Journal of Computer Science
https://dergipark.org.tr/en/pub/bbd
Anatolian Science

ISSN,e-ISSN: 2548-1304
Volume:8, Issue:2, pp:130-147, 2023
https://doi.org/10.53070/bbd.1349208
Research Paper

Kripto Para Cüzdanının (Sıcak Cüzdan) Adli Bilişim Açısından İncelenmesi

Examination of Cryptocurrency Wallet (Hot Wallet) in Terms of Forensics

Ramazan Oğuz [*1], Emin Kınacı [*1], Hakkı Halil Babacan[2]
İstanbul Üniversitesi-Cerrahpaşa,
Adli Tıp Ve Adli Bilimler Enstitüsü
(ramazan.oguz@ogr.iuc.edu.tr; eminkinaci@gmail.com; hakki.babacan@erzincan.edu.tr)

Received:Aug.24, 2023 Accepted: Sep.26, 2023 Published: Dec.20, 2023

Özetçe— Kripto varlıklar son yıllarda önemli bir yatırım aracı haline gelmiştir ve kripto varlıkların piyasa değeri 1 trilyon doların üzerine çıkmıştır. Son yıllarda önemli bir büyüme elde eden kripto varlıkların takibi ve üzerindeki suç unsurlarını tespit etmek kaçınılmaz bir hale gelmiştir. Bu çalışmanın amacı, kripto para cüzdanlarının (Soğuk, Sıcak ve Donanım cüzdan) genel yapılarının tanıtılması ve dünya genelinde yaygın bir kullanım alanı olan Tronlink isimli sıcak cüzdan üzerinde çeşitli transfer/görüntüleme işlemlerinin yapılarak (bilgisayar ve cep telefonlarında) oluşan adli kanıtların tespit edilmesidir. Bu kapsamda, android ve windows işletim sistemlerine sahip bilgisayar ve cep telefonu üzerine sıcak cüzdan kurulumu gerçekleştirilmiş ve müteakibinde bir dizi kripto para transfer işlemleri yapılmıştır. İşlemlerin tamamlanması üzerine cihazların adli kopyaları alınmıştır. İşlemler sonucunda kripto para cüzdanlarının Cellebrite UFED ve Xways adli bilişim yazılımları ile incelemesi gerçekleştirilmiştir. İncelemeler sonucunda sıcak cüzdan üzerinde bulunan hesap ve kullanıcı bilgileri kullanılmak suretiyle yapılan tüm transfer işlemlerine ulaşılmıştır. İncelemeler sonucunda kripto para işlemlerini tespit edecek anahtar kelimeler oluşturulmuştur. Böylece bu çalışmanın adli bilişim kapsamında gelecek olan kripto para cüzdanlarının incelemelerine referans olacağı değerlendirilmektedir.

Anahtar Kelimeler : *Adli bilişim, kripto para, blok zincir, kripto para cüzdanı, tronlink, genel anahtar.*

Abstract— In recent years, cryptocurrency assets have become a significant investment tool, and the market value of these assets has surpassed 1 trillion dollars. Given the substantial growth of cryptocurrency in the past few years, monitoring these assets and detecting potential criminal activities associated with them has become imperative. The aim of this study is to introduce the general structures of cryptocurrency wallets (Cold, Hot, and Hardware wallets) and to identify forensic evidence generated from various transfer/view operations on the widely used hot wallet named Tronlink (on both computers and mobile devices). Within this scope, hot wallets were installed on devices running Android and Windows operating systems, followed by a series of cryptocurrency transfer transactions. Upon the completion of these operations, forensic copies of the devices were obtained. The subsequent analysis of the cryptocurrency wallets was conducted using the forensic software tools Cellebrite UFED and Xways. Consequently the examinations, all transfer transactions executed using the account and user information on the hot wallet were accessed. Key terms to identify cryptocurrency transactions were established based on the findings. It is assessed that this study will serve as a reference for future forensic examinations of cryptocurrency wallets within the realm of digital forensics.

Keywords : *Digital forensics, cryptocurrency, blockchain, cryptocurrency wallet, tronlink, public key.*

1. Giriş

İnsanoğlu son dönemlere kadar birikimlerini, güvenli olması nedeniyle ve enflasyona karşı değer kaybetmesini önlemek adına ya bankalarda tutmakta, ya da evlerinde nakit veya emtia (altın, gümüş vb.) olarak muhafazasını sağlamaktaydı. Blok zincir teknolojisinin hayatımıza girmesiyle birlikte kripto varlıklar (Bitcoin ve diğer kripto paralar) da bir yatırım aracı olarak görülmeye başlanmıştır. Dünya genelinde Haziran 2023 tarihi itibariyle kripto paralara yatırılan miktar 1,170 trilyon dolara ulaşmıştır (CoinMarketCap, 2023). Ülkemizde bankalara yapılan yatırımların bir kısmı veya tamamı bankaların ya da T.C. Devleti hazinesinin güvencesi altında bulunmaktadır. Bankalarda meydana gelen hırsızlık, hesaplara yetkisiz erişim sonucu dolandırıcılık veya bankaların iflas etmesi gibi durumlarda devletler yatırımcıların mağduriyetlerini bağlı oldukları kanunlar çerçevesinde gidermektedir. Türkiye'de "Sigortaya Tabi Mevduat ve Katılım Fonları İle Tasarruf Mevduatı Sigorta Fonunca Tahsil Olunacak Primlere Dair Yönetmelik" ile mevduatlar TMSF kapsamında güvence altında bulunmaktadır. 2023 yılı için bu oran 400 bin TL ye kadar ki mevduatları karşılamaktadır (Resmi Gazete, 2022).

Bu durum yatırımcıyı kısmen de olsa güvence altına almaktadır. Kripto para birimlerinde ise durum biraz daha farklı olup kripto paralar cüzdanlarda fiziksel olarak saklanamazlar ve kripto paraların altyapısını oluşturan blok zincirlerin merkeziyetsiz yapıları vardır (Jokić, 2019). Kripto paraların itibari para ile alınması ve satılması kripto para borsaları üzerinden gerçekleştirilmektedir. Kripto para borsalarının hayatımıza çok hızlı bir şekilde giriş yapması nedeniyle dünya üzerindeki ülkeler, bunların geçerliliğini ve hayatımıza nasıl entegre edileceğini henüz yasal bir zemine oturtamaması nedeniyle farklı uygulamaların doğmasına sebep olmuştur. 16.04.2021 tarihli Resmi Gazetede yayınlanan "Ödemelerde Kripto Varlıkların Kullanılmamasına" dair yönetmeliğe göre ülkemizde kripto para varlıkları ile mal/hizmet alım satımı yapılması yasaklanmıştır (Resmi Gazete, 2021). Fakat Ağustos 2023 tarihi itibariyle ülkemizde faaliyet gösteren bir banka kripto cüzdan ve transfer işlemlerini duyurduğunu açıkladı (CHIP, 2023). Bitcoin ve diğer kripto para birimlerinin popülerliğinin artması bilgisayar korsanlarını da dijital paralara siber saldırı düzenleme hususunda motive etmektedir (Rezaeighaleh H, Zou C.C, 2022). Ülkemizde yakın zamanda bir kripto para borsa platformu sahibinin, borsasında işlem yapan kullanıcılarının hesaplarına erişimlerini durdurmak suretiyle yaklaşık 400.000 yatırımcının hesabında bulunan 2 milyar dolara yakın bir parayla beraber yurtdışına kaçtığı haberlerde yer almıştır (Bdturkey, 2023). Bu olay özelinde suç işleyen kişi veya kişilerin bu kadar parayı yurtdışına nasıl çıkarmış olduğu sorusu akıllara gelmektedir. Bu noktada sorumuzun cevabı, kripto varlıkların tutulduğu kripto para cüzdanlarıdır. Varlıklarının güvenli bir şekilde muhafaza edilebildiği kripto para cüzdanları gelecek dönemin en önemli konularından biri haline geleceği değerlendirilmektedir.

Kripto paralarla ilgili araştırmaların çoğu, blok zincir üzerinde ki işlemleri analiz ederek kullanıcıyı takip etmeye odaklanmış durumdadır. Son zamanlarda çeşitli araştırmacılar, kripto para cüzdanlarının bellek, disk ve ağ trafiği analizi yoluyla izini sürmeye çalışmışlardır (Tyler, 2020; Zollner, Kwang, Choo, Le-Khac. 2019). Bu kapsamda, Bitcoin kripto para cüzdanlarının kurulu olduğu windows işletim sistemine sahip bilgisayarların imajları ve RAM analizleri adli açıdan gerçekleştirildi (Doran, 2014; Jones, 2014; Van Der Horst, Kwang, Choo, Le-Khac, 2017;). Koerhuis, Kechadi ve Le-Khac, Linux işletim sistemine sahip bilgisayara kurulmuş olan Monero ve Verge isimli koinlere ait kripto para cüzdanlarını adli açıdan analizlerini gerçekleştirilmiştir. Çalışmada bilgisayarın RAM analizinden kritik bilgiler elde edilmiştir (Koerhuis, Kechadi, Le-Khac 2020). Montanezin yaptığı çalışmada, ios ve android cihazlarda Litecoin ve Darkcoin kripto paraları analiz edilmiştir (Montanez, 2014). Chang, Darcy, Choo ve Le-Khac, Android cihazlarda Bitcoin ve Dogecoin cüzdanlarını Ciphertrace programı ile analizini gerçekleştirilmiştir. Araştırmada cüzdan tanımlayıcı bilgileri, işlem tanımlayıcaları, zaman damgaları, email'ler, cookies ler gibi bilgiler elde edilebilmiştir (Chang, Darcy, Choo, Le-Khac, 2022). Mirza, Ozer ve Karabiyik, trush wallet ve metamask cüzdanların Ios ve android cihazlara kurulumu gerçekleştirilerek yapılan kripto para işlemlerinin sonuçları adli açıdan analiz edilmiştir (Mirza, Ozer, Karabiyik,2022). Blockchain teknolojisi adli bilişim açısından hala göreceli olarak yeni bir teknolojidir. Dolayısıyla WEB3 cüzdanlarda kripto para işlemleri yoğun bir şeklide artmaya devam ettiğinden bu alanların adli açıdan incelenmesine devam edilmelidir (Mirza, Ozer, Karabiyik,2022). Bundan dolayı çalışmanın amacı, bu alandaki boşluğu doldurmaya katkı sağlamak için dünya genelinde yaygın olarak kullanılan tronlink isimli sıcak cüzdan üzerinden yapılan kripto para transfer işlemlerinin Windows işletim sistemine sahip bilgisayarlarda ve android işletim sistemine sahip cihazlarda bıraktığı adli kalıntıların tespitini yapmaktır.

