ve CD'nin isimi "Macforensic" olarak girilmiştir.
- BlackBag MacQuisition ile bilgisayarın imajı alınmıştır.

Alınan imajın yapılan incelemesinde "…\private\var\db\diagnostics\Persist\ 0000000000000005.tracev3" dosyası içerisinde USB belleğe ait seri numarası, adı, dosyalama sistemi tespit edilmiştir (Şekil 3.37). Aynı zamanda bu dosya içerisinde İnternet isimli USB üzerinden erişilen dosya bilgisi tespit edilmiştir (Şekil 3.38).

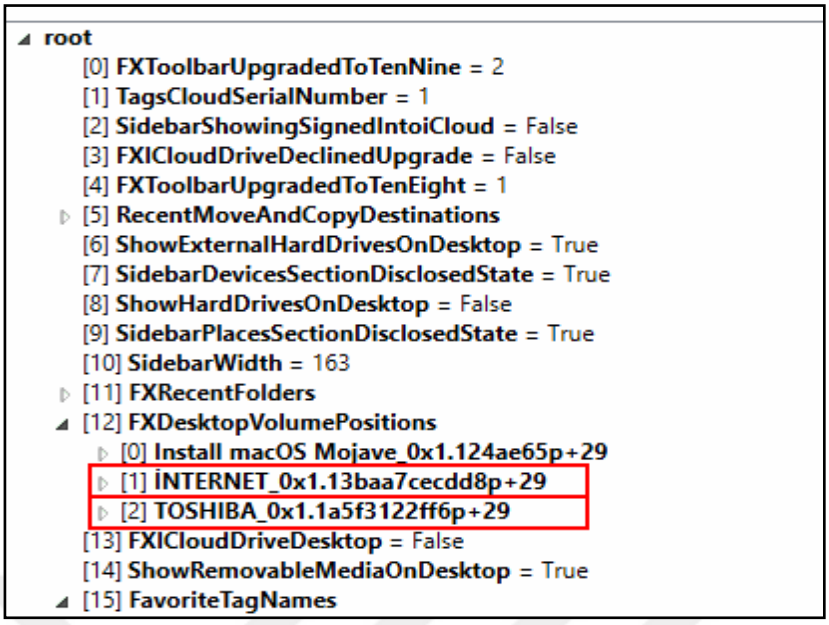


Şekil 3.37. Toshiba marka USB'ye ait tespit edilen bilgiler.



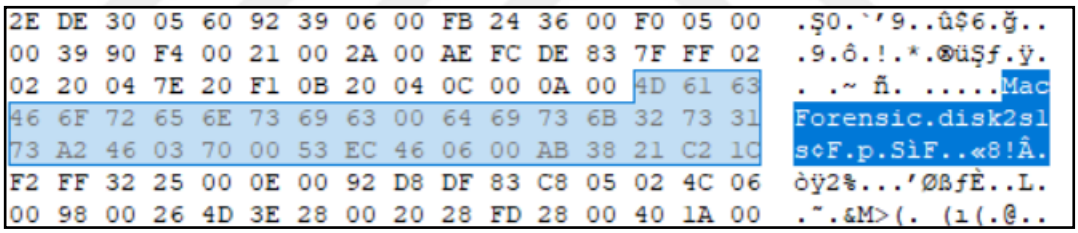
Şekil 3.38. İnternet isimli USB üzerinden erişilen dosya adı bilgisi.

"…\Users\Yonetici\Library\Preferences\" konumu altındaki "com.apple. finder.plist" isimli dosya içerisinde ise takılan USB belleklerin isim bilgileri tespit edilmiştir (Şekil 3.39).



Şekil 3.39. Takılan USB belleklerin isim bilgileri.

Yine "…\private\var\db\diagnostics\Persist\" konumu altındaki "tracev3" dosyası içerisinde yazdırılan CD'nin adı tespit edilmiştir (Şekil 3.40).



Şekil 3.40. Yazdırılan CD'nin isim bilgisi.

Tespit edilmesi hedeflenen, USB bellek ve CD'ye ait birim etiketleri, USB bellek seri numarası ve USB bellek üzerinden erişilen dosya adına ait kayıtlara ulaşılmıştır. Veri toplama aşamasında elde ettiğimiz veriler ile tespit edilen kayıtların doğruluğu görülmüştür. Ancak CD içerisine yazdırılan dosyaya ait kayıtlar tespit edilememiştir.

3.11. Bilgisayara Programların Yüklenmesi

Macbook bilgisayara programlar yüklenmiştir. Veri toplama aşamasında elde ettiğimiz veriler;

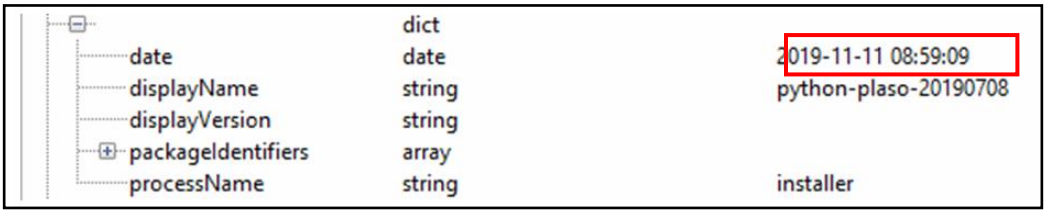
- Apple Uygulama Mağazası (App Store) üzerinden, "Educationterra English Class" isimli program tarih 11.11.2019 saat 09:08'de (UTC+3),
- Apple Uygulama Mağazası (App Store) üzerinden, "Kindergarten Reading For Mac" isimli program tarih 11.11.2019 saat 09:10'da (UTC+3),
- Apple Uygulama Mağazası (App Store) üzerinden, "Pool Byterun" isimli program tarih 11.11.2019 saat 09:14'de (UTC+3),
- Terminal üzerinden "plaso-20190708" isimli program tarih 11.11.2019 saat 11:59'da (UTC+3) kurulmuştur.
- Ardından BlackBag MacQuisition ile bilgisayarın imajı alınmıştır.

Alınan imajın BlackLight yazılımı ile yapılan incelemesinde; Apollo eklentisinin çalıştırılması sonucu "../private/var/db/CoreDuet/ Knowledge/" konumu altında bulunan "knowledgeC.db" dosyası içerisinde yüklenen program adı, yüklenme tarihi ve kullanım süresi tespit edilmiştir (Şekil 3.41).

Name	Usage In Seconds	Day Of Week	Gmt	Start	End
com.educationterra.EnglishClass	2912	Thursday	3	2019-11-11 06:08:45 (UTC)	2019-11-11 06:57:17 (UTC)
Anne-Gardner.Kindergarten-Reading-For-Mac-Free	2808	Thursday	3	2019-11-11 06:10:29 (UTC)	2019-11-11 06:57:17 (UTC)
com.byterun.pool-mac	49	Thursday	3	2019-11-11 06:14:07 (UTC)	2019-11-11 06:14:56 (UTC)

Şekil 3.41. Uygulama mağazası üzerinden yüklenen programlara ait bilgiler.

"…\Library\Receipts\InstallHistory.plist" dosyasının plist görüntüleyicisi ile yapılan analizinde ise komut satırından yüklenen programın yükleme tarihi ve program adı tespit edilmiştir (Şekil 3.42).



Şekil 3.42. Terminal üzerinden yüklenen programlara ait bilgiler.

Tespit edilmesi hedeflenen, yüklenen programlara ait isim ve tarih bilgilerine ulaşılmıştır. Veri toplama aşamasında elde ettiğimiz veriler ile tespit edilen kayıtların doğruluğu görülmüştür. BlackLight yazılımında ek olarak bu programların çalıştırılma sürelerinin olduğu görülmüştür. Bu program ile "knowledgeC.db" dosyası incelendiğinde Apple Uygulama Mağazasından yüklenen programlara ait verilerin olduğu görülmüştür.

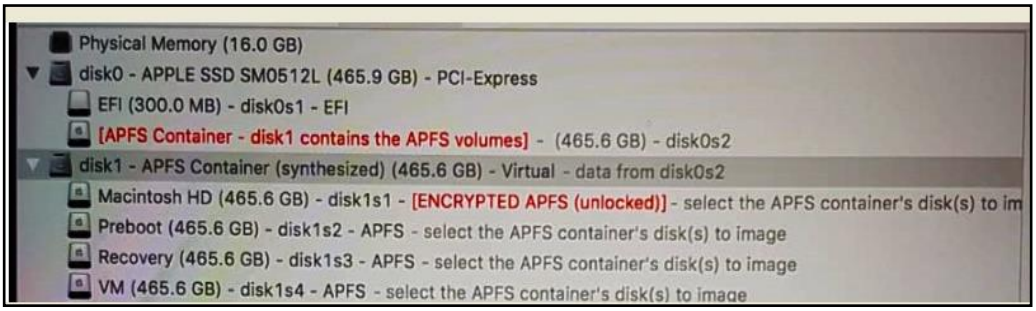
3.12. MacBook Pro Bilgisayarın FileVault2 Özelliğini Aktif Etme

İmaj alma ve inceleme sırasında Filevault2 özelliğinden kaynaklı karşılaşılabilecek problemlere karşı, bilgisayarın Filevault2 özelliği Bölüm 1.1'de anlatıldığı gibi aktif edilmiştir. Veri toplama aşamasında elde ettiğimiz veriler;
- Filevault2 özelliği aktif edilmiş, kullanıcı şifresi ise JKDB olarak belirlenmiştir.
- Ardından BlackBag MacQuisition ile bilgisayarın imajı alınmıştır.

