UMA ANÁLISE FORENSE DE CARTEIRAS ELETRÔNICAS MÓVEIS COM FOCO NA COMPROVAÇÃO DA AUTORIA DE CRIME CIBERNÉTICO

Filipe Oliveira de Marins [1], **Luciano Ignaczak** [2]

[1]Curso Superior de Tecnologia em Segurança da Informação
Universidade do Vale do Rio dos Sinos (UNISINOS)
São Leopoldo – RS – Brazil

{filipe.marins@hotmail.com[1],lignaczak@unisinos.br[2]}

Abstract. *Within the context of cybercrime, Darknet is the most wanted location for trading and conducting virtual crimes. In recent years the marketplaces of Darknet have also gone on to support cryptocurrencies payments making it even harder to track illegal activities by legal authorities. In this research is presented a forensic analysis experiment using emulated Android devices and mobile cryptocurrencies wallets in order to evaluate if it is possible to prove the payment link between two wallets through the digital evidences produced by the transactions in their respective devices. Test results showed that the three evaluated applications produced digital evidences on the emulators sufficient to establish a payment link between two wallets.*

Resumo. *Dentro do contexto de crime cibernético, a Darknet é o local mais procurado para comércio e realização de crimes virtuais. Nos últimos anos os marketplaces da Darknet passaram também a suportar pagamentos em criptomoedas dificultando ainda mais o rastreamento de atividades ilícitas pelas autoridades legais. Nesta pesquisa é apresentado um experimento de análise forense utilizando dispositivos Android emulados e carteiras móveis de criptomoedas com o objetivo de avaliar se é possível comprovar o vínculo de pagamento entre duas carteiras através das evidências digitais produzidas pelas transações em seus respectivos dispositivos. Os resultados dos testes demonstraram que os três aplicativos avaliados produziram evidências digitais nos emuladores suficientes para estabelecer um vínculo de pagamento entre duas carteiras.*

1. INTRODUÇÃO

Segundo pesquisa realizada por [McGuire 2018], o crime cibernético fatura anualmente 1.5 trilhão de dólares, o que equivale ao PIB da Rússia. Segundo o pesquisador, mais de 50% deste valor está relacionado a compras ilegais nos mercados online. Outra pesquisa realizada pela [JUNIPER RESEARCH 2015], estima que o custo global anual com o crime cibernético deve chegar em 2 trilhões de dólares em 2019. Estes números demonstram a importância do desenvolvimento de soluções para conter o avanço do crime cibernético no mundo.

Os *marketplaces* da Darknet, locais mais procurados para negociação e realização de crimes virtuais na internet, oferecem uma plataforma para vendedores e compradores

negociarem os seus produtos de forma ilícita sem que as suas identidades reais sejam descobertas. Crimes realizados a partir da Darknet têm se mostrado muito difíceis de serem rastreados pelas autoridades, sendo que nos últimos anos esta tarefa tem sido dificultada ainda mais com o surgimento das criptomoedas [Ablon et al. 2014].

Para que um indivíduo possa realizar a transação de criptomoedas com um terceiro é preciso que ele faça uso de um componente chamado de carteira eletrônica. Este componente pode ser instalado de diversas formas, em um computador, na nuvem ou em um dispositivo móvel como um *smartphone*, sendo neste último caso chamada de carteira eletrônica móvel [Antonopoulos 2017]. O uso de carteiras eletrônicas móveis vem crescendo ao longo dos anos dada a redução dos custos de aquisição de *smartphones*, a procura constante por mobilidade e também a sua praticidade de uso semelhante aos aplicativos de *mobile banking*.