1.1. Kripto Para

Kripto paranın tanımı yapmadan önce kripto paraların üzerinde çalıştığı blok zincirin ne olduğunu tanımlamak gerekmektedir. Blok zincir, ürettiği defterin merkezsiz yapısı nedeniyle birçok kripto paranın üretiminde kullanılan temel teknolojidir (Mirza, Ozer, Karabiyik,2022). Tekniğin amacı dijital belgelere zaman damgası vurarak geriye dönük tarihlemeyi imkansız kılmaktır. Blok zincir banka veya hükümet gibi üçüncü taraf bir aracıya ihtiyaç duymadan para, mülk, sözleşmeler vb. ögelerin güvenli transferi için kullanılır (Smart Mind, 2023). Kripto para ise, kriptografik/şifreli olarak güvenli işlem yapmaya ve ek sanal para arzına olanak sağlayan dijital değerler olarak tanımlanmıştır (Çarkacıoğlu, 2016). Kripto paralar "Bitcoin" adıyla ilk kez Satoshi Nakamoto takma isimli kişi veya kişilerin Ekim 2008'de yayınladığı "Bitcoin: A Peer-to-Peer Electronic Cash System", isimli makalesiyle dünyaya duyurulmuştur. Makalede Bitcoin'in dünyada yeni bir uluslararası para birimini temsil edecek dijital bir coin olacağı belirtilmektedir (Nakamoto, 2008). Bugün kripto paraların sayısı binlere ulaşmıştır (Usta, Doğantekin, 2017). Günümüz şartlarında bu paraların güvenilirliği, blok zincir ağında dağınık vaziyette bulunan ve merkezi olmayan kullanıcılar tarafından sağlanmaktadır. İşlem güvenliği yüzde %51 çoğunluğun onayı ile kayıtların bloklar halinde işlenmesi ve teyit edilmesi ile onaylanmış kesin sonuçlardır.

1.2. Kripto Para Cüzdanı

Kripto para cüzdanları, çeşitli blok zincirler ile etkileşime geçerek kripto varlıkların alınmasına ve gönderilmesine olanak sağlayan yazılımlardır (Martino, 2021). Kripto para cüzdanları, public key (genel anahtar)

ve private key (özel anahtar) bilgilerini içeriğinde tutan aynı zamanda kripto varlıkları da içeriğinde barındıran dijital ortamlardır (Jokić S, et al., 2019). Genel ve özel anahtar bilgileri kriptografik şifreleme algoritmalarıyla oluşturulmaktadır. Kriptografik şifrelemeler, dijital dünyada güvenliğin ve gizliliğin korunmasında hayati öneme sahiptir. RSA (Rivest-Shamir-Adleman) (Rivest, Shamir, Adleman, 1978) ve ECC (Eliptik Eğri Kriptografisi) (Koblitz, 1987), gibi asimetrik şifreleme algoritmaları, bu alanda uzun yıllardır kullanılan ve kabul görmüş yöntemlerdendir. Kripto para cüzdanlarında ECC ve RSA kriptolojik şifreleme yöntemleri sıklıkla kullanılabilmektedir. Genel anahtar bilgisi banka hesap numarası/IBAN (International Bank Account Number) numarası bilgisi olarak, özel anahtar bilgisi ise kullanıcı şifresi olarak düşünülebilir. Kullanıcılar arasında yapılan kripto para transfer işlemlerinde fiziki bir para değişimi bulunmamakta olup, yapılan her işlem blok zincire ve kripto para cüzdanı içerisine kaydedilmektedir (Jokić S, et al., 2019).

1.3. Kripto Para Cüzdan Tipleri

Kripto para cüzdanları genel olarak; soğuk/kağıt cüzdan (cold/paper wallet), donanım cüzdan (hard wallet) ve sıcak cüzdan (hot wallet) olarak adlandırılmaktadır (Khan, Zahid, Hussain, Riaz, 2019). Sıcak cüzdanlarda kendi aralarında kuruldukları ortama göre, "Online", "Desktop" ve "Mobile" olarak kategorilere ayrılmaktadır. Kripto para cüzdanlarına ait genel özellikler Tablo 1'de gösterilmiştir (Bulut, Sertkaya, 2020).

Tablo 1. Kripto para cüzdanların özellikleri.

	Cüzdanlar **(Wallet (From Hot to Cold))**				
Özellikleri **(Specifications)**	İnternet Üzerinden **(Online)**	Masaüstü **(Desktop)**	Mobil **(Mobile)**	Donanım **(Hardware)**	Kağıt **(Paper)**
Fiziksel **(Physical)**	X	X	X	√	√
Her zaman Erişime Açık **(Always online)**	√	√	√	X	X
Anahtarları tutmak için bir donanıma sahip **(Own hardware to keep keys)**	X	X	X	√	√
İşlemleri doğrulamak için tüm blok zincire ihtiyaç duyuyor **(Need whole Blockchain to verify transaction)**	√	√	X	X	X
Donanımsal hataya veya kayba yatkınlığı varmı **(Prone to hardware failure or loss)**	X	X	X	√	√
Farklı coin tiplerini kolayca ekler ve destekler **(Easy to support or add different coin types)**	√	√	√	X	X

1.3.1. Soğuk(Kağıt) cüzdan

Kağıt cüzdanlar, kripto paraların çevrimdışı olarak depolandığı bir soğuk cüzdan sistemidir. Bu cüzdanlar, ilgili internet sitelerine girilerek kullanıcı tarafından oluşturulabilir. Cüzdan üzerinde genel anahtar ve özel anahtar bilgisinin Hash değerleri bulunmaktadır. Hash değerleri verilerin bütünlüğünü kontol etmek için kullanılan ve ait olduğu verinin ilk sektöründen son sektörüne kadar bütün bitlerin özel bir algoritmik işleme tabi tutulması sonucu eşsiz bir sabit değer oluşturan matematiksel değer bütünüdür (Okuyucu, 2020). Kağıt cüzdanlar kullanılarak kripto para işlemleri (transfer, alım/satım) yapabilmek için öncelikli olarak internet bağlantısı olan bir bilgisayar üzerinden ilgili kripto para borsasına erişim sağlamak gerekmektedir. Cüzdanın üzerinde bulunan genel ve özel anahtara ait hash bilgileri girilmek suretiyle içeriğine erişim sağlanıp istenilen işlemler yapılabilir.

Bu tip cüzdanlar genellikle kağıt üzerinde fiziksel ortamlarda tutulurlar. Özellikle yetkisiz erişim sağlamaya çalışanlara karşı özel anahtarların zor ulaşılır olması kripto varlıkların korunması açısından önem arz etmektedir.

Büyük miktarlarda kripto para birimlerini depolamak veya değerli dijital varlıkların korunmasını sağlayan bir "sakla ve tut" yatırım stratejisi için ideal cüzdan tipleridir (Khan, Zahid, Hussain, Riaz, 2019).

1.3.2. Donanım cüzdan

Donanım cüzdan, kullanıcının genel ve özel anahtarları ile kripto varlıklarını güvenli bir donanım aygıtında (genellikle USB bellek formunda) depolayan en güvenli cüzdan tiplerinden bir tanesidir (Rezaeighaleh, Zou, 2022). Bu tip cüzdanlara kötü amaçlı yazılımlar ve şahıslar kolayca erişim sağlayamazlar. Öncelikli olarak bu cüzdanların kurulumu yapıldıktan sonra kullanıcıya cüzdan içerisinde kayıtlı bulunan kelimelerden rastgele olarak 12 veya 24 tanesi seçtirilerek özel anahtar bilgisi oluşturulur. Bu bilgiler ayrıca başka bir ortama da kaydı yapılır. Donanım cüzdanlarının kaybolması veya bozulması gibi durumlarda başka ortamlara kaydı oluşturulan özel anahtar bilgisi sayesinde içerisindeki kripto varlıklara tekrar erişim sağlanabilmektedir (Karame, Androulaki, 2016). Cüzdanın kullanımı için ayrıca bir PIN kodu belirlenir. Bu işlemlerinin bitimine müteakip ilgili kripto paraların transfer işlemlerinin yapılabilmesi için blok zincir ağ altyapıları eklenir. Her blok zincir ağ alt yapısının ayrı bir genel anahtar bilgisi bulunmaktadır. Örneğin kullanıcı bitcoin ve ethereum blok zincir ağ alt yapısı kurmuş ise kullanıcının 2 ayrı genel anahtar bilgisi bulunmaktadır. Buradaki blok zincir ağ alt yapıları ayrı banka hesapları olarak düşünülebilir.

1.3.3. Sıcak cüzdan

Sıcak cüzdan, kripto para cüzdan türlerinden bir tanesi olup, bünyesinde genel ve özel anahtarlarla birlikte kripto varlıklarının tutulduğu yazılımlardır. Bu cüzdanlar bir tarayıcı uzantısı, mobil uygulama veya masaüstü uygulaması olabilmektedir. Bu sebeple kullanıcılar kripto varlıklarına istedikleri zaman erişimde bulunabilmektedirler (Suratkar, Shirole, Bhirud, 2020). Sıcak cüzdanların kullanılabilmesi için uygulamanın bulunduğu cihazın internet bağlantısının yapılmış olması gerekmektedir. Bu nedenle de virüs ve saldırılara karşı sürekli olarak korunmaları gerekmektedir (Karame, Androulaki, 2016). Diğer cüzdanlardan farklı olarak bu cüzdanlar şu an itibari ile dünya genelinde en çok tercih edilen türleridir. Bu cüzdanların çalışma prensibi diğer kripto para cüzdanlarının şifreleme ve kriptografi mantığıyla aynıdır.

2. Gereç ve Yöntem

2.1. Gereç

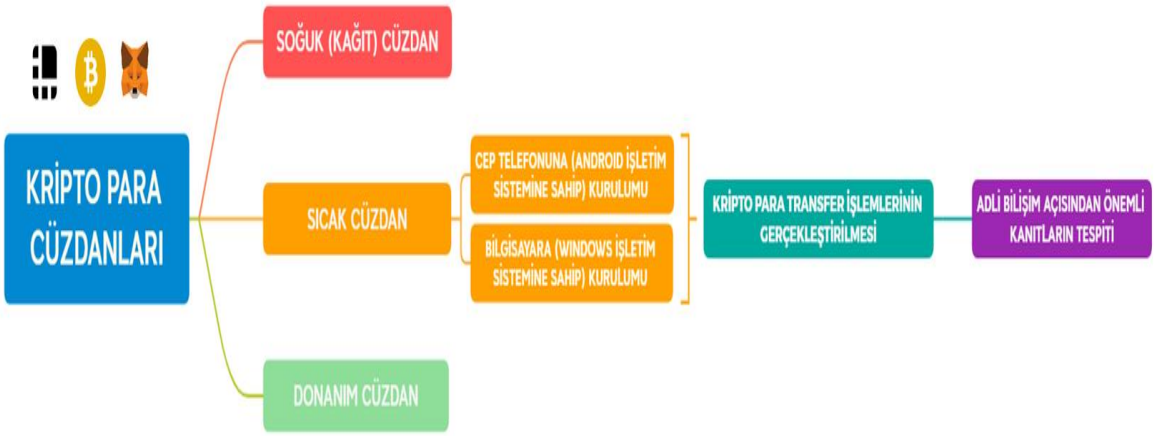
Bu çalışmada Windows ve android işletim sistemine sahip cihazlarda tronlink uygulaması üzerinden yapılan kripto para transfer işlemlerinin tespiti amacıyla Tablo 2'de belirtilen donanım ve yazılımlar kullanılmıştır.