İmaj alma sırasında; APFS dosyalama sistemine sahip Mac bilgisayarı FileVault2 özelliği aktif iken BlackBag MacQuisition boot edildiğinde, MacQuisition tarafından bu şifrelemeye dair uyarı ekranı gelecektir (Şekil 3.43).

Şekil 3.43. FileVault 2 İle şifreleme olduğuna dair uyarı.

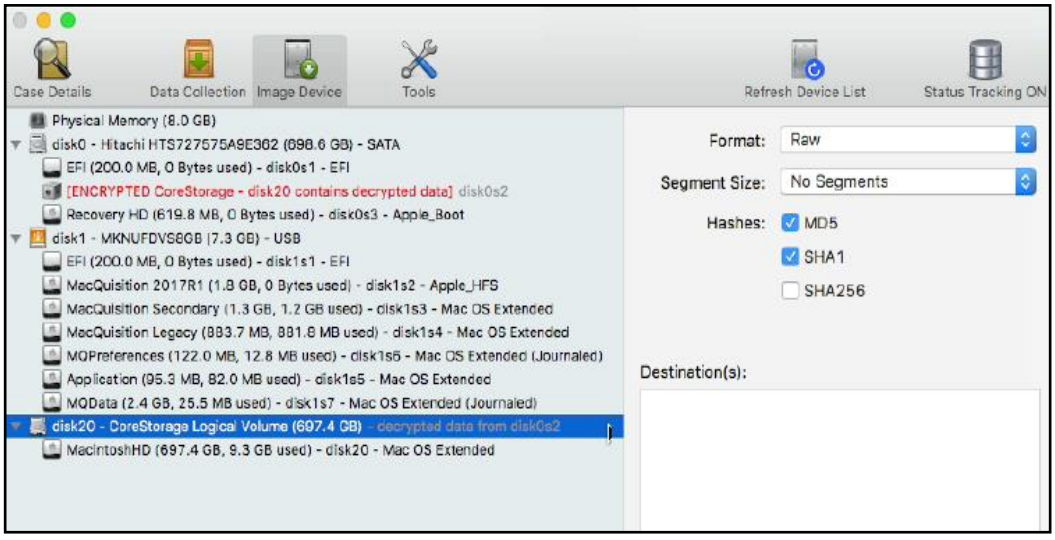
BlackBag MacQuisition arayüzü açılığında disk durumu aşağıdaki gibi gözükmektedir. MacQuisition APFS Container ile karşılaştığı zaman genelde "disk0" olarak fiziksel diski, "disk1" olarak da synthesized APFS Container'ı gösterir (Şekil 3.44).



Şekil 3.44. Apfs Container'a sahip mac bilgisayarın Blackbag Macquisition ile boot edildikten sonraki arayüz görünümü.

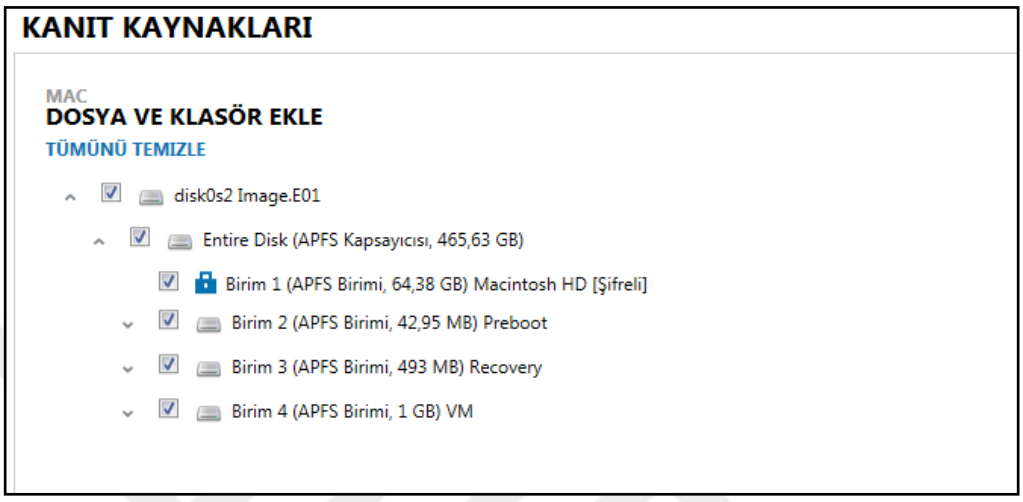
Yukarıdaki örnekte APFS Container şifreli olarak gözükmektedir. Tool menüsünden Macintosh HD seçilerek kullanıcı şifresi ya da kurtarma anahtarı girildiğinde Macintosh HD UNLOCK olarak görülecektir. Ancak bu işlem ile önceki versiyonlar da olduğu gibi diskin şifresi **çözülmediği tespit edilmiştir.** UNLOCK durumda iken Data Collection menüsünden bazı sistem ve kullanıcı verileri dosya olarak çıkartılabilir.

Eski versiyon Core Storage olan birimlerde tool menüsünden şifre girildiği zaman diskin şifresi çözümlenir ayrı bir disk olarak mount edilir (verilen örnekte disk20 olarak mount edilmiştir) ve kırmızı ile yazılı şekilde "decrypt data" olarak gözükür. Bu durumda imaj alındığı zaman şifresi çözülmüş olarak incelemeye devam edilebilir (Şekil 3.45)

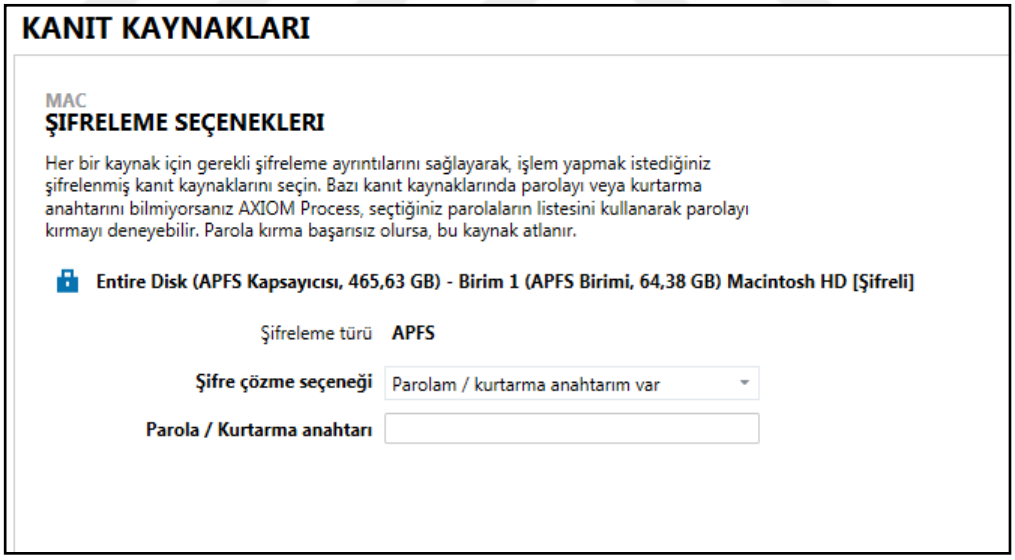


Şekil 3.45. CoreStorage mantıksal birime sahip mac bilgisayar için kullanıcı şifresi girildikten sonraki macquisition arayüz görünümü.

Ancak APFS Container'da imaj alma sırasında kullanıcı **şifresi girilse** bile inceleme yazılımları tarafından disk tekrar şifreli olarak **görülebilmektedir** (Şekil 3.46). Bazı inceleme yazılımlarına, imaj eklendiğinde disk şifreleme çözmeyi destekliyorsa işlem öncesi tekrar şifre girilmesini istemektedir (Şekil 3.47).

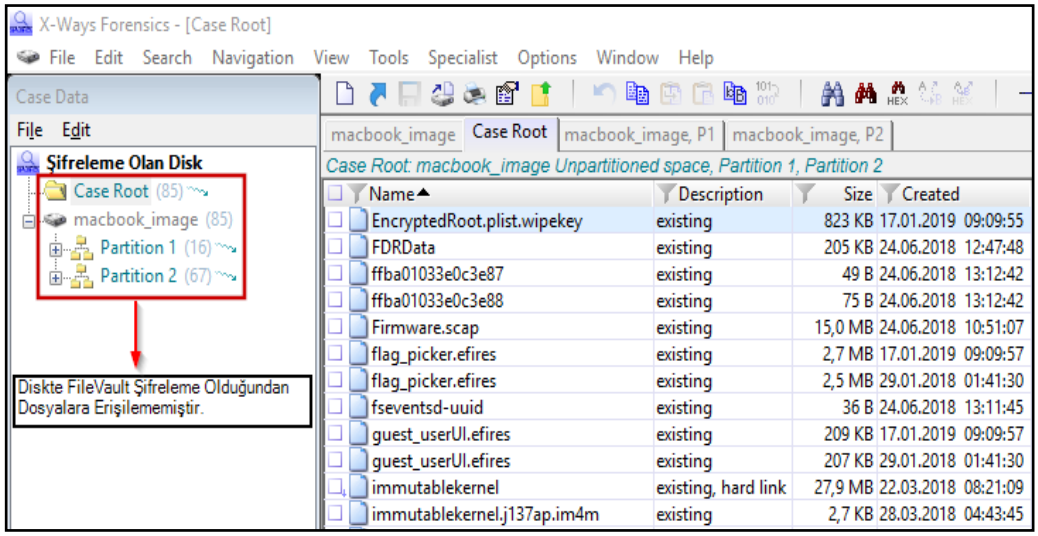


Şekil 3.46. AXIOM yazılımı tarafından FileVault şifreleme olduğuna dair görüntü.