Um estudo divulgado no início do ano de 2018 realizado por [Barysevich and Solad 2018] buscou avaliar a tendência das criptomoedas mais utilizadas para pagamento pelos criminosos nos próximos anos. Para chegar ao seu objetivo, o estudo analisou mais de 150 *marketplaces* e fóruns da Darknet. A pesquisa aponta que as diferentes comunidades de cibercriminosos espalhadas pelo mundo tem optado por criptomoedas distintas, tendo os russos optado pelo Litecoin com 35% da preferência enquanto que nos países de língua inglesa 15% dos usuários tem optado pelo uso da criptomoeda Monero. O estudo ainda aponta que os cibercriminosos estão usando criptomoedas como forma de pagamento por serviços ou produtos ilícitos e que está ocorrendo uma recente migração do pagamento com Bitcoin para outras criptomoedas mais modernas. Baseado nisso, esse trabalho definiu as seguintes questões de pesquisa: (i) Usando técnicas de forense digital é possível obter evidências em dispositivos *smartphones* Android que associem a carteira eletrônica móvel com uma transação de criptomoedas? (ii) Com as informações obtidas através da forense digital é possível estabelecer um vínculo de pagamento entre duas carteiras?

Para responder as perguntas foram realizados testes com transações da criptomoeda Litecoin entre três carteiras móveis de criptomoedas instaladas em emuladores Android independentes. Após a confirmação das transações foi realizada uma análise forense nos dispositivos Android que hospedam cada carteira móvel a fim de buscar por evidências produzidas pelas transações que pudessem responder as perguntas de pesquisa.

Este artigo foi organizado da seguinte forma. A seção 2 traz os resultados da análise dos trabalhos relacionados e a seção 3 aborda a metodologia de pesquisa utilizada. Na seção 4 são apresentados os resultados obtidos, enquanto que na seção 5 são realizadas as considerações finais sobre estes resultados e as expectativas para trabalhos futuros.

2. TRABALHOS RELACIONADOS

Com o intuito de incluir e relacionar apenas estudos relevantes e de boa qualidade com o tema do artigo em questão, foi utilizado um processo de seleção de artigos científicos com critérios e procedimentos padronizados permitindo que o método possa ser reproduzido por outros pesquisadores. O processo de seleção se baseou nas seguintes etapas:

1. Busca com *search queries* nas bases escolhidas: Foram escolhidas 3 bases de pesquisa sendo elas Association for Computing Machinery, Institute of Eletric and

Eletronic Engineers e Springer Link. As *search queries* escolhidas para busca de artigos em cada uma das bases de dados foram *mobile forensics*, *android forensics* e *Bitcoin wallet forensics*. Na última *search query* foi incluido o termo Bitcoin para ampliar as buscas já que o termo *wallet forensics* não trouxe resultados.

2. Contabilização dos resultados: As buscas realizadas na etapa 1 totalizaram em 4953 artigos, sendo 4596 referente a forense em dispositivos móveis no geral, 341 a forense em dispositivos móveis com Android e 16 a forense em carteiras de Bitcoin.
3. Classificação e corte por Qualis: Depois de ordenar os resultados por relevância dentro da sua respectiva base de pesquisa, foram selecionados os 3 primeiros artigos com corte por qualis em B1 ou superior. No total obteve-se 9 artigos para *mobile forensics*, 9 artigos para *android forensics* e somente 5 artigos para *Bitcoin wallet forensics*.
4. Leitura dos *Abstracts* e seleção dos artigos mais relevantes: Nesta etapa foram removidas as 4 duplicatas entre todos os 23 artigos selecionados na etapa anterior. Restaram 19 artigos, dos quais foi lido o *Abstract* de cada um e selecionados 6 artigos, cujo conteúdo se mostrou mais relevante para o tema desta pesquisa de acordo com a avaliação do autor. Os 6 artigos escolhidos são abordados abaixo.

No estudo desenvolvido por [Kim et al. 2017] é apresentado um modelo de referência forense para a investigação de dispositivos Android com o objetivo de otimizar a classificação e análise da crescente gama de aplicativos e dispositivos. Através de um sistema desenvolvido pelos pesquisadores pôde ser realizado um pré-processamento das evidências coletadas de vários *smartphones* Android, comparando estas informações com as bases de referência criadas. [Marturana et al. 2011] também destaca em seu estudo uma outra abordagem de triagem para forense em dispositivos móveis com o uso de algoritmos de classificação para determinar a probabilidade de um telefone ter sido utilizado em um crime de pedofilia. O experimento proposto se mostrou eficiente em predizer se um *smartphone*, entre um grande conjunto de dispositivos apreendidos, teve envolvimento com crime de pedofilia.