Tablo 2 Kullanılan donanım ve yazılımlar

➢ Lenovo marka, P920 model iş istasyonu (Virtual Box sanal makinesi kurulum aşamasında kullanılmıştır)	➢ Android 12.15. İşletim sistemine sahip Xiaomi M2101K6G Cep Telefonu
➢ Windows 10 Pro 64 bit işletim sistemi.	➢ Google Chrome Web Tarayıcı (115.0.5790.170)
➢ X-Ways Forensics Adli Bilişim Yazılımı (Version 19.8)	➢ Tron Link Eklentisi (3.28.4)
➢ UFED 4PC Adli Bilişim Yazılımı (7.54.0.444)	➢ Oracle VM VirtualBox(6.1.12)
➢ UFED 7.57.0.13 mobil adli bilişim yazılımı	➢ Unix Timestamp Converter
➢ Android işletim sistemi için uyumlu Tron Link Uygulaması	➢ Virtualbox Sanal Makine 6.1.12
➢ SBH SQLite Manager (1.3)	

2.2. Yöntem

Sıcak cüzdanının çalışma prensibinin tespiti amacıyla Şekil 1'de belirtilen işlemler sırasıyla bilgisayar ve cep telefonu içerisine gerçekleştirilmiştir.

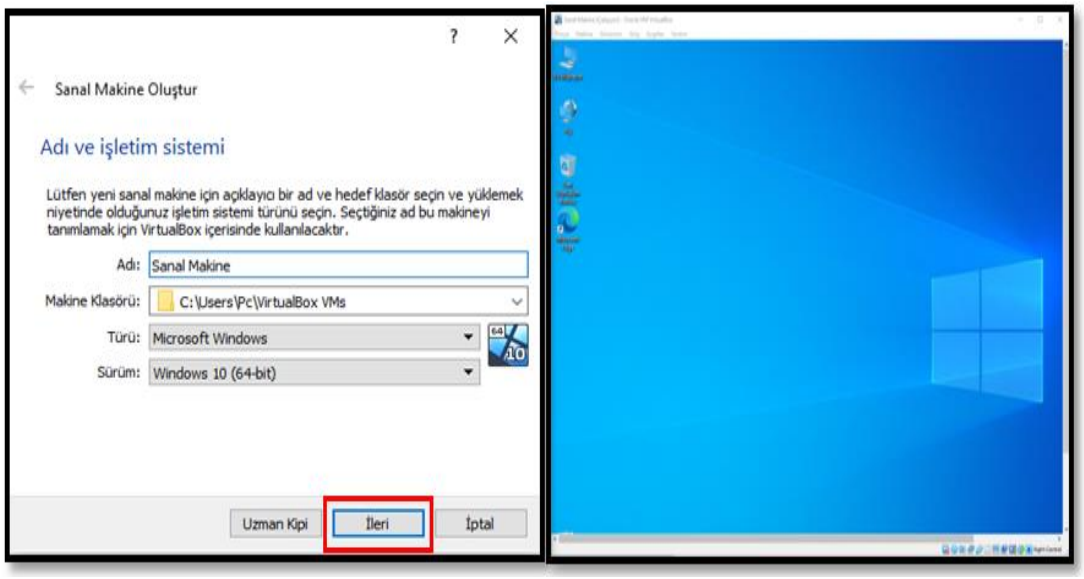


Şekil 1. Çalışmanın akış şeması

2.2.1. Sıcak cüzdanın bilgisayar içerisinde yapılan işlemleri

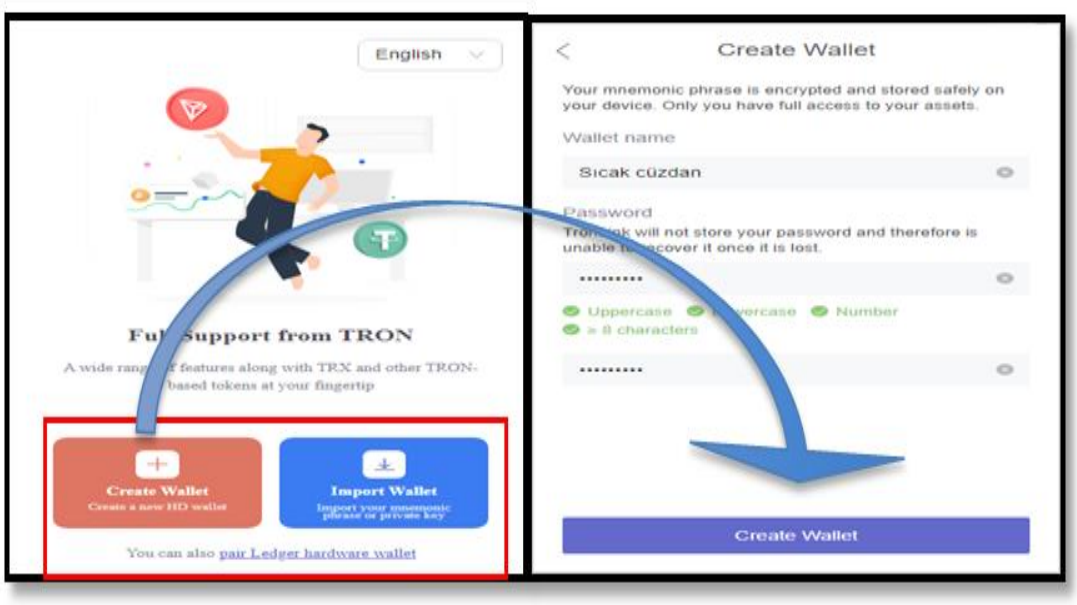
2.2.1.1. Kurulum işlemleri

Öncelikle Windows 10 işletim sistemine sahip bilgisayar içerisinde Virtualbox sanal makine kurulumu gerçekleştirilmiştir (Şekil 2).



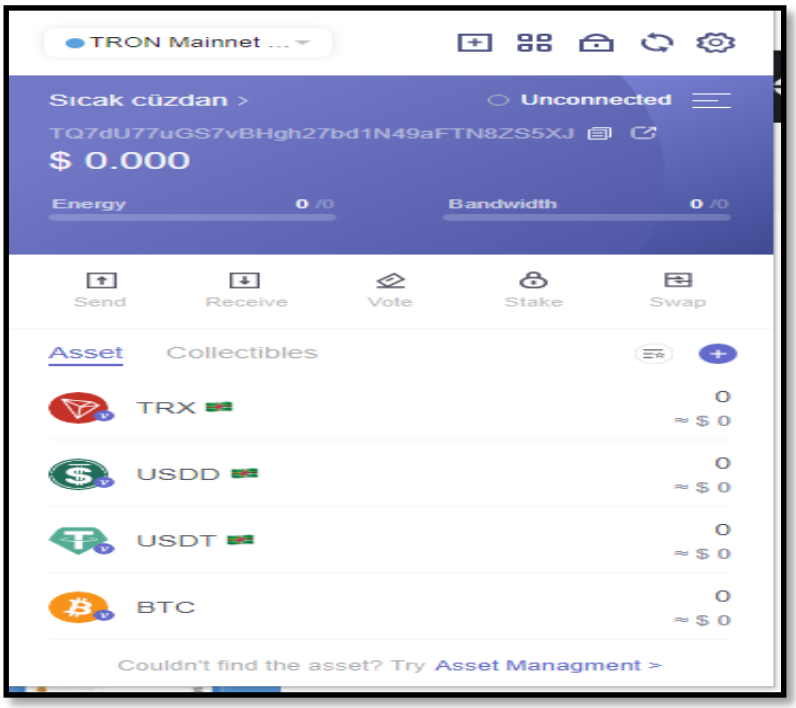
Şekil 2. Sanal makine kurulumu görünümü

Kurulan sanal makine içerisinde bulunan Google Chrome Web tarayıcısına sıcak cüzdana ait olan "Tronlink Wallet" eklentisi kurulmuştur. Sonraki aşamada "TronLink" eklentisi üzerinden açılan pencerede kullanıcıya yeni bir cüzdan mı oluşturacağı "Create Wallet", yoksa daha önce oluşturduğu sıcak cüzdan bilgilerini mi gireceği "Import Wallet" bilgisi sorulmaktadır. Bu aşamada "Create Wallet" sekmesi seçilerek "Sıcak Cüzdan" isimli bir cüzdan kurulumu gerçekleştirilmiştir. Cüzdana giriş yaparken kullanılmak üzere gerekli olan parola oluşturma işlemi gerçekleştirilmiştir (Şekil 3).



Şekil 3. Sıcak cüzdanın kurulumu ve parola oluşturma

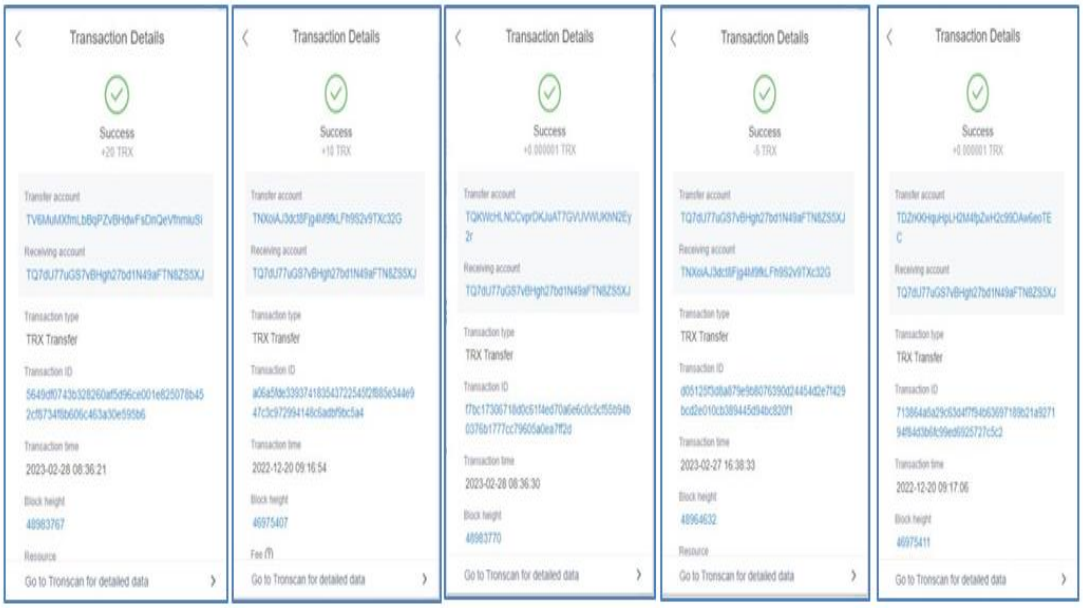
Sıcak cüzdanı yeni oluşturacağımız için kurtarma kelimeleri seçilerek cüzdan kurulumu tamamlanmıştır. Kurulan sıcak cüzdana ait "Public Key" numarasının **"TQ7dU77Ugs7vBHgh27bd1N49aFTH8ZS5XJ"** olduğu tespit edilmiştir (Şekil 4).