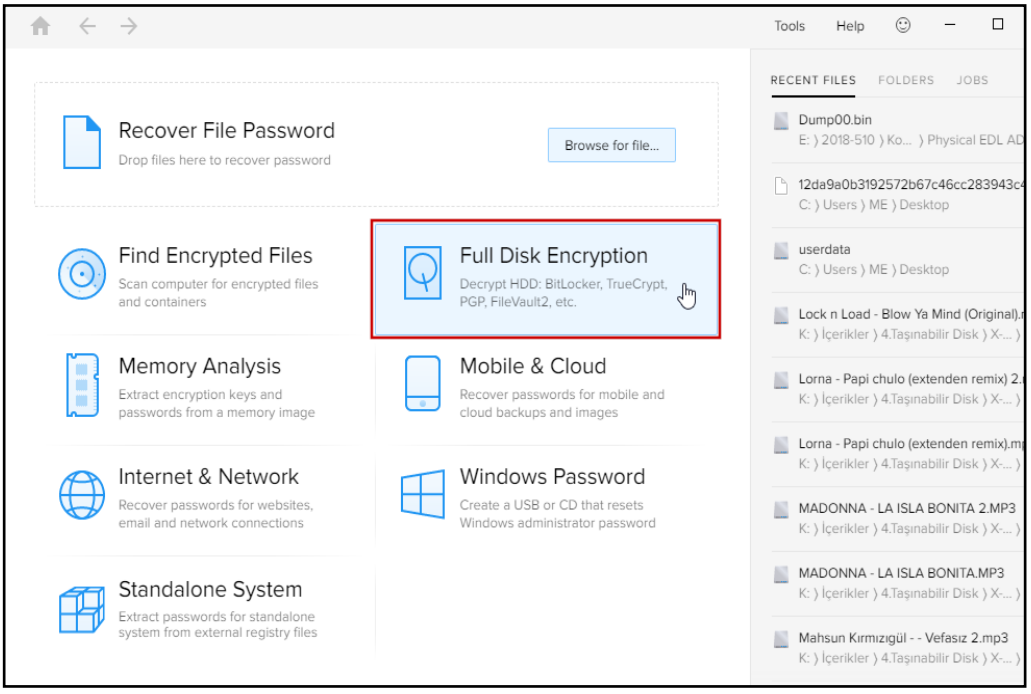
Şekil 3.47. AXIOM yazılımı tarafından FileVault şifrelemesine dair destek.

İnceleme aşamasında disk FileVault şifrelemesini çözmeyi desteklemeyen, X-Ways yazılımı için örnek gösterilmiştir (Şekil 3.48). Resimde görüldüğü üzere kullanıcı verisine erişim sağlanamamaktadır. Buda incelemenin yapılamayacağı anlamına gelmektedir.

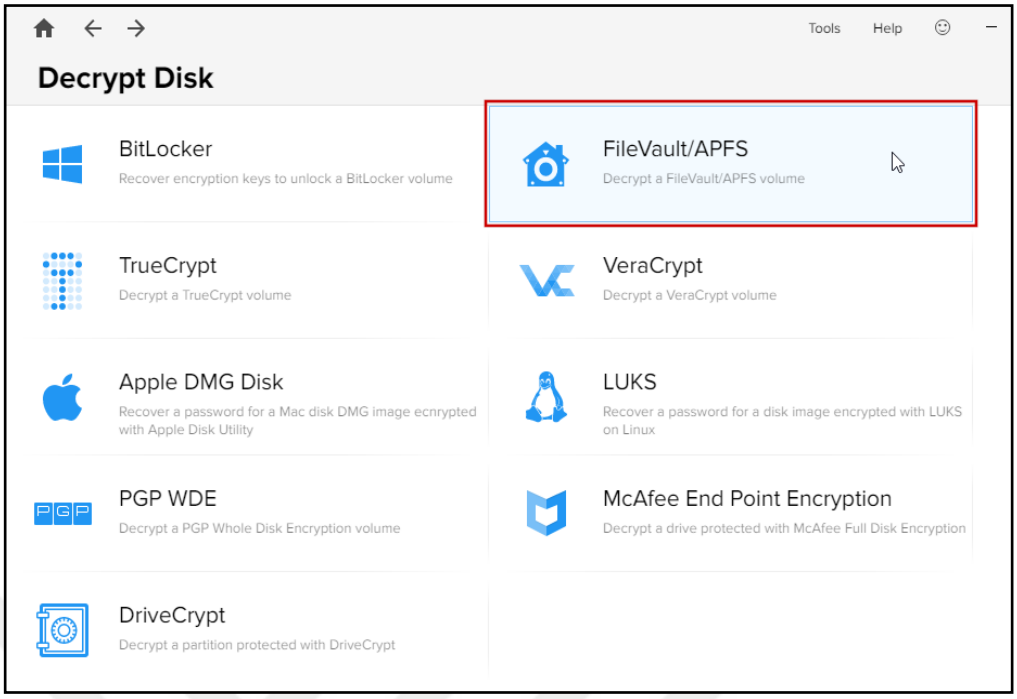


Şekil 3.48. FileVault şifrelemesi olan disk imajının X-Ways yazılımı ile görüntüsü.

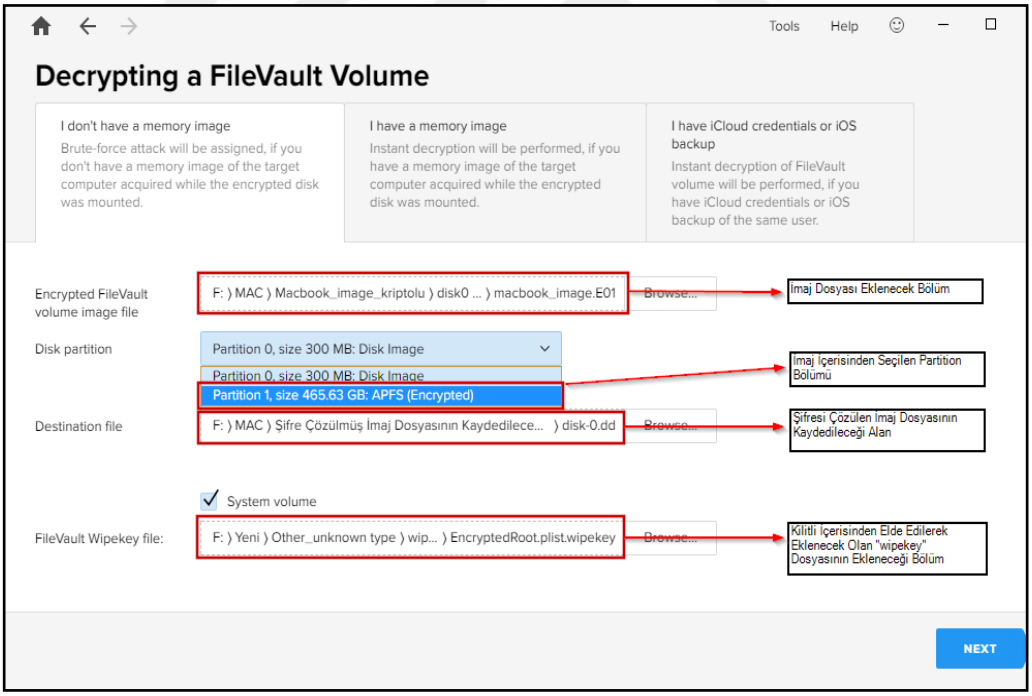
Disk şifreleme çözmeyi desteklemeyen inceleme yazılımları için çözüm olarak; Passware Password Recovery Kit ile şifreli imajın çözümlenerek, çözümlenen imajın inceleme yazılımına verilmesi sunulmuştur. Şifreli disk imajı Passware Password Recovery Kit ile aşağıdaki gibi çözümlenmiştir (Şekil 3.49, Şekil 3.50, Şekil 3.51, Şekil 3.52).