Na pesquisa de [Meiklejohn et al. 2013], os autores demonstraram ser possível desanonimizar o usuário de Bitcoin usando uma análise de Blockchain agrupando em *clusters* os endereços de carteira sob certas propriedades do protocolo da criptomoeda. Em um outro estudo realizado por [Portnoff et al. 2017] é empregada a mesma abordagem de análise focada no Blockchain para desanonimizar usuários, mas neste caso a técnica é usada para atribuir a compra de vários anúncios de tráfego sexual com Bitcoin através de um *marketplace*, a um mesmo usuário do Blockchain.

Além das propostas de modelos para investigação forense descritos até aqui, ainda existem alguns desafios com relação a preservação das evidências digitais nas cenas dos crimes investigados. Os pesquisadores [Ding and Zou 2011] propõem uma abordagem de análise por referência cruzada relacionando informações temporais de metadados e entradas de registros para detectar adulteração de evidências digitais armazenadas em sistemas de arquivos NTFS. Uma outra alternativa para preservação de evidências é apresentada por [Wang et al. 2018] onde sugere-se a implementação de uma arquitetura em cima do Blockchain do Bitcoin para preservar dados de evidências digitais.

Os artigos relatados demonstram a importância da área da forense digital no apoio

às investigações de crimes cibernéticos. Somado a isto são trazidos modelos para facilitar a análise forense de casos mais complexos com uso de técnicas de triagem e modelos de referência, e também algumas técnicas anti-forense utilizadas para ocultar ou destruir evidências. Baseado nos artigos que foram selecionados e descritos anteriormente, a pesquisa proposta no presente artigo se assemelha mais aos estudos realizados por [Meiklejohn et al. 2013] e [Portnoff et al. 2017], os quais também buscam a desanonimização dos usuários de criptomoedas só que através de análises focadas no Blockchain. Diferentemente, o nosso estudo propõe desanonimizar os usuários de criptomoedas fazendo uso apenas de técnicas de forense digital em aplicativos de carteira focada no dispositivo móvel.

3. METODOLOGIA

Com o objetivo de obter respostas para a pergunta de pesquisa apresentada na introdução deste artigo, o autor elaborou e realizou testes em ambiente virtual. Para a execução destes testes foram utilizados três aplicativos de carteira móvel para Android e uma criptomoeda específica. Cada aplicativo foi instalado em um emulador de Android independente e realizadas transações entre as carteiras instaladas nos emuladores. A partir dos artefatos produzidos pelas transações das carteiras foi feita uma análise forense em cada emulador na busca por evidências que pudessem estabelecer uma relação de pagamento entre carteiras instaladas em emuladores distintos. A condução do processo é detalhada nesta seção.

3.1. Processo de seleção dos aplicativos de carteira móvel

Para possibilitar a escolha das carteiras móveis de criptomoedas que seriam avaliadas, em um primeiro momento foi necessário definir a criptomoeda utilizada nas transações. Com base na pesquisa realizada por [Barysevich and Solad 2018], a criptomoeda mais utilizada para pagamento pelos cibercriminosos é a Litecoin (LTC), portanto, para a realização dos testes foi escolhida esta criptomoeda.

Definida a criptomoeda, o próximo passo foi escolher os três aplicativos de carteiras móveis suportados em plataforma Android para a execução dos testes. Para a escolha dos aplicativos foi utilizado como critério a seleção das carteiras móveis melhor avaliadas pelos usuários do *website* CryptoCompare[1] que não fazem uso da API do Google Play. A escolha por aplicativos que operem sem a necessidade da API do Google Play foi uma decisão do autor para otimizar a etapa de análise forense em disco, tendo em vista que as imagens de emuladores Android sem suporte à API do Google Play disponibilizadas pelo Android Virtual Device possuem uma quantidade muito menor de arquivos para a análise. A escolha de imagens Android e aplicativos que não fazem uso da API do Google Play para a realização dos testes não impacta nos resultados da pesquisa.