Şekil 4. Sıcak cüzdanın genel anahtar numarasının görüntülenmesi

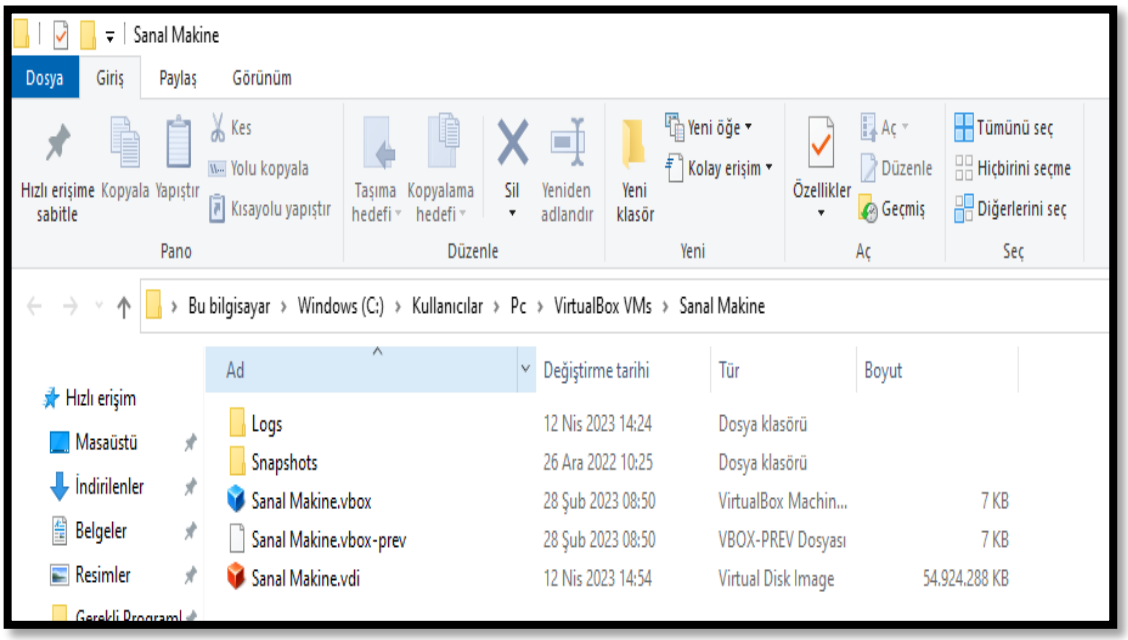
2.2.1.2. Kripto para transfer işlemleri

Binance kripto para platformunun web sitesine girilerek daha önce kurulmuş olan **Public Key "TQ7dU77Ugs7vBHgh27bd1N49aFTH8ZS5XJ"** numaralı hesaba transfer işlemleri(5 işlem) gerçekleştirilmiştir (Şekil 5).



Şekil 5. Sıcak cüzdanın transfer işlemleri

Kripto para transfer işlemlerin gerçekleştirildiği sanal makineye ait disk imajları, üzerinde incelemeler gerçekleştirilmek üzere arşivlenmiştir (Şekil 6).

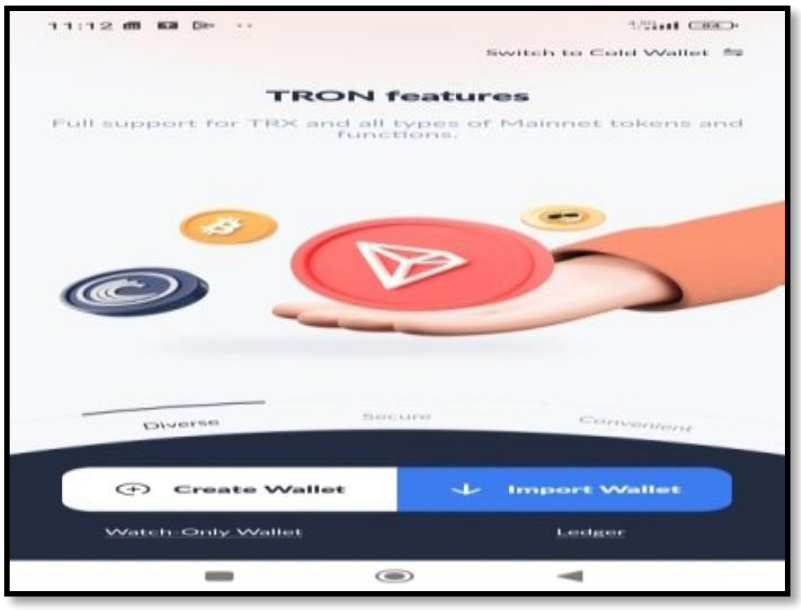


Şekil 6. Sanal makine arşiv dizini

2.2.2. Sıcak cüzdanın cep telefonu içerisinde yapılan işlemleri

2.2.2.1. Kurulum işlemleri

Cep telefonunun Play Store uygulaması üzerinden, Tronlink sıcak cüzdanına ait apk indirilip, yükleme işlemi gerçekleştirilmiştir. Tronlink pro uygulaması cep telefonuna indirildikten sonra kullanıcıya yeni bir cüzdan mı oluşturacağı (Create Wallet) yoksa daha önce oluşturduğu sıcak cüzdan bilgilerini mi gireceği (Import Wallet) bilgisi sorulmaktadır (Şekil 7).



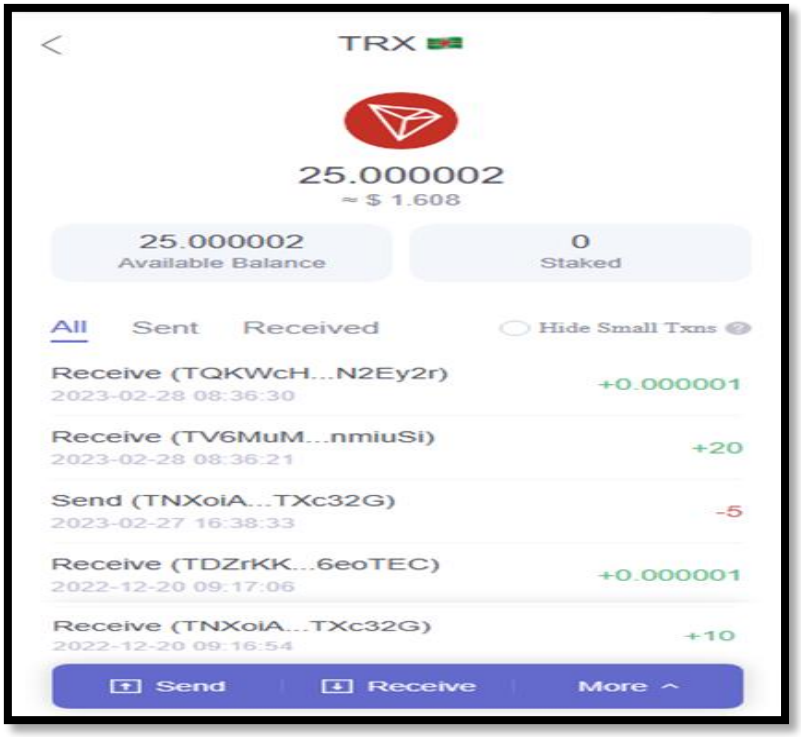
Şekil 7. Sıcak cüzdan kurulum aşaması

Bu aşamada "Import Wallet" seçeneği seçilerek daha önceden bilgisayar ortamında oluşturulup üzerinde işlemler gerçekleştirilen sıcak cüzdana ait kurtarma anahtar kelimeleri girilmiş ve cüzdan içeriğine erişim sağlanmıştır (Şekil 8).

Şekil 8. Kurtarma kelimelerinin seçim sırası

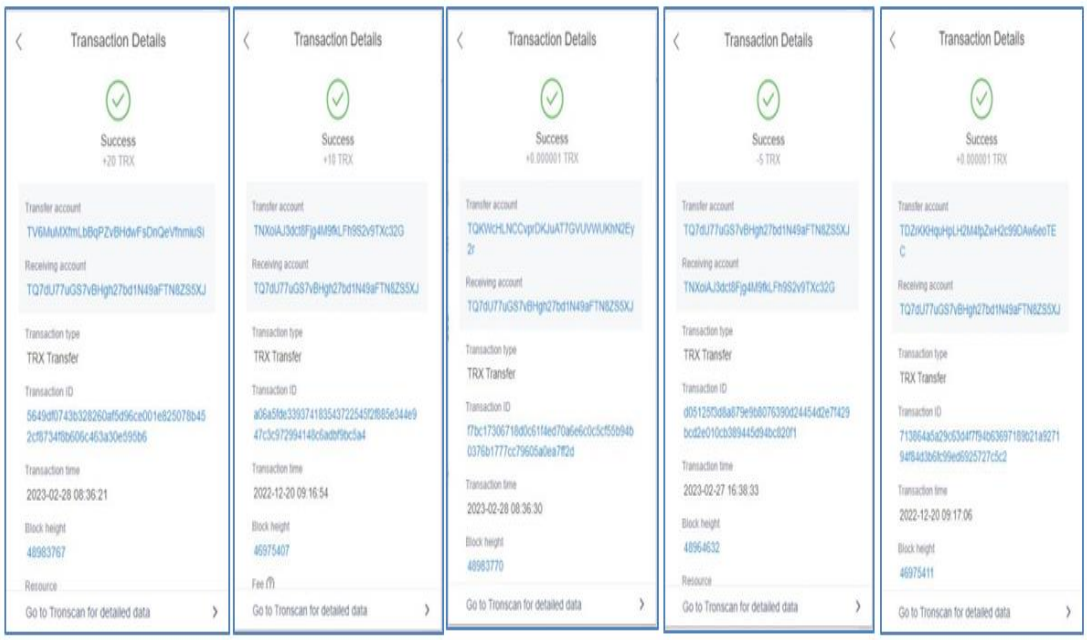
2.2.2.2. Transfer işlemlerinin görüntülenmesi

Sıcak cüzdan içeriğinde bulunan kripto varlıklara ait tüm işlemler toplu olarak (5 işlem) görüntülenmiştir (Şekil 9).