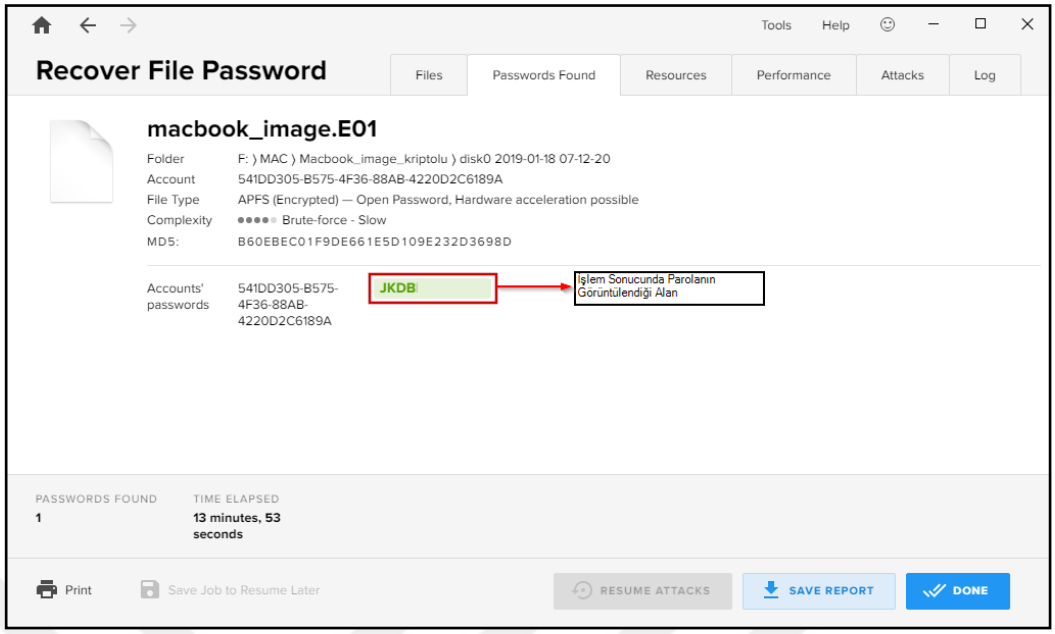
Şekil 3.49. Passware Password Recovery Kit yazılımının full disk encrypytion desteği.



Şekil 3.50. Passware Password Recovery Kit yazılımının FileVault/APFS desteği.

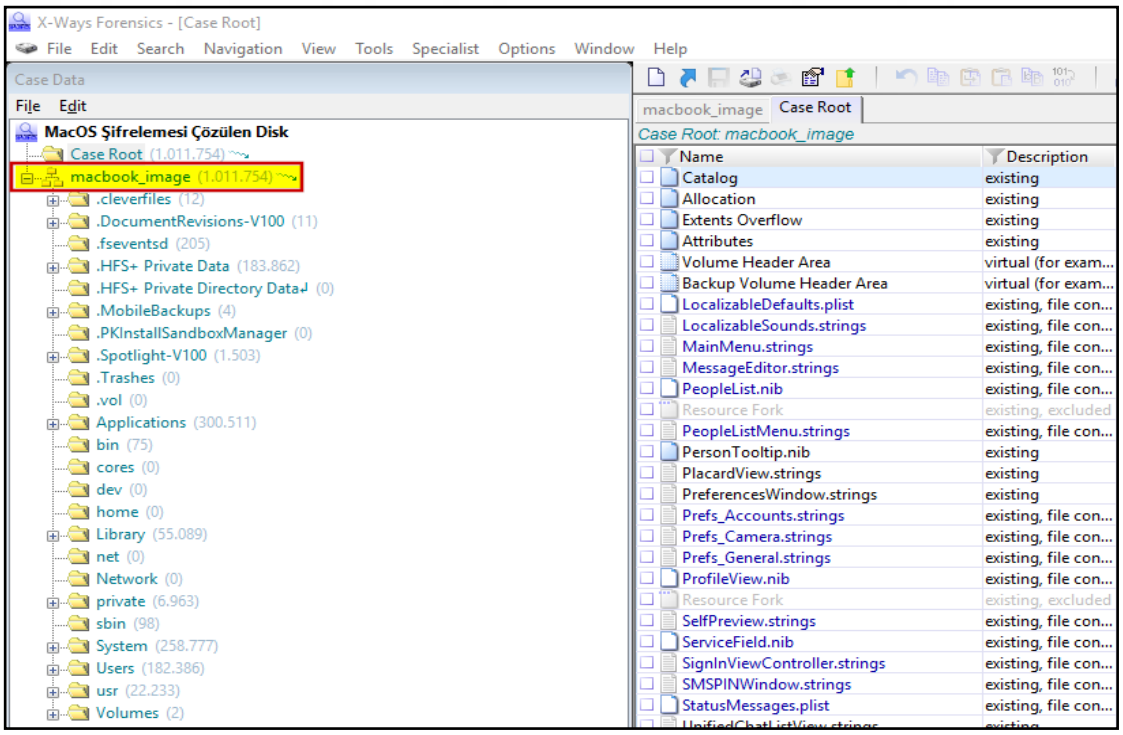


Şekil 3.51. Passware Password Recovery Kit yazılımının FileVault şifrelemesi olan disk imajının eklenmesi.



Şekil 3.52. Passware Password Recovery Kit yazılımı ile imajın çözümlenmesi.

Çözümlenen imaj, şifreleme çözmeyi desteklemeyen X-Ways yazılımına eklenmiştir ve görüldüğü gibi incelemeye bu işlemden sonra devam edilebilir haldedir (Şekil 3.53).



Şekil 3.53. Çözümlenen imajın X-Ways yazılımına eklenmiş hali.

İmaj alma sırasında karşılaşılan diğer bir problem ise; yeni model T2 çipi kullanan Mac bilgisayarların harici bir cihaz üzerinden boot edilmeye karşı önlenmiş olmasıdır. Bu ayar Recovery partition'dan ulaşabilen "Startup Security Utility" ile değiştirilebilir. Boot sırasında "Command (⌘) – R" tuşlarına basılarak Recovery partition'a erişilir. "Startup Security Utility" ayarı için **kullanıcı şifresi gereklidir** (MacQusion, 2019).

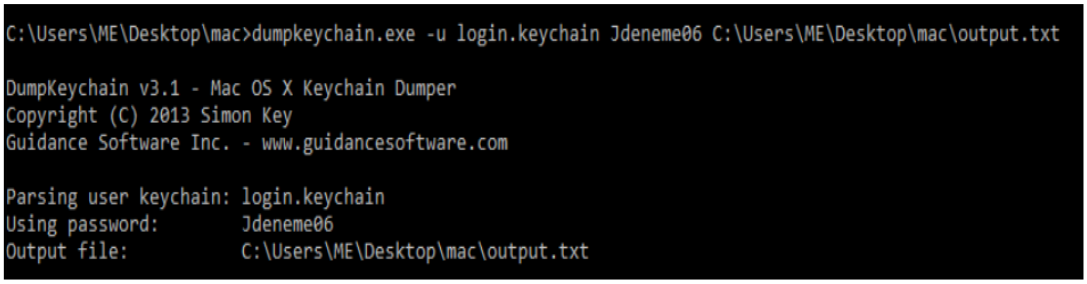
Önceki versiyonlarda Filevault disk şifreleme özelliği aktif olan Mac bilgisayarın, BlackBag MacQuisition ile imajı alınırken kullanıcı şifresi girildiğinde çözümlenmiş imaj elde ediliyordu. Ancak yeni versiyon ile beraber imaj alma sırasında kullanıcı şifresi girilse bile disk imajının çözümlenmediği ve inceleme sırasında problemlerle karşılaşıldığı görülmüştür. Bu probleme çözüm önerisi sunulmuştur.

3.13. MacBook Pro Bilgisayar Üzerinden Şifre Tespitleri

Macbook bilgisayara, iOS cep telefonunun iTunes yedeği alınmıştır. Ağ parolalarının tespit edilebilmesi içinde kablosuz ağlara bağlanılmıştır. Veri toplama aşamasında elde ettiğimiz veriler;

- Bilgisayara alınan iTunes yedeğinin şifresi, "Yntc06" olarak belirlenmiştir. (Bilgisayar oturum açma şifresi Jdeneme06)
- "X" isimli ağa bağlanılmış, ağın parolası "189706.." olarak belirlenmiştir.
- "Güven's İphone" isimli ağa bağlanılmış, ağın parolası "Deneme01.01" olarak belirlenmiştir.
- "DIRECT-xY_Canon10" isimli ağa bağlanılmış, ağın parolası "7858003581" olarak belirlenmiştir.
- "NiHaT" isimli ağa bağlanılmış, ağın parolası "19072828" olarak belirlenmiştir.
- "AndroidAP" isimli ağa bağlanılmış, ağın parolası "pvdq1009" olarak belirlenmiştir.
- Ardından BlackBag MacQuisition ile bilgisayarın imajı alınmıştır.

Alınan imajın yapılan incelemesinde "…\Users\(username)\ Library\Keychains\" konumu altında bulunan "login.keychain" dosyası dışarı çıkartılmıştır. "Dumpkeychain.exe" komut satırından aşağıdaki gibi çalıştırılmıştır (Şekil 3.54).

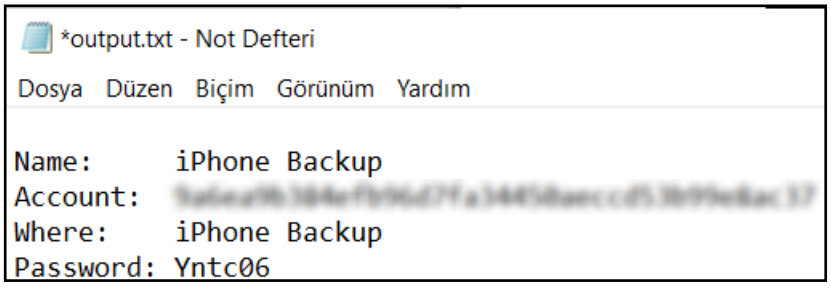


Şekil 3.54. Dumpkeychain.exe'nin çalıştırılması.

Komut satırındaki;

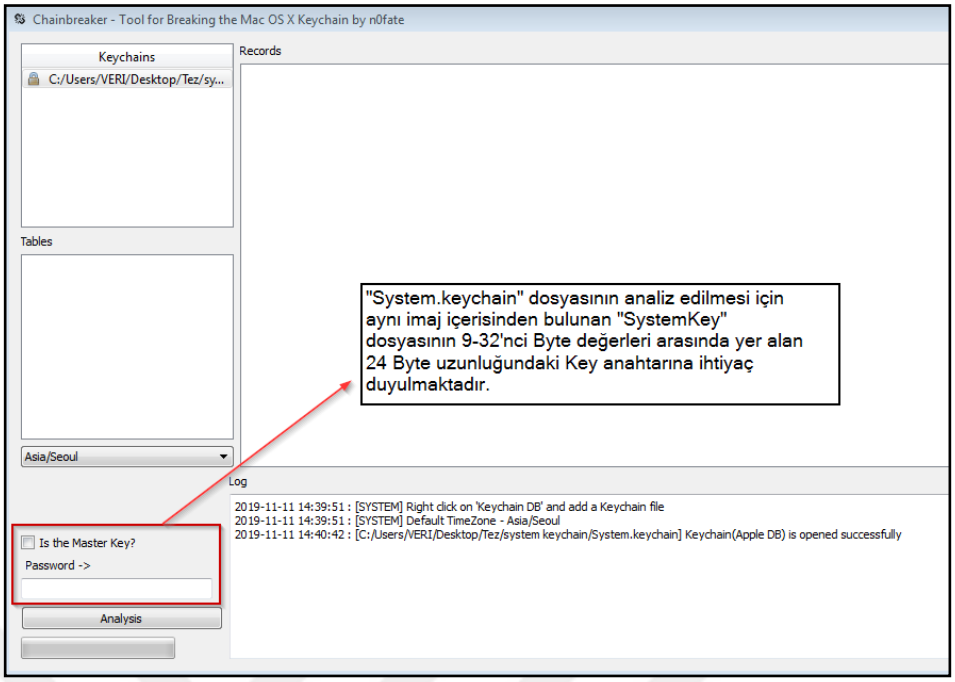
- <keychain> – imajdan dışarı çıkardığımız "login.keychain" dosyası,
- <password> – Bilgisayarın kullanıcı şifresi,
- <output_file> – çıktı olarak alınacak, kullanıcının şifrelerinin tutulduğu dosya.

Çıktı olarak alınan dosya içerisinde iTunes Yedeğinin şifresi tespit edilmiştir (Şekil 3.55).



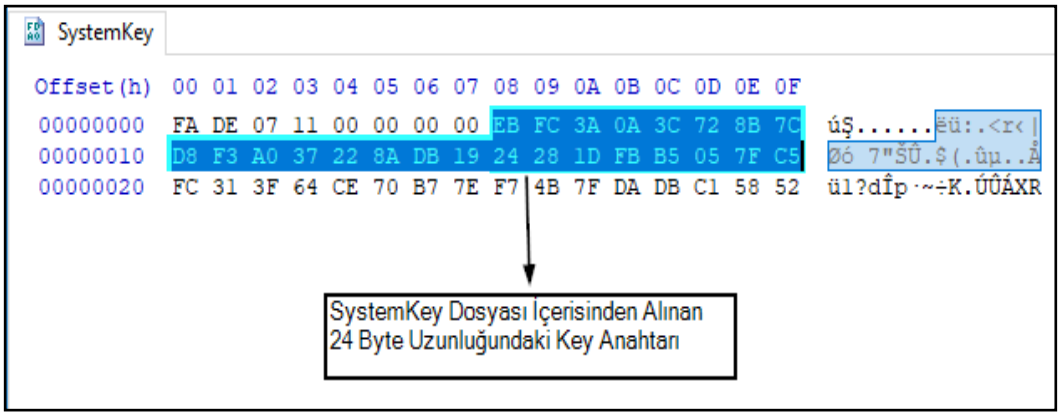
Şekil 3.55. Dumpkeychain.exe'nin çalıştırılması sonucu oluşan .txt uzantılı dosyada iTunes şifresi.

Bağlanılan ağların parolasını tespit etmek amacıyla "Chainbreaker" programı kullanılmıştır. Alınan imaj içerisinden elde edilen "System.keychain" dosyasının "Chainbreaker" programı ile analizi sırasında key anahtarına ihtiyaç duyulmaktadır (Şekil 3.56).



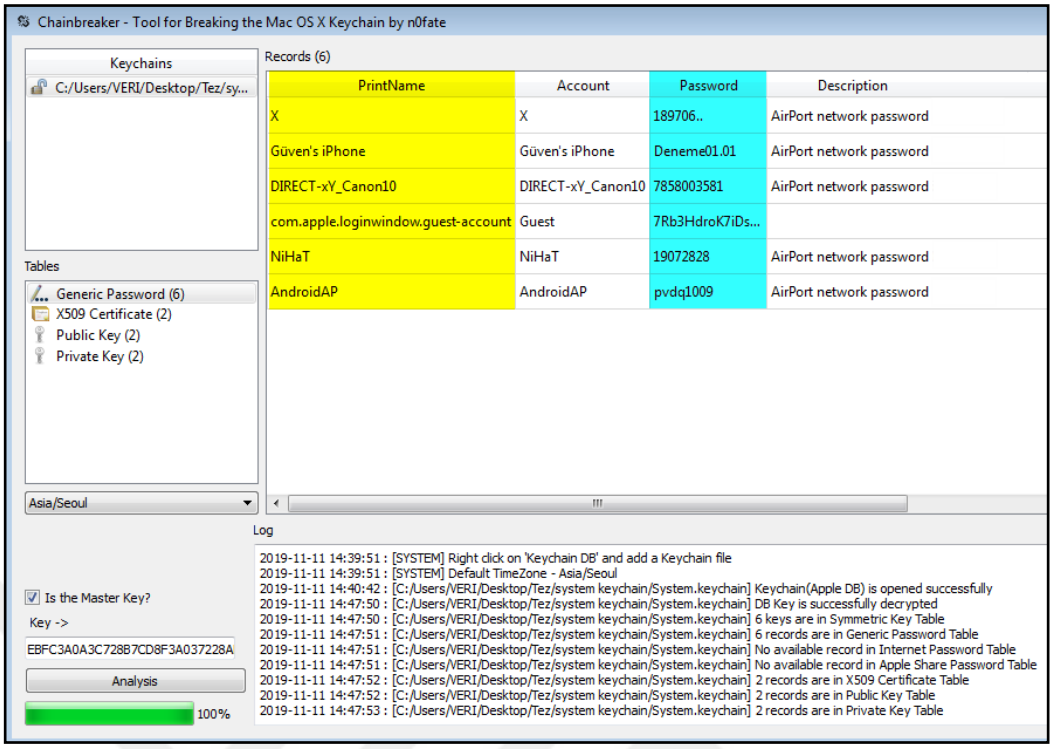
Şekil 3.56. Chainbreaker.exe'nin arayüzü.

Aynı imaj içerisinden tespit edilen "SystemKey" dosyasının 9'uncu Byte değeri ile 32'inci Byte değerleri arasında yer alan 24 Byte uzunluğundaki alan kopyalanarak Key (anahtarı) olarak kullanılmıştır (Şekil 3.57).



Şekil 3.57. SystemKey dosyasından elde edilen key (anahtarı) değeri.

"System.keychain" dosyasının "Chainbreaker" yazılımı ile analizinde bilgisayar üzerinden bağlanılan ağ isimleri ve bağlanılan ağların parola bilgileri tespit edilmiştir (Şekil 3.58).



Şekil 3.58. Tespit edilen ağ parolaları.

Parolalar adli bilişim incelemelerinde önemli olmaktadır. Tespit edilmesi hedeflenen iTunes yedek şifresi ve bağlanılan ağların şifresine ulaşılmıştır. Veri toplama aşamasında elde ettiğimiz veriler ile tespit edilen kayıtların doğruluğu görülmüştür. Parola tespitleri şifrenin karmaşasından bağımsız bir şekilde şifre kırma yöntemleri kullanılmadan tespit edilebilir.

4. TARTIŞMA

MacOS'un yeni sürümlerinden biri olan Mojave ile yapılan çalışma ile imaj alma ve inceleme sırasında bir takım problemler ile karşılaşılmış olup önerilerde bulunulmuştur.

- FileVault özelliği aktif olan yeni APFS Container birimler için imaj alma sırasında kullanıcı şifresi girilmesine rağmen imaj inceleme yazılımları tarafından yine de şifreli olarak gözükebilmektedir. Şifreleme çözmeyi desteklemeyen yazılımlarla incelemeye devam etmek için Passware yazılımı gibi yazılımlar ile çözümleme yapıldıktan sonra inceleme yazılımı ile devam edilebilir. Fakat kullanıcı şifresi bilinmiyor ve şifre güçlü ise bu işlem bir o kadar zor olacaktır.