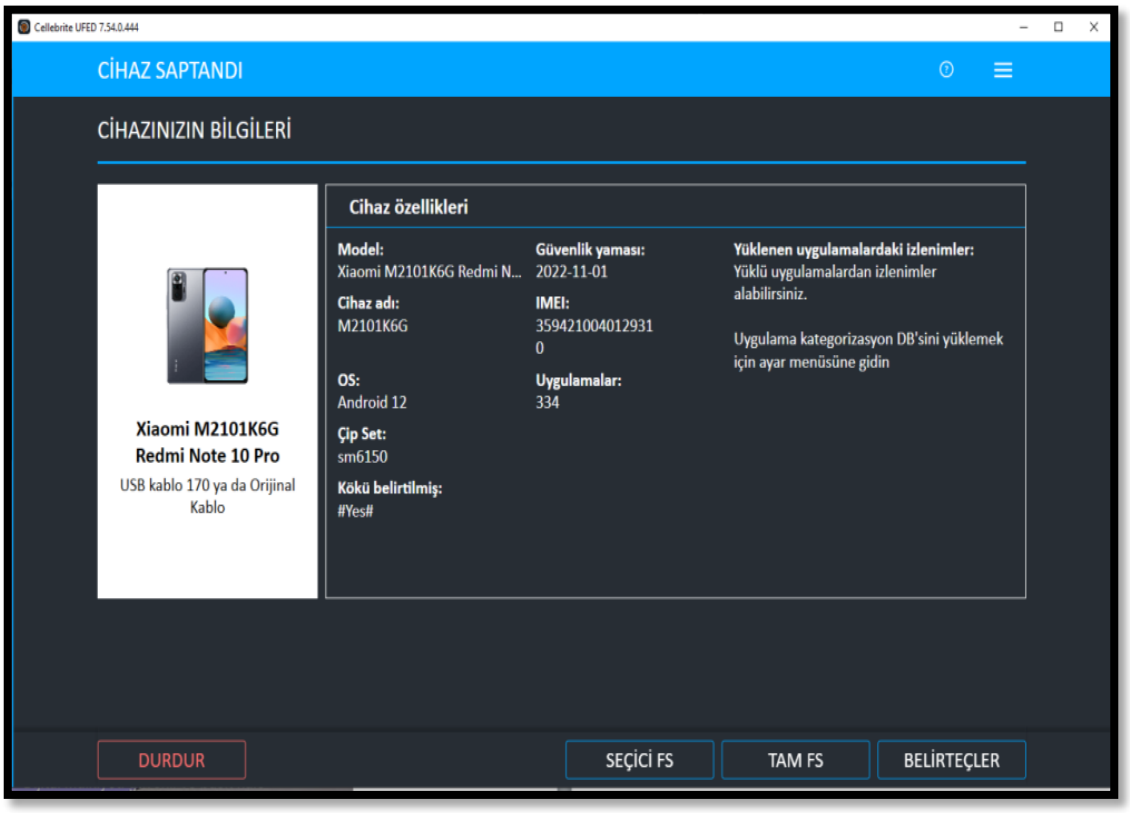
Şekil 9. Sıcak cüzdan içerisindeki kripto varlıkların görüntülenmesi

Sıcak cüzdan içeriğinde bulunan kripto varlıklara ait tüm işlemler (5 işlem) ayrı ayrı görüntülenmiştir. Yapılan her bir işlem kaydı içerisinde, gönderici adresi (transfer account), alıcı adresi (receiving account), yapılan işlemin bilgisi (transection ID), işlem zamanı (transaction time), yapılan işlem bloğunun numarası (block height) ve işlem ücreti (fee) bilgisi bulunmaktadır (Şekil 10).



Şekil 10. Sıcak Cüzdan içerisindeki kripto varlıkların görüntülenmesi

Tüm işlemler tamamlandıktan sonra UFED 7.54.0.444 mobil adli bilişim yazılımı ile Dosya Sistemi (QualcommLive) kopya alma yöntemi ile kopyası alınmıştır (Şekil 11).



Şekil 11. Cep Telefonu Kopya Alma İşlemi Görünümü

3. Bulgular

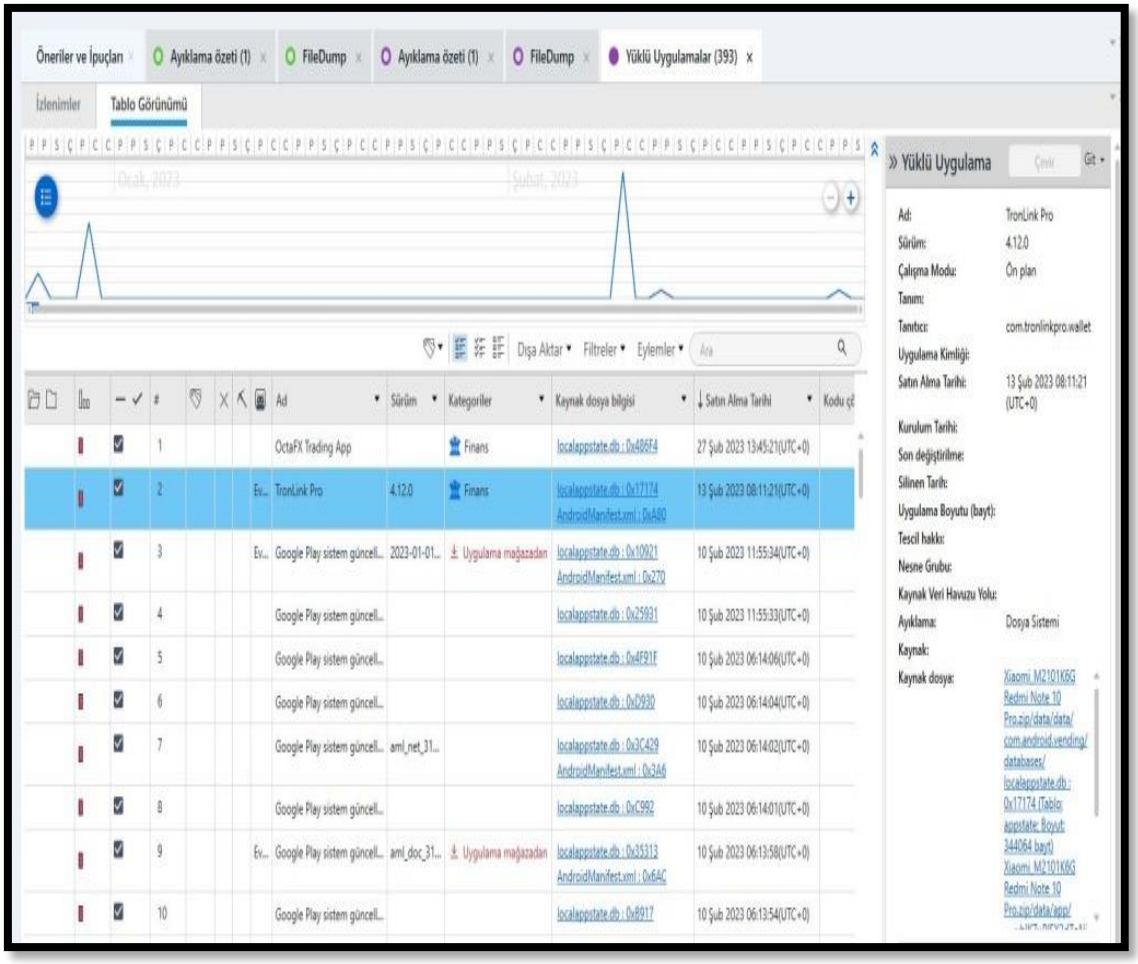
3.1. Cep telefonu içerisinden;

3.1.1. Sıcak cüzdanın kurulum işleminin tespiti

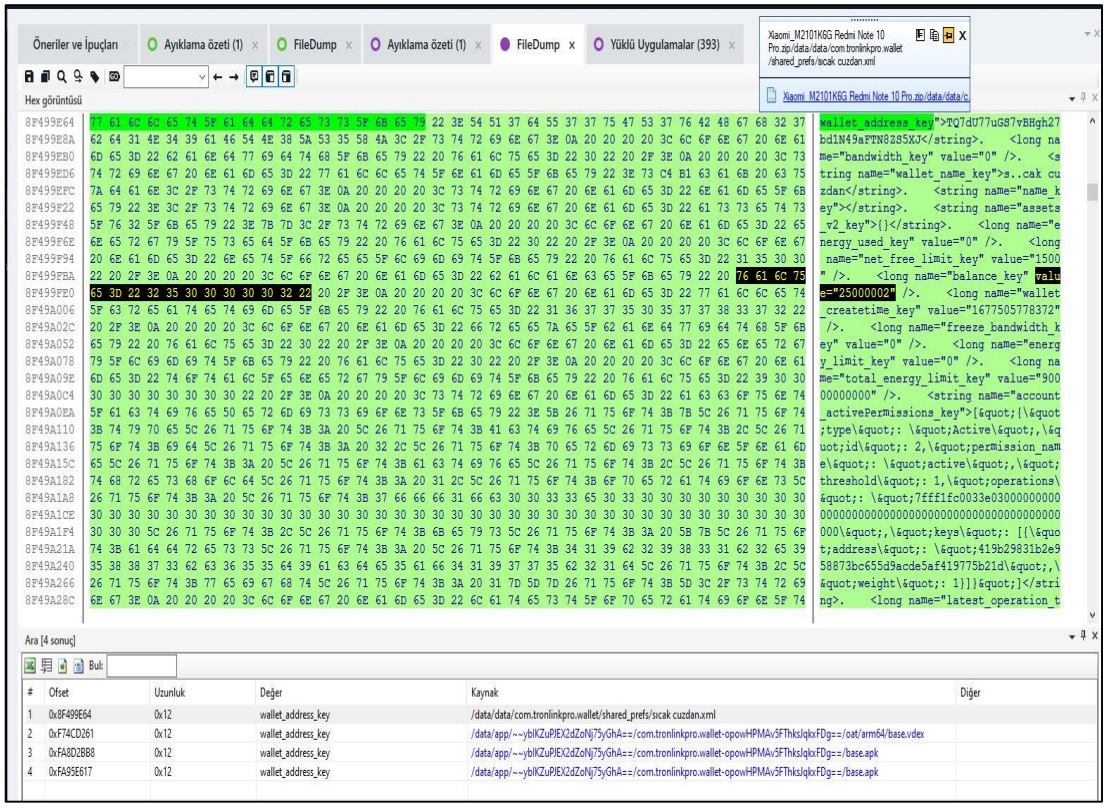
Cep telefonunun alınan kopyası UFED Phsiycal Analyzer 7.57 adli bilişim yazılımı ile yapılan incelemesinde, tarafımızca kurulan "TronLink Pro 4.12.0" isimli sıcak cüzdanın "Yüklü Uygulamalar" içerisinde kayıtlı bulunduğu tespit edilmiştir. "TronLink Pro 4.12.0" isimli uygulamanın tanıtıcı bilgisinin ise "com.tronlinkpro.wallet" olduğu görülmüştür (Şekil 12).

3.1.2. Sıcak cüzdanın transfer işlemlerinin tespiti

Sıcak cüzdanın kurulumu ile oluşturulan **"TQ7dU77Ugs7vBHgh27bd1N49aFTH8ZS5XJ"** isimli Public Key bilgisi UFED 7.57.0.13 mobil adli bilişim yazılımı içerisinde anahtar kelime olarak aratılmış olup; Arama sonucunda "/data/data/com.tronlinkpro.wallet/shared_prefs/sıcak cuzdan.xml" dosyası içerisinde "wallet_address_key" ibaresi sonrasında tespit edilmiştir (Şekil 13).