- İşletim sistemleri üzerine düşen kayıtlar arasında MAC adresinin tespiti önem arz etmektedir. Ancak incelemeler sırasında işletim sistemine düşen MAC adresi kayıtlarının her seferinde doğru sonucu vermediği, bağlantı türünün sonuçları etkilediği görülmüştür. Dolayısıyla bilgisayar ile ağ bağlantısı gerçekleştirilen telefonlara ait MAC adresi tespitine yönelik yapılacak olan incelemenin; sadece inceleme yazılımı sonuçlarına göre yapılması ve sonuçların rapora yansıtılmasının dava sonucunu yanıltabileceği ön görülmüştür. Bu sebeple yapılan çalışmada iOS cihazlar için Wi-Fi ile bağlantı sağlandığı zaman, MAC adresi kayıtlarının tamamen farklı olabileceği ve bu durumun göz önüne alınması gerektiği önerilmiştir. USB ile bağlantı sağlandığı zaman MAC adresi kaydının doğrusunun nasıl bulunabileceği gösterilmiş ve aşağıdaki öneriler sunulmuştur.

- Alınan imaj, AXIOM yazılımı ile incelenip "ağ arayüzleri" yapı görüntüsü raporlandığı zaman sadece en son bağlanılan iPhone marka telefonlar gözüktüğü, daha önce bağlanan iPhone marka telefonlara ait herhangi bir kayıt gözükmediği tespit edilmiştir. Bu durumun eksik sonuçlara yol açacağı düşünülmelidir. Burada yapılması gereken "ağ arayüzleri" kaynağı "NetworkInterfaces.plist" dosyasının plist görüntüleyicisi ile manuel olarak incelenip "MatchingMACs" kısmından daha önce iPhone marka telefonun bağlanıp bağlanılmadığının kontrol edilmesidir.

- iOS için, “NetworkInterfaces.plist” dosyasında yer alan MAC adresinin ilk byte değerinden 2 çıkartıldığında telefonun kendi MAC adresini verdiği görülmüştür. Yani burada gözüken MAC adresi “3E:2E:FF:41:60:A0” ise ilk byte değeri olan 3E’den iki çıkarıldığında edilen sonucun (“3C:2E:FF:41:60:A0”) telefonun kendi MAC adresini verdiği tespit edilmiştir. Dolayısı ile iOS işletim sistemine sahip telefonlar USB ile ağ bağlantısı gerçekleştirdi ise önerilen şekilde inceleme yazılımına bağlı kalmaksızın MAC adresi tespit edilebilir. iOS ile yapılan 5. uygulama sonucunda aslında MacOS bilgisayar ile toplam 3 adet iPhone’nun USB üzerinden ağ bağlantısı işlemi gerçekleştirilmiştir. Bu üç adet iPhone için Çizelge 4.1’de inceleme yazılımının verdiği sonuç ve uygulanılan metodoloji sonrası önerilen analiz yöntemi ile tespit edilen sonuçlar yer almaktadır.

Çizelge 4.1. İnceleme yazılımının verdiği sonuç ve önerilen analiz yöntemi sonrası tespit edilen sonuçlar.

USB ile ağ bağlantısı gerçekleştirilen iOS işletim sistemine sahip telefonların MAC adresleri	İnceleme yazılımının verdiği sonuç	Önerilen analiz yöntemi ile tespit edilen MAC adresleri
98:00:C6:42:A5:03	3E:2E:FF:41:60:A0	98:00:C6:42:A5:03
B4:9C:DF:01:B3:DD		B4:9C:DF:01:B3:DD
3C:2E:FF:41:60:A0		3C:2E:FF:41:60:A0

- MacOS işletim sisteminde “…\Macintosh HD\private\var\db\lockdown\” konumu altında MAC bilgisayara USB ile bağlanan (ağ bağlantısı gerçekleştirilmediyse de) her iOS işletim sistemine sahip cihaz için plist dosyası oluşmaktadır (Bommisetty ve ark. 2014). Bu dosya içerisinde USB ile bağlanan iOS işletim sistemine sahip cihazın gerçek MAC adresinin bulunduğu tespit edilmiştir. Bu dosyadaki MAC adresi ile “NetworkInterfaces.plist” dosyasında bulunan MAC adresinin ilk byte değerinden iki çıkartılıp elde edilen adres karşılaştırıldığında aynı sonucu verip vermediği teyit edilebilir.

- MAC adresinin ilk 3 byte’ı üretici firmaya özgüdür. Bulunan MAC adreslerinin ilk 3 byte’ı internet üzerinde sorgulanarak ulaşılacak üretici firma ile teyit edilebilir. Örneğin; “NetworkInterfaces.plist” dosyasında bulunan MAC adresinin ilk üç byte’ı 9A:00:C6 idi, bu değerden ilk byte’ı olan 9A’dan 2 çıkarıldığında elde edeceğimiz sonuç 98:00:C6 olacaktır. Bu ilk üç byte MAC adresi-üretici firma eşleştiren veritabanlarında sorgulandığında karşımıza üretici firma olarak Apple çıktığı görülmüş ve böylelikle cihazın Apple ürünü olduğu tespit

edilmiştir. Aksi takdirde inceleme yazılımlarında çıkan MAC adresi raporlandığı zaman yanlış sonuçlara varılmaktadır. Çünkü 9A:00:C6 ile başlayan MAC adresi sorgulatıldığında üretici firma hiçbir firma adı ile eşleşmemektedir.

- iOS işletim sistemine sahip telefonlar Wi-Fi üzerinden bağlanıldığında "com.apple.airport.preferences.plist" ve "netusage.sqlite" dosyasında yer alan MAC adresi kayıtlarının, telefonun kendi MAC adresinden tamamen farklı olabileceği görülmüştür. Telefonların kendi MAC adresleri imaj içerisinde anahtar kelime olarak aratılmış ancak bulunamamıştır. İnceleme yazılımlarındaki yer alan MAC adreslerinin direk olarak raporda sunulması yerine bu durum raporda belirtilebilir.

- Tespit edilen her MAC adresi internet ortamında MAC adresleri ile üretici firmaları eşleştiren veri tabanı ile sorgulatılıp herhangi bir üretici ile eşleşmiyorsa raporda belirtilebilir.

- Yapılan literatür çalışmalarında; "NetworkInterfaces.plist" , "netusage.sqlite" ve "com.apple.airport.preferences.plist" isimli dosyalarda MAC adresleri bulunduğundan bahsedilmiştir. Bu çalışmada ise "netusage.sqlite" ve "com.apple.airport.preferences.plist" isimli dosyalarda MAC adreslerinin cihazın kendi MAC adresinden tamamen farklı olabileceği görülmüştür.

- Literatürde RAM analizi gerçekleştirilen çalışmada bağlanılan Wi-Fi ağının parolası tespit edilmeye çalışılmış ancak tespit edilememiş olup bu çalışmada imaj üzerinde ağ parolalarının tespit edilebileceği gösterilmiştir.

5. SONUÇ VE ÖNERİLER

Bu çalışmada, Mac işletim sistemi üzerinde adli bilişim açısından önem arz edebileceği değerlendirilen kayıtların tespit edilmesi hedeflenmiştir. Öncelikle literatür taraması yapılmış ve literatür taraması sonucunda yapılan çalışmaların yoğunlukla Mac işletim sisteminin eski versiyonları üzerinde olduğu görülmüştür. Mac, yeni versiyonlarla beraber yeni dosyalama sistemine geçiş yaptığı için bu konu büyük bir eksiklik olarak görülmüş çalışma platformu yeni versiyonlardan Mojave seçilmiştir. Önerilen metodolojiye uygun olarak yapılan ve yaklaşık bir sene süren bu çalışma ile birlikte;

- MacOS bilgisayarların imajı üzerinde veri toplamak, analizini yapmak ve sonuçları değerlendirmek için bir metodoloji önerilmiştir.
- Önerilen metodolojiye uygun olarak çalışmanın 2. bölümünde belirtilen uygulamalar gerçekleştirilmiştir.
- Uygulamaların analiz edilmesi ile birlikte tespit edilmesi istenen kayıtlara ulaşılmış, inceleme önerilerinde bulunulmuştur.
- Uygulamaların analiz edilmesi sırasında olası karşılaşılacak problemler listelenmiş ve çözüm önerileri sunulmuştur.
- İnceleme yazılımlarının bazı kayıtları eksik veya yanlış gösterdiği tespit edilmiştir. Bu kayıtların ulaşılabilirliği değerlendirilmiştir. Bu sebeple sadece inceleme yazılımı sonuçlarına göre raporlama yapılmasının dava sonucunu yanıltabileceği uyarısında bulunulmuştur
- MacOS bilgisayarlarda kayıtlara ait izlerin nerede bulunduğunu gösteren bir çizelge oluşturulmuştur (Çizelge 5.1).

Çizelge 5.1. Tespit edilen veriler.

Tespitler	Bulunduğu Dosya Yolu	Dosya Adı
İşletim Sisteminin Kurulma Zamanının Tespiti	\private\var\db	AppleSetupDone
Bilgisayar Adının Tespiti	\Library\Preferences\SystemConfiguration	preferences.plist

Çizelge 5.1. Tespit edilen veriler.(Devamı)

Tespitler	Bulunduğu Dosya Yolu	Dosya Adı
İşletim Sistemi Versiyon Bilgisinin Tespiti	\System\Library\CoreServices	SystemVersion.plist
Mevcut Kullanıcılar (kullanıcı id'leri, adları parola hashleri ve ipuçları)	\private\var\db\dslocal\nodes\Default\users	kullanıcı adı.plist Oluşturulan her kullanıcıya ait .plist dosyası.
Silinen Kullanıcılar (kullanıcı idleri, adı ve silinme zamanları)	\Library/Preferences	com.apple.preferences.accounts.plist ve audit log kayıtları
Sistem Güncelleştirmelerinin Tespiti	\var\log	install.log
Tarih Zaman Değişiklikleri	\var\db\timed \private\var\db\timed\Library\Preferences	com.apple.timed.plist
Takılan Harici Depolama Birimlerine Ait Bilgiler	\private\var\db\diagnostics\Persist \Users\Yonetici\Library\Preferences	*.tracev3 dosyaları com.apple.finder.plist
Kullanıcının Giriş-Çıkış İşlemleri	\private\var\log\asl	Sistem günlükleri içerisinde Giriş-Çıkış işlemlerine ait zaman bilgileri (BOOT_TIME ve SHUTDOWN_TIME ibarelerinden sonra)
Bağlanılan Ağın İsim Bilgisi ve MAC Adresleri Tespiti	\Library\Preferences\SystemConfiguration \Library\Preferences\SystemConfiguration \private\var\networkd	com.apple.airport. preferences.plist netusage.sqlite" NetworkInterfaces.plist"
Yazıcı İle İlgili Kayıtlar (Yazıcı adı, yazıcı MAC adresi, yazdırma tarihi, yazdırılan belge tipi, yazıcı adı, kullanıcı adı)	\Library\Preferences \private\var\spool\cups	org.cups.printers.plist, cxxxxx (bu dosya içerisinde time-at-completed ibaresinden sonra zaman bilgileri) ve dxxxxx kontrol dosyaları (bu çalışmada d kontrol dosyası için imaj mac_apt çalıştırılmıştır.)
Yüklenen Programların İsim Bilgileri ve Yüklenme Tarihlerinin Tespiti	\private\var\db\CoreDuet\Knowledge Library\Receipts	knowledgeC.db InstallHistory.plist

- Çizelge 5.1'de yer alan dosyaların açıklamaları aşağıda listelenmiştir.

- "AppleSetupDone" dosyası, işletim sistemi kurulduğunda oluşmaktadır.

- "kullanıcıadı.plist" dosyası; kullanıcılara özgü id numaralarını, kullanıcı adları, kullanıcı şifresinin PBKDF2-SHA512 algoritmasıyla hesaplanan hash değeri ve ipuçlarını tutar.

- "com.apple.preferences.accounts.plist" dosyası; silinen kullanıcılara ait isim bilgisi, kullanıcılara özgü id numaralarını, kullanıcı adlarını ve silinme zamanlarını içermektedir.

- "install.log" dosyası; içerisinde yüklenecek olan sürümünün indirilme zaman bilgisi, güncelleme işleminin yapıldığı zaman bilgisi, güncelleme

yapılmadan önceki versiyon sürümü ve güncelleme yapıldıktan sonraki versiyon sürümleri bilgisi tespit edilmiştir.

- "com.apple.timed.plist" dosyası, belirtilen yollardaki konumlarına göre asıl sistem zaman bilgilerini ve değiştirilen sistem zaman bilgilerini tutmaktadır.
- "com.apple.finder.plist" dosyası ve "*.tracev3" dosyaları içerisinde USB'ye ait seri numarası, adı, dosyalama sistemi ve USB üzerinden erişilen dosya bilgisi, yazdırılan CD'nin isim bilgisinin tutulduğu tespit edilmiştir.
- "org.cups.printers.plist" dosyası içerisinde bağlanılan yazıcı ile ilgili bilgiler tespit edilmiştir.
- "cxxxxx" ve "dxxxxx" kontrol dosyaları içeresinde yazdırılan dosyanın ne zaman yazdırıldığı, dokümanın tipi, yazıcı adı ve yazdırma işlemini yapan kullanıcı adı bilgileri yer almaktadır.
- "knowledgeC.db" ve "InstallHistory.plist" isimli dosyalarda, yüklenen programların adı ve yüklenme zamanları tespit edilmiştir.

- Filevault özelliği dışında bazı durumlarda alınan imajlar incelme yazılımlar tarafından açılmamaktadır. Bu durumda istenen bilgilere anahtar kelime aratılması sonucu erişilebilir. Bu çalışmada da bir takım anahtar kelimeler üretilmiştir.
  - audit log kayıtları içerisinde; Kullanıcı oluşturduğunda "Create record type Users", kullanıcı silindiğinde "Delete record type Users" ibareleri aratılabilir.
  - system.log kayıtları içerisinde; Bilgisayarın açma zamanı için; BOOT_TIME, bilgisayarın kapanma zamanı için; SHUTDOWN_TIME ibareleri aratılabilir.
- Analiz için sadece bir yazılıma bağlı kalınmaması önerilmektedir. Farklı yazılımlar kullanılıp elde edilen sonuçlar birbirleri ile karşılaştırılabilir.
- Kullanılan yazılımların sınırlarına bağlı kalınmaması önerilmektedir. Örneğin bir inceleme yazılımı yardımıyla yazdırılan belgeler ile ilgi sadece yazdırılan belge adı tespit ediliyorsa bu işlemi hangi kullanıcının ne zaman yapmış olduğu bilgisi, bu çalışmada gösterilen şekilde manuel olarak da bulunabilir.
- Kayıtların raporlaması yapılırken yazılımların hangi zaman dilimine göre sonuç verdiği ve sistemin gerçek zaman bilgisinin dikkate alınması önerilir.

- Yazılımların versiyonları arasında değişiklikler olabileceğinden aynı yazılımın farklı versiyonları ile de analiz sonuçları arasındaki farklılıkların olup olmadığı var ise bu farklılıkların sebepleri incelenebilir.
- Yazılım kullanılmasının yanında dosyaların manuel olarak da incelenmesi önerilmektedir. Manuel inceleme ile yazılımların verdiği sonuçlar arasındaki tutarlılıklara bakılabilir.
- İncelemelerden önce delilin işletim versiyonu dikkate alınarak aynı versiyona sahip sanal makineler oluşturulup, önerilen metodolojiye uygun uygulamalar gerçekleştirilerek sistem üzerinde nasıl bir etki bıraktığı incelenebilir. İşletim sistemi versiyonları arasında farklılıklar olabilmektedir.
- Zamandan kazanç sağlanması adına iTunes yedekleri ve ağ parolaları tespitleri için (oturum açma şifresi biliniyorsa) şifre kırma ataklarına alternatif olarak önerilen Chainbreaker.exe ve Dumpkeychain.exe kullanılabilir.

- Kullanıcı oluşturma ve silme işlemlerini hangi kullanıcının gerçekleştirdiğine dair kayıtlar, CD içerisine yazdırılan dosyaya ait kayıtlar ve sadece Wi-Fi ile bağlantı kurulan iOS cihaza ait gerçek MAC adreslerine ait kayıtlar tespit edilememiştir.

Bu çalışmada, ülkemizde daha çok imaj üzerinden incelemeler gerçekleştirildiği için canlı inceleme veya önceliklendirme yöntemi kullanılmamıştır. İleriki çalışmalarda, literatürde farklı görüşler bulunsa da adli bilişim sürecinin zaman alıcı bir süreç olmasına çözüm olarak sunulan önceliklendirme yöntemi kullanılabilir. Canlı incelemeler yapılabilir. Ayrıca iOS cihazlara ek olarak ağ ile ilgili yapılan uygulamalar Android işletim sistemine sahip telefonlarla da gerçekleştirilebilir. Yine bu çalışmada olduğu gibi imaj üzerinden incelemeler, MacOS'un eski dosyalama sitemleri üzerinde ya da yeni versiyonlar üzerinde gerçekleştirilebilir. Böylece çalışmalar arasında karşılaştırmalar da yapılabilecektir.

ÖZET

MacOS İşletim Sistemine Sahip Bilgisayarlar Üzerinde Adli Bilişim Açısından Önem Arz Eden Kayıtların İncelenmesi

Bu çalışma, Mac işletim sistemine sahip bilgisayarlar üzerinde; adli bilişim açısından önem arz eden kayıtların tespit edilmesi ve analizi için bir metodoloji önerilmesi, inceleme yaparken karşılaşılan problemleri tespit etmek ve bu problemlere çözüm önerisi sunmak amacıyla yapılmıştır.

Bu çalışma için ilk aşamada literatür taraması yapılmıştır. Literatür taraması sonucunda; yapılan çalışmaların MacOS 10.14 versiyonundan önceki sürümler üzerinde gerçekleştirildiği görülmüş olup platform olarak MacOS 10.14 (Mojave) versiyonu seçilmiştir.

İncelemeler için, adli bilişim açısından önem arz edebileceği değerlendirilen ve genel olarak inceleme isteklerinde belirtilen istekler doğrultusunda çeşitli uygulamalar yapılmış ve bu uygulamaların ardından; lisanslı programlar ve internet üzerinden araştırılarak ücretsiz temin edilen programlar ile analizleri gerçekleştirilmiştir.

Önerilen metodoloji kullanılarak yapılan analizlerin sonucunda; işletim sisteminin kurulma tarihi, oluşturulan ve silinen kullanıcılar, kullanıcı giriş (login) ve çıkış (logout) verileri, bilgisayarın başlatma ve kapama bilgileri, tarih-saat değişiklikleri, ağ yapılandırması, ağ üzerinden erişim, kablosuz erişim noktalarına yapılan bağlantılar, MAC adresi tespitleri, yazıcı ile ilgili kayıtlar, bilgisayara takılan harici veri depolayan cihazlar, yüklü programlara ait kayıtlar gibi çeşitli veriler tespit edilmiştir. Ayrıca karşılaşılan problemlere ait çözüm önerileri sunulmuştur.