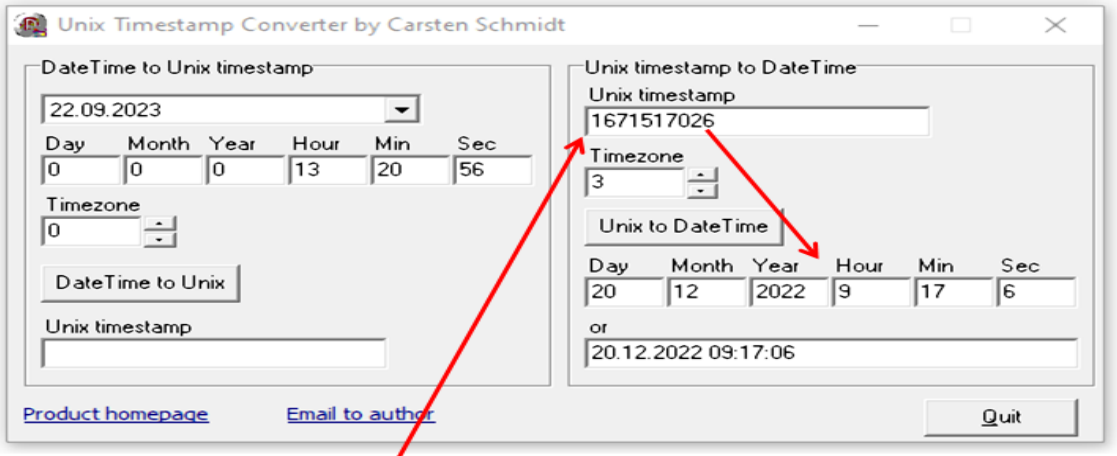


Şekil 12. UFED adli bilişim yazılımı ile kurulum bilgisinin listelenmesi



Şekil 13. UFED adli bilişim yazılımı ile genel anahtar bilgisinin tespiti

Arama sonucunda "/data/data/com.tronlinkpro.wallet/cache" adresi içerisinde, 2.2.1.2'de yapılan 5 adet işleminde kaydının bulunduğu tespit edilmiştir. Her işlem kaydı öncesinde "contractsMap" ibaresinin bulunduğu tespit edilmiştir. **Şekil-13'de** gösterilen bilgiler **Şekil-14'ün** 2. sırasında belirtilen işleme ait kayıttır. Kayıt içerisinde bulunan tarih bilgisi UNIX Time formatında olduğundan "Unix Timestamp Converter" yazılımı ile güncel tarih bilgisine dönüştürülmüştür (Şekil 14).



{"code":200,"contractMap":{"TNXoiAJ3dct8Fjg4M9fkLFh9S2v9TXc32G":false,"TQ7dU77uGS7vBHgh27bd1N49aFTN8ZS5XJ":false,"TDZrKKHquHpLH2M4fpZwH2c99DAw6eoTEC":false},"data":[{"amount":"1","block_timestamp":1671517026000,"block":46975411,"from":"TDZrKKHquHpLH2M4fpZwH2c99DAw6eoTEC","to":"TQ7dU77uGS7vBHgh27bd1N49aFTN8ZS5XJ","hash":"713864a5a29c63d4f7f94b63697189b21a927194f84d3b6fc99ed6925727c5c2","confirmed":0,"contract_type":"TransferContract","contractType":1,"revert":0,"contract_ret":"SUCCESS","symbol":"","issue_address":"","decimals":6,"token_name":"","direction":2}

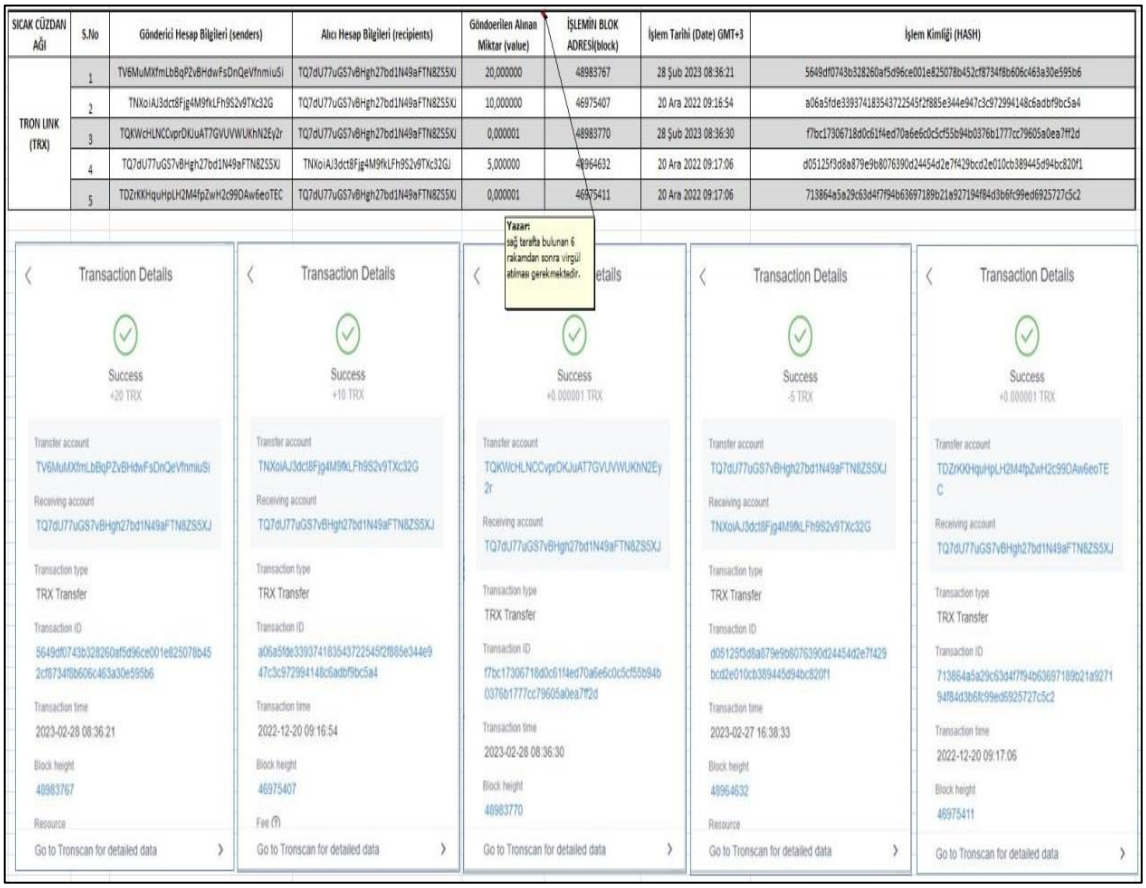
Şekil 14. Kripto para işlem kaydının yapısı

Söz konusu kayıt içeriğinin Tablo 3'te belirtilen yapıda olduğu anlaşılmıştır.

Tablo 3. Tespit edilen kayıt içeriğinin gösterimi

"amount:10000000"	Transfer edilen kripto para miktarı (sondaki 6 sıfır küsüratı temsil etmektedir)
"block:46975407"	Transfer işleminin kaydının tutulduğu block numarası
"block_timestamp:1671517014000"	Transfer işlem zamanı
confirmed:1	İşlem onaylama bilgisi
from: TNXoiAJ3dct8Fjg4M9fkLFh9S2v9TXc32G	Transfer işleminde Gönderici Adres Bilgisi
hash":"a06a5fde339374183543722545f2f885 e344e947c3c972994148c6adbf9bc5a4"	Transfer işlemine ait Hash Bilgisi
to":"TQ7dU77uGS7vBHgh27bd1N49aFTN8ZS5XJ"	Transfer işleminde Alıcı Adres Bilgisi

Tespit edilen tüm işlemlere **(5 adet transfer işlemi)** ait transfer bilgileri Şekil 15'de sunulmuştur.



SICAK CÜZDAN AĞI	S.No	Gönderici Hesap Bilgileri (senders)	Alıcı Hesap Bilgileri (recipients)	Gönderilen Alınan Miktar (value)	İŞLEMİN BLOK ADRESİ(block)	İşlem Tarihi (Date) GMT+3	İşlem Kimliği (HASH)
TRON LINK (TRX)	1	TV6MuMXfmLbBqPZvBHdwFsDnQeVfnmiuSi	TQ7dU77uGS7vBHgh27bd1N49aFTN8ZS5XJ	20,000000	48983767	28 Şub 2023 08:36:21	5649df0743b328260af5d96ce001e825078b452cf8734f8b606c463a30e595b6
	2	TNXoiAJ3dct8Fjg4M9fkLFh9S2v9TXc32G	TQ7dU77uGS7vBHgh27bd1N49aFTN8ZS5XJ	10,000000	46975407	20 Ara 2022 09:16:54	a06a5fde33937418354372254 5f2f885e344e947c3c97299414 8c6adbf9bc5a4
	3	TQKWcHLNCCvprDKJuAT7GVUVWUKhN2Ey2r	TQ7dU77uGS7vBHgh27bd1N49aFTN8ZS5XJ	0,000001	48983770	28 Şub 2023 08:36:30	f7bc17306718d0c61f4ed70a6e6c0c5cf55b94b0376b1777cc79605a0ea7ff2d
	4	TQ7dU77uGS7vBHgh27bd1N49aFTN8ZS5XJ	TNXoiAJ3dct8Fjg4M9fkLFh9S2v9TXc32GJ	5,000000	48964632	20 Ara 2022 09:17:06	d05125f3d8a879e9b8076390d24454d2e7f429bcd2e010cb389445d94bc820f1
	5	TDZrKKHquHpLH2M4fpZwH2c99OAw6eoTEC	TQ7dU77uGS7vBHgh27bd1N49aFTN8ZS5XJ	0,000001	46975411	20 Ara 2022 09:17:06	713864a5a29c63d4f7f94b63697189b21a927194f84d3b6fc99ed6925727c5c2

Şekil 15. Tespit edilen kayıt içeriklerinin gösterimi

3.2. Bilgisayar içerisinden,

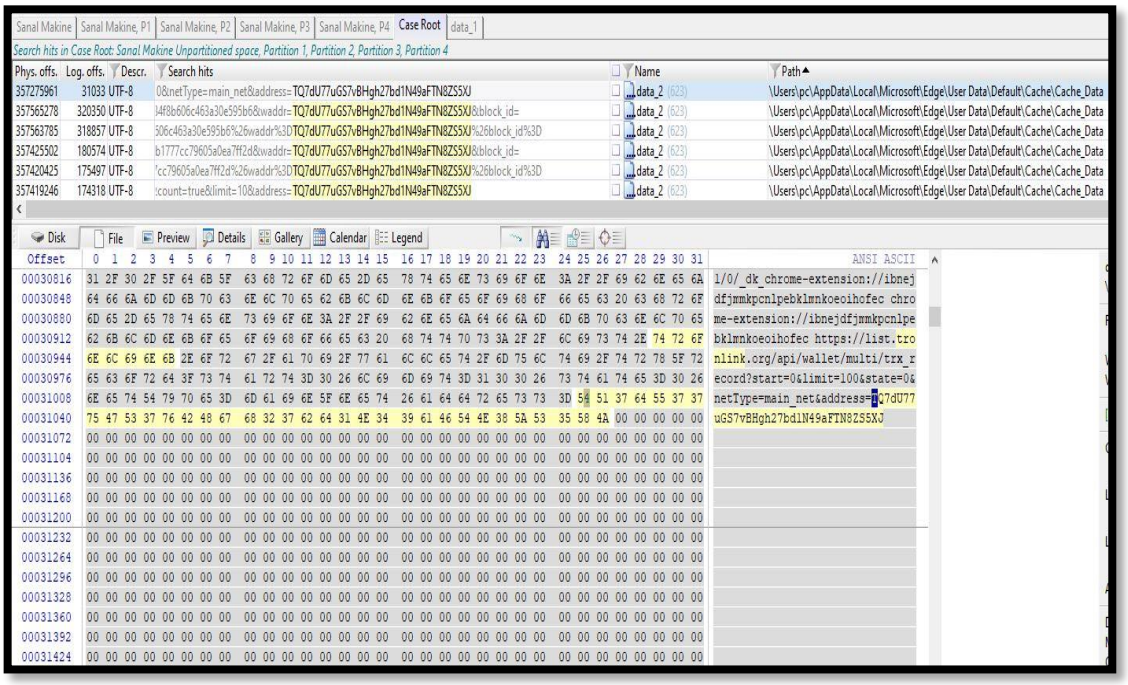
3.2.1. Sıcak cüzdanın kurulum işleminin tespiti

Sıcak cüzdana ait tronlink eklentisinin tespiti amacıyla kurulum esnasında oluşturulan **"TQ7dU77uGS7vBHgh27bd1N49aFTN8ZS5XJ"** Public Key bilgisi, X-Ways adli bilişim yazılımı ile anahtar kelime olarak aratılmıştır. Arama sonucunda; "\Users\pc\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data" isimli klasör dizini altında bulunan "Web Data" dosyası içerisinde, Public Key bilgisi ile birlikte Chrome tarayıcısına kurulan Tronlink sıcak cüzdan eklentisine ait kayıtlar tespit edilmiştir (Şekil 16).