Çalışmalar neticesinde yapılan tespitler ve yapılan literatür taramasında tespit edilen diğer kayıtlara ait izlerin nerede bulunduğunu gösteren bir çizelge oluşturulmuştur.

Anahtar Kelimeler: Adli Bilişim, Kayıtlar, MacOS, Mojave, İşletim Sistemi.

SUMMARY

Investigation of Important Records in terms of Forensic Computing on MacOS Operating System

This study was conducted on computers with Mac operating system sent to our laboratory for examination; The aim of this study was to determine the problems that are important for forensic informatics and to create a methodology for the analysis of the records, to identify the problems encountered during the investigation and to propose solutions to these problems.

In the first stage of this study, literature review was executed. As a result of literature review; It has been noticed that the studies were performed on versions which are earlier than MacOS 10.14. For this reason, MacOS 10.14 (Mojave) version was chosen as the platform.

For the investigations, various applications have been made in line with the requests that are considered to be of importance in terms of forensic informatics and that are generally stated in the requests for examination. And in addition; the licensed programs and the programs that were provided free of charge were searched through the internet and analyzed.

As a result of analysis using the proposed methodology; operating system installation date, created and deleted users, user login and logout data, computer startup and shutdown information, date-time changes, network configuration, network access, connections to wireless access points, MAC addresses, printer-related records various data, such as devices attached to the computer, external data storage devices, records of installed programs have been identified. In addition, solutions for the problems encountered are presented.

As a result of the studies, a table showing the traces of the other records found in the findings and the literature search has been created.

Keywords: Digital Forensics, MacOS, Mojave, Operating System, Records.

KAYNAKLAR

ASLAN Ö, SAMET R (2020). A Comprehensive Review on Malware Detection Approaches. *IEEE Access*, **8:** 1-1, 6249-6271.

ATWAL T S, SCANLON M, LE-KHAC N (2019). Shining a light on Spotlight: Leveraging Apple's desktop search utility to recover deleted file metadata on macOS. *Digital Investigation*, **28:** Supplement.

BLACKMAN D, SZEWCZYK P (2015). The challenges of seizing and searching the contents of Wi-Fi devices for the modern investigator, Erişim adresi: [https://doi.org/10.4225/75/57b3f385fb887]. Erişim Tarihi:23.09.2019.

BOMMISETTY S, TAMMA R, MAHALIK H (2014). Data Acquisition from iOS Backups. In PRACTICAL MOBILE FORENSICS: Dive into mobile forensics on iOS, Android, Windows, and BlackBerry devices with this action-packed, practical guide, Chapter 5. Birmingham, UK: Packt Pub.

BOURSALIAN A, STAMP M (2019). BootBandit: A macOS bootloader attack. Engineering Reports. 1. 10.1002/eng2.12032.

BURGHARDT A, FELDMAN A (2008). Using the HFS+ journal for deleted file recovery. *Digital Investigation*, **5:** 10.1016/j.diin.2008.05.013.

COOK M, NICASTRO J, DALZELL TJ, GEYER M, TRUAX A (2015). Mac OS X Forensic Artifact Locations. Champlain college leahy center for digital investigation.

CRAIGER P, BURKE P K (2006). "Mac Forensics : Mac OS X and the HFS+ File System" Department of Engineering Technology University of Central Florida.

CUSSEN T, BRYANT W (2015). Domestic/family homicide in Australia. Research in practice no. 38. Canberra: Australian Institute of Criminology.

DEĞİRMENCİ O (2020). "Adli bilişimde önceliklendirme (triyaj) yönteminin ceza muhakemesi hukuku açısından değerlendirilmesi". *Bilişim Hukuku Dergisi*, **2:** 47-79.

ETENG I, OGBAN F, BASSEY H, (2007). Analysis of the Unix Operating System And Improvement Of The Password Authentication Technique. *International Journal of Pure & Applied Sciences*, Vol **2**:152 – 159.

FARONICS (2017). Deep Freeze Mac and CoreStorage Technical Report.

GARG U, VERMA P, MOUDGIL Y S, SHARMA S (2012). MAC and Logical addressing. *International Journal of Engineering Research and Applications*, Vol. **2**: Issue 3, May-Jun 2012, pp.474-480/ISSN: 2248-9622.

GARIJO J M (2015). Mac OS X Forensics Technical Report, Information Security Group Royal Holloway University of London.

GARIJO J M, CAVALLARO L (2015). Mac OS X persistent evidences for forensics purposes Royal Holloway University of London

GEDİK D (2019). "Bilişim suçlarında ıp tespiti ile ekran görüntüleri çıktılarının ispat değeri". *Bilişim Hukuku Dergisi*, **1:** 51-84.

GUPTA S, ROGERS M (2014). Exploring Forensic Implications of the Fusion Drive. *Journal of Digital Forensics, Security and Law*. 10.15394/jdfsl.2014.1177.

HENKOĞLU T (2011). ADLİ BİLİŞİM: DİJİTAL DELİLLERİN ELDE EDİLMESİ VE ANALİZİ. Bölüm 8.

HITCHCOCK B, LE-KHAC N, SCANLON M (2016). Tiered Forensic Methodology Model for Digital Field Triage by Non-Digital Evidence Specialists. Digital Investigation. 16. 10.1016/j.diin.2016.01.010.

HOENE T, CREUTZBURG R (2011). iPhone forensics based on Macintosh open source and freeware tools. 10.1117/12.879318.

JOYCE R A, POWERS J, ADELSTEIN F (2008). "MEGA: A tool for Mac OS X operating system and application forensics", Digital Investigation. Elsevier BV, 5: pp. S83–S90. doi: 10.1016/j.diin.2008.05.011.

KAUSHIK R (2007). A Spotlight on Spotlight. University of Wisconsin, Madison.

KIM K, MIN A W, GUPTA D, MOHAPATRA P, SINGH J P (2011). Improving energy efficiency of Wi-Fi sensing on smartphones. 2930-2938. 10.1109/INFCOM.2011.5935133.

LEVIN J (2012). MAC OS X AND IOS INTERNALS: TO THE APPLE'S CORE (1st. ed.), Chapter 2, 2122, Wrox Press Ltd., GBR.

MAC4N6, Network and Application Usage using netusagesqlite&DataUsagesqlite iOS Databases, Erişim Adresi: https://www.mac4n6.com/blog/2019/1/6/network-and-application-usage-using-netusagesqlite-amp-datausagesqlite-ios-databases Erişim Tarihi:10.09.2019.

MADDU B, RAO P P (2019). OS X artifact analysis. *International Journal of Recent Technology and Engineering*, **7:** 26-32.

MARTIN D M (2016). "OS X as a Forensic Platform".

MARTIN J, RYE E, BEVERLY R (2016). Decomposition of MAC address structure for granular device inference. 78-88. 10.1145/2991079.2991098.

MATELJAN V, PETER K, JURIČIĆ V (2020). An Optimization of Command History Search.

NEWCOMER S, MARTIN L (2014). Determining User Actions In Os X Based On Quicklook Thumbnail Cache Database Entries. *International Association of Computer Investigative Specialists*, Volume **15:** Issue II, pp. 421-430, 2014.

PEARSON S, WATSON R (2010). DIGITAL TRIAGE FORENSICS: PROCESSING THE DIGITAL CRIME SCENE (1st. ed.), Chapter 2, (Syngress).

PRASAD E, DIJA S, LAKSHMI D M P (2018). "Towards Live Forensic Acquisition & Analysis of Mac OS Systems," International CET Conference on Control, Communication, and Computing (IC4), Thiruvananthapuram, pp. 415-418, doi: 10.1109/CETIC4.2018.8530928.

PRIMEAUX D, DAHLBERG R, KEO K, LARSON S, PENNELL B, SHERMAN K (2011). "MAC OS X Forensics: Password Discovery" Annual ADFSL Conference on Digital Forensics, Security and Law. 5.

RATHOD D M (2017a). MAC OSX Forenscis. *International Journal of Advanced Research in Computer Engineering & Technology*, **6:** 1240.

RATHOD D M (2017b). MAC OSX: iMessage, Face Time, Apple Mail Application Forensics. *Journal of ınformatıon, knowledge and research ın computer engıneerıng*, **4:** 1000.

REDDY N (2019). PRACTICAL CYBER FORENSİCS: AN INCIDENT-BASED APPROACH TO FORENSIC INVESTIGATIONS. Chapter 4. 10.1007/978-1-4842-4460-9.

SARWAR M, SOOMRO T R (2013). Impact of Smartphone's on Society. European Journal of Scientific Research. 98.

STAMM C (2012). Mac RAM Analysis. The Senator Patrick Leahy Center for Digital Investigation Champlain College.

SUMMERS D, RILEY C, CREMALDI L, SANDERS D A (2001). Work with Apple's Rhapsody Operating System which Allows Simultaneous UNIX Program Development, UNIX Program Execution, and PC Application Execution. CHEP98, hep-ex/0105082.

SWGDE (2015). Scientific Working Group on Digital Evidence Mac OS X Tech Notes. Erişim Adresi: https://www.swgde.org/documents/Current%20Documents/ SWGDE%20Mac %20OS%20X%20Tech%20Notes Erişim Tarihi:30.07.2019.

THOMPSON J (2017). Demystifying Full-Disk Encryption: A Special Case of Applied Cryptography Independent Security Evaluators LLC.