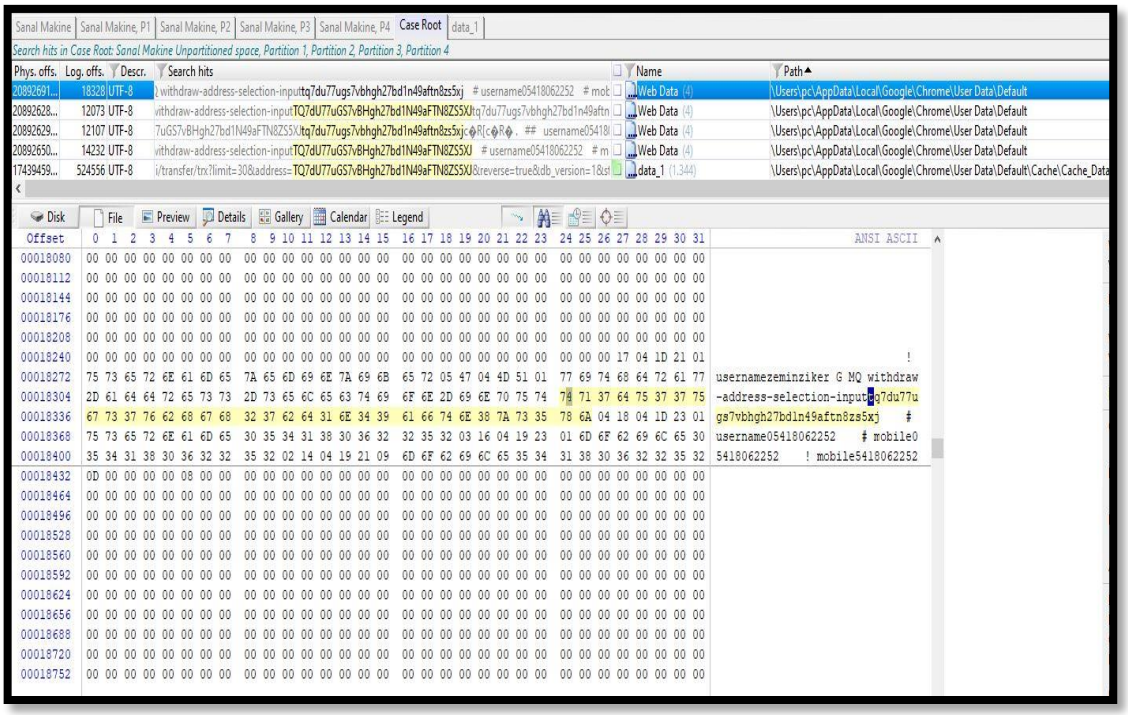
Ayrıca Public Key bilgisinin kurulduğu Google Chrome tarayıcısında oturum açan kullanıcı bilgilerini de ***(usernamezemin*****, username0541806****)*** getirdiği tespit edilmiştir (Şekil 17).

3.2.2. Sıcak cüzdanın transfer işlemlerinin tespiti

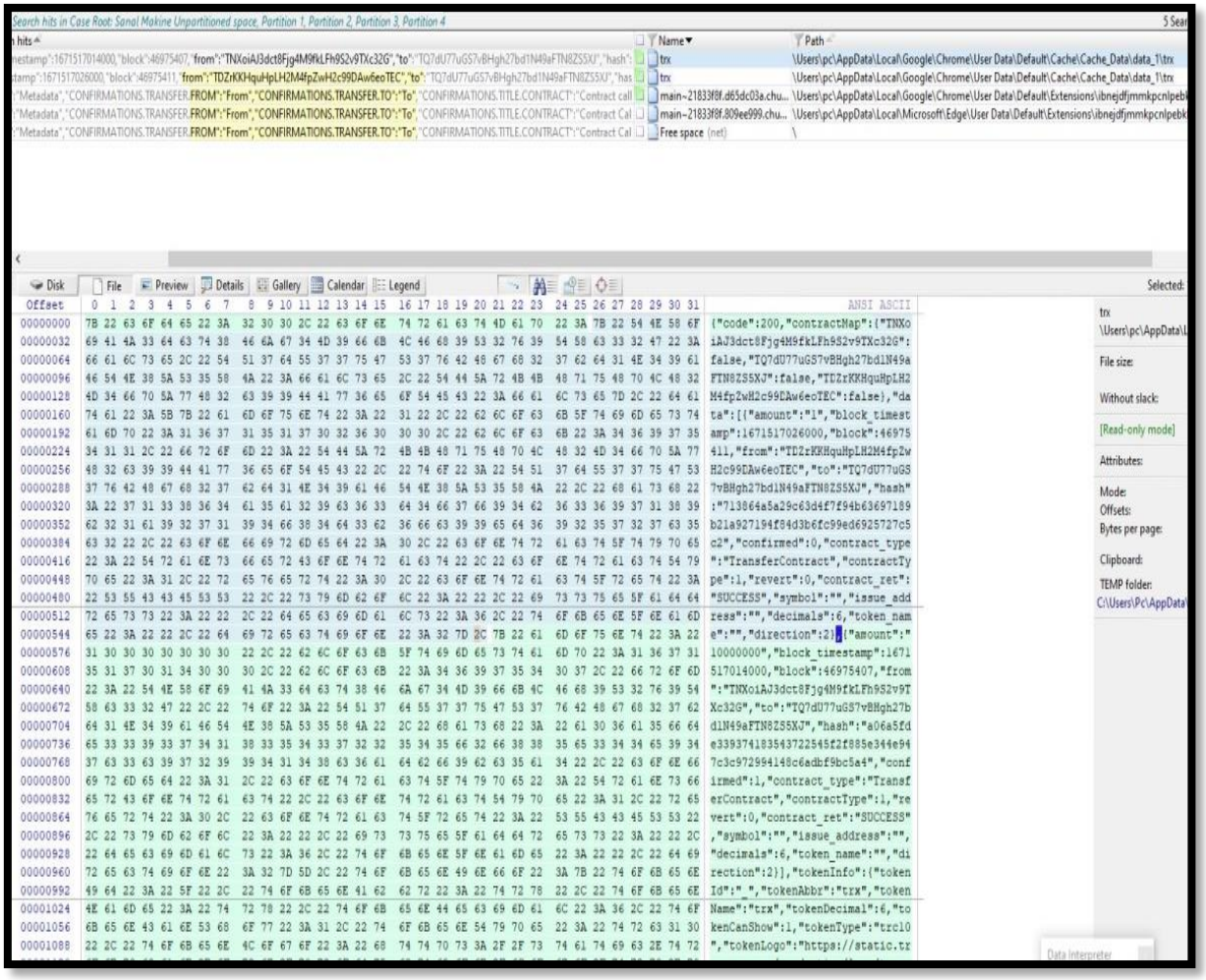
Bilgisayara ait sanal makine yedek dosyalarının, X-Ways adli bilişim yazılımı ile yapılan incelemesinde *(Cep telefonuna ait kopya incelemesinde tespit edilen ve gönderici/alıcı bilgilerinin kaydını tutan yapı analiz edilerek imaj içerisinde tüm transfer işlemlerinin tespitini yapacak anahtar kelime oluşturulmuştur)* tarafımızca oluşturulan **"from":".{30,45}"to"** anahtar kelimesi kopya içerisinde aratıldığında \Users\pc\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data \data_1\trx" isimli klasör dizini altında bulunan "trx" dosyası içerisinde tüm işlemler tespit edilmiştir (Şekil 18).



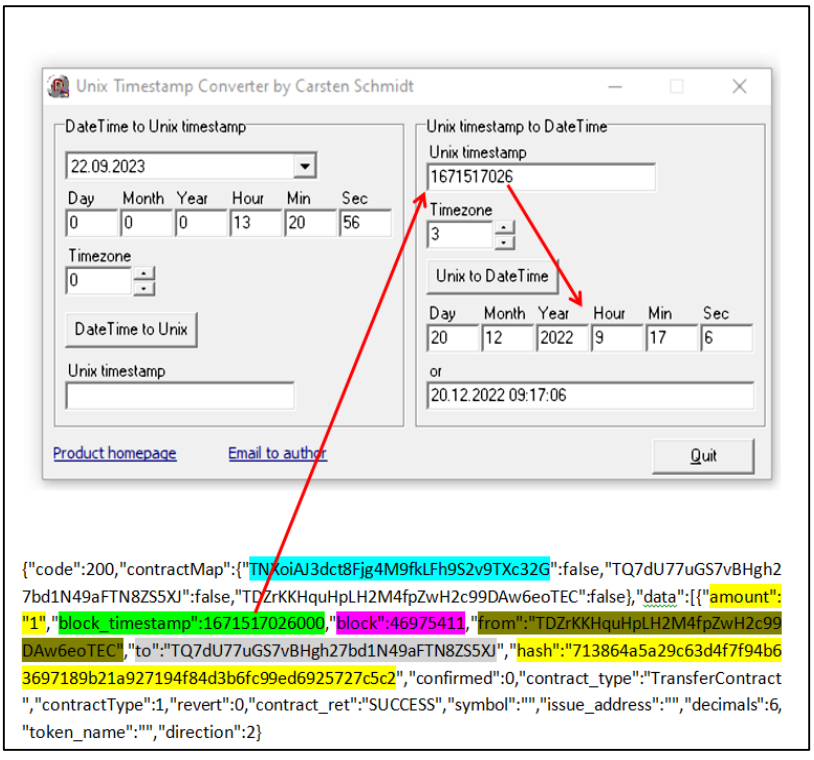
Şekil 16. X-Ways adli bilişim yazılımı ile genel anahtar bilgisinin tespiti



Şekil 17. X-Ways adli bilişim yazılımı ile kullanıcı bilgilerinin tespiti



Şekil 18 X-Ways adli bilişim yazılımı ile transfer işlemlerinin bilgisinin tespiti



Şekil 19. Kripto para işlem kaydının yapısı

Şekil 18'de gösterilen kayıt **Şekil 14'ün** 5. sırasında belirtilen işleme ait kayıttır. Kayıt içerisinde bulunan tarih bilgisi UNIX Time formatında olduğundan **"Unix Timestamp Converter"** yazılımı ile güncel tarih bilgisine dönüştürülmüştür (Şekil 19).

Söz konusu kayıt içeriğinin Tablo 4'te belirtilen yapıda olduğu anlaşılmıştır.

Tablo 4. Tespit edilen kayıt içeriğinin gösterimi

TNXoiAJ3dct8Fjg4M9fkLFh9S2v9TXc32G	Kullanıcıya ait sıcak cüzdanın Public Key bilgisi
amount":"1"	Transfer edilen kripto para miktarı (sondaki 6 sıfır küsüratı temsil etmektedir) (miktarda küsürat olmadığı zaman önüne 6 sıfır eklenir ve gerçek değere ulaşılır 0,000001)
block":46975411	Transfer işleminin kaydının tutulduğu block numarası
block_timestamp":1671517026000	Transfer işlem zamanı
from":"TDZrKKHquHpLH2M4fpZwH2c99DAw6eoTEC"	Transfer işleminde Gönderici Adres Bilgisi
hash":"713864a5a29c63d4f7f94b63697189b21a927 194f84d3b6fc99ed6925727c5c2"	Transfer işlemine ait Hash Bilgisi
to":"TQ7dU77uGS7vBHgh27bd1N49aFTN8ZS5XJ"	Transfer işleminde Alıcı Adres Bilgisi

4. Sonuç

Bu çalışmada dünyada yaygın kullanım alanına sahip olan TronLink sıcak kripto para cüzdanı üzerinde çeşitli kripto para işlemleri gerçekleştirilmiş ve sonuçları uluslararası kriminal laboratuvarlarda da kullanılan adli bilişim yazılımları ile incelenmiştir.

Bu kripto para cüzdanının çalışma prensibinin tespiti amacıyla öncelikli olarak; Windows 10 işletim sistemine sahip bir bilgisayarın Google Chrome Web Tarayıcısına TronLink eklentisi kurulmuştur. Müteakibinde bir dizi kripto para transfer işlemi gerçekleştirilmiştir. Ayrıca Android işletim sistemine sahip cep telefonu üzerine TronLink sıcak cüzdan uygulaması kurularak bilgisayar ortamında yapılan kripto para transfer işlemleri cep telefonunda görüntülenmiştir.

İşlemlerin tamamlanması üzerine bilgisayarın yedek dosyaları üzerinde adli bilişim yazılımları ile yapılan incelemesinde;

Sıcak cüzdana ait tronlink eklentisinin tespiti amacıyla kurulum esnasında oluşturulan Public Key bilgisi X-Ways adli bilişim yazılımı ile aratılmış olup; arama sonucunda; "\Users\pc\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data" isimli klasör dizini altında bulunan "Web Data" dosyası içerisinde Public Key bilgisi ile birlikte Chrome tarayıcısına kurulan Tronlink sıcak cüzdan eklentisine ait kayıtlar tespit edilmiştir.

Ayrıca, X-Ways adli bilişim yazılımı ile yapılan işlemlere ait kayıtların tespiti amacıyla tarafımızca oluşturulan **"from":".{30,45}"to"** anahtar kelimesi aratıldığında, \Users\pc\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\data_1\trx" isimli klasör dizini altında bulunan "trx" dosyası içerisinde tüm işlemler tespit edilmiştir. Söz konusu ibare anahtar kelime olarak kullanıldığında tüm sonuçlara eksiksiz ulaşılabilmektedir.

Cep telefonunun kopyası üzerinde adli bilişim yazılımları ile yapılan incelemesinde;

"TronLink Pro 4.12.0" isimli sıcak cüzdanın "Yüklü Uygulamalar" içerisinde kayıtlı bulunduğu tespit edilmiştir. Sıcak cüzdanın kurulumu ile oluşturulan Public Key bilgisi UFED adli bilişim yazılımı içerisinde anahtar kelime olarak aratılmış olup, arama sonucunda "/data/data/com.tronlinkpro.wallet/shared_prefs/sıcak cuzdan.xml" dosyası içerisinde **"wallet_address_key"** ibaresi sonrasında tespit edilmiştir. Ayrıca "/data/data/com.tronlinkpro.wallet/cache" adresi içerisinde yapılan 5 adet işleminde kaydının bulunduğu

görülmüştür. Her işlem kaydı öncesinde **"contractsMap"** ibaresinin bulunduğu tespit edilmiştir. Söz konusu ibare anahtar kelime olarak kullanıldığında tüm sonuçlara eksiksiz ulaşılabilmektedir.

Blockchain teknolojisi adli bilişim açısından hala göreceli olarak yeni bir teknolojidir. Bu nedenle, interpol dahil olmak üzere dünya genelindeki kolluk kuvveti organizasyonları, uyuşturucu kaçakçılığı, çocuk istismarı, para aklama ve terör saldırıları gibi bir dizi yasadışı faaliyetle ilişkilendirildiği için blockchain teknolojisine odaklanmaya başlamıştır (Tziakouris, 2018).

İncelemeler sıcak cüzdan üzerinde gerçekleştirilmiştir. Bu kapsamda, diğer cüzdan türleri (kağıt cüzdan ve donanım cüzdan) üzerinde de incelemeler yapılıp adli bilişim açısından önemli bilgilerin tespit edilmesinin faydalı olacağı değerlendirilmektedir.

Kaynaklar

Bdturkey (2023) 400 Bine Yakın Yatırımcı Mağdur: Thodex Kurucusu 2 Milyar Dolarlık Kripto Parayla Yurt Dışına Kaçtı. BD Turkey, 2023. https://www.bdturkey.com/400-bine-yakin-yatirimci-magdur-thodex-kurucusu-2-milyar-dolarlik-kripto-parayla-yurt-disina-kacti?ysclid=ll0fg3eynk846822176.

Bulut Y. E, Sertkaya İ (2020) *Security Problem Definition and Security Objectives of Cryptocurrency Wallets in Common Criteria* Bilişim Teknolojileri Dergisi, Cilt:13, Sayı2, S.159.

Çarkacıoğlu A (2016) Kripto-Para Bitcoin, Sermaye Piyasası Kurulu Araştırma Raporu

Chang E, Darcy P, Choo R, Le-Khac N. (2022) Forensic Artefact Discovery and Attribution from Android Cryptocurrency Wallet Applications *arXiv preprint,* , arXiv:2205.14611.

CoinMarketCap (2023) *Kripto Paralara Dünya Genelinde Yatırılan Toplam Miktar.*. https://coinmarketcap.com. Erişim: 1 Ağustos 2023

CHIP (2023) *Garanti BBVA'dan kripto hamlesi.* *https://www.chip.com.tr/haber/garanti-bbvadan-kripto-hamlesi_158769.html*

Doran, M.D. A Forensic Look at Bitcoin Cryptocurrency; ProQuest LLC.: Ann Arbor, MI, USA, 2014.

Jokić S, et al. (2019) Comparative analysis of cryptocurrency wallets vs traditional wallets. *ekonomika* 65.3: 65-75.

Jones, L.D. Examining the Forensic Artifacts Produced by Use of Bitcoin Currency; ProQuest LLC.: Ann Arbor, MI, USA, 2014.

Karame G, Androulaki E (2016) *Bitcoin and Blockchain Security,* Boston: Artech House.

Khan A. G, Zahid A. H, Hussain M, Riaz U (2019) *Security Of Cryptocurrency Using Hardware Wallet And QR Code* University of Management and Technology, F2016114012; S:1-10,

Koblitz N (1987) Elliptic curve cryptosystems. *Mathematics of computation* 48.177 203-209.

Koerhuis W, Kechadi T, Le-Khac N. (2020) Forensic analysis of privacy-oriented cryptocurrencies *Forensic Science International: Digital Investigation* 33 200891.

Mirza M M, Ozer A, Karabiyik U (2022) *Mobile Cyber Forensic Investigations ofWeb3 Wallets on Android and Ios Appl. Sci.* ***2022****, 12, 11180. https://doi.org/10.3390/app122111180*

Martino P (2021) *Blockchain and banking: how technological innovations are shaping the banking industry,* Springer Nature.

Montanez, A. Investigation of Cryptocurrency Wallets on iOS and Android Mobile Devices for Potential Forensic Artifacts; Department Forensic Science, Marshall University: Huntington, WV, USA, 2014.

Nakamoto S, (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/.

Resmi Gazete (2021) Ödemelerde Kripto Varlıkların Kullanılmasına Dair Yönetmelik, Yayın Tarihi:16.04.2021, Sayı:31456,

Resmi Gazete (2022). Tasarruf Mevduatı Sigorta Fonu Fon Kurulu Kararı, Karar No:2022/595, Karar Tarihi:15.12.2022, Yayın Tarihi:22.12.2022, Sayı:32051,

Rezaeighaleh H, Zou C.C. (2022) New Secure Approach to Backup Cryptocurrency Wallets, *2019 IEEE Global Communications Conference (GLOBECOM)*, İstanbul Üniversitesi – Cerrahpaşa.

Rivest R. L, Shamir A, Adleman L (1978) A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM* 21.2 : 120-126.

Smart Mind (2023) *Blockchain Nedir Bitcoin Nedir* 2023. https://www.smartmind.com.tr/blockchain-nedir-bitcoin-nedir-i-955 Erişim: 1 Ağustos 2023

Suratkar S, Shirole M, Bhirud S (2020) *Cryptocurrency wallet: A review,* in 4th International Conference on Computer, Communication and Signal Processing. IEEE

Okuyucu H H (2020) Hash Fonksiyonlarının Adli Bilişimde Uygulamaları ve C++ ile Şifreleme Algoritması Tasarımı konulu Yüksek Lisans Tezi. Karabük Üniversitesi

Tyler T, et al. (2020) Memory foreshadow: memory forensics of hardware cryptocurrency wallets–a tool and visualization framework *Forensic Science International: Digital Investigation* 33 301002.

Tziakouris, G. Cryptocurrencies—A forensic challenge or opportunity for law enforcement? An interpol perspective. IEEE Secur.Priv. **2018**, 16, 92–94. [CrossRef]

Usta A, Doğantekin S (2017).*Blockchain 101* Bankalar Arası Kart Merkezi (BKM)., s.:75,

Van Der Horst L, Kwang K, Choo R, Le-Khac N. (2017) Process memory investigation of the bitcoin clients electrum and bitcoin core *IEEE Access* 5: 22385-22398.

Zollner S, Kwang K, Choo R, Le-Khac N. (2019) An automated live forensic and postmortem analysis tool for bitcoin on windows systems. *IEEE Access* 7: 158250-158263.