No *website* CryptoCompare[1] foram definidas três condições nos filtros da sessão de carteiras. O primeiro filtro foi configurado para exibir apenas carteiras suportadas pela plataforma Android totalizando em 117 instâncias. Posteriormente, foi configurado um segundo filtro para exibir quais destas 117 carteiras Android davam suporte ao uso da criptomoeda Litecoin totalizando em 51 carteiras. Por fim, dentre as 51 carteiras foi configurado para exibir um *ranking* de acordo com as notas de avaliações dos usuários

[1] https://www.cryptocompare.com/wallet

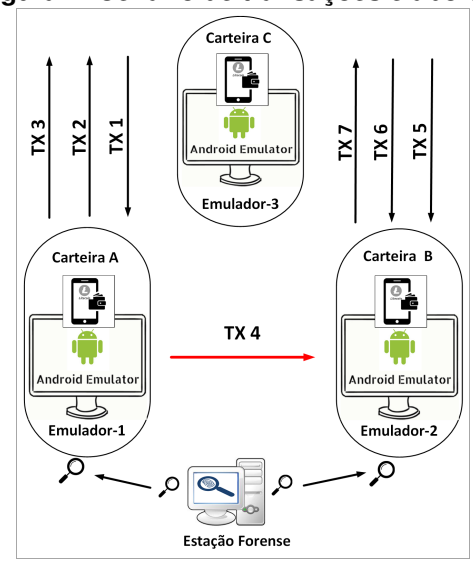
da comunidade do *website*. Desta forma os aplicativos de carteira selecionados foram Coinomi, Paytomat e Freewallet.

3.2. Organização do cenário de testes

Para que fossem realizados os testes de transações entre os aplicativos escolhidos elaborou-se um cenário com a implementação de emuladores Android. Neste cenário foram implementados três emuladores Android, os quais foram denominados emulador-1, emulador-2 e emulador-3. No emulador-1 e emulador-2 foram instalados os aplicativos de carteira escolhidos para os testes, a fim de simular dois usuários realizando transações financeiras entre as carteiras de criptomoedas. Já o emulador-3 foi criado apenas para gerar transações adicionais aos usuários das carteiras instaladas no emulador-1 e emulador-2, buscando criar um ambiente de testes mais próximo do cenário real. Caso contrário, o ambiente de testes teria apenas uma única transação realizada entre as carteiras instaladas no emulador-1 e emulador-2, diferente do que ocorre no mundo real onde um usuário que realiza negócios envolvendo pagamento com criptomoedas provavelmente terá registrado em seu *smartphone* milhares de transações tanto de débito quanto de crédito.

Durante a realização dos testes no cenário elaborado foram efetuadas sete transações, identificadas por TX, entre as carteiras dos três emuladores implementados conforme pode ser observado com mais detalhes na Figura 1. Nela foi destacada na cor vermelha a transação TX 4 realizada pela carteira A para um endereço de pagamento na Carteira B, cuja análise forense realizada no emulador-1 e emulador-2 teve como objetivo a obtenção de evidências que pudessem comprovar o vínculo de pagamento entre as duas carteiras e consequentemente responder a pergunta de pesquisa.

Figura 1. Cenário de transações elaborado



Optou-se por realizar três testes no cenário apresentado na Figura 1 para que pudessem ser feitas as transações da Carteira A para Carteira B com cada par de aplicativo de carteira escolhido e então comparar os resultados obtidos. Dito isso, os três testes foram realizados conforme apresentado na Tabela 1.

Tabela 1. Transação entre os aplicativos de carteira selecionados para o teste

Teste	Carteira A	Carteira B
1	Coinomi	Freewallet
2	Coinomi	Paytomat
3	Paytomat	Freewallet

3.3. Implementação do cenário de testes

Para a implementação dos três emuladores Android foi escolhida a arquitetura x86 pelo fato da emulação ARM apresentar um desempenho muito limitado em plataformas de virtualização com arquitetura Intel x86. Segundo informações da página do Android[3], os APKs geralmente são compilados em multiarquitetura fazendo com que o binário gerado seja homologado para realizar instruções tanto x86 como ARM, portanto os processos desta pesquisa podem ser replicados em *smartphones* reais.

Optou-se pela utilização do Android versão 7.0, popularmente chamado de Nougat, pelo fato de ser a versão do Android mais recente que permitiu a inicialização do emulador com *kernel* customizado, cuja compilação foi feita para permitir o uso da ferramenta de aquisição de memória para este *kernel*.

A estação forense utilizada para a instalação do kit Android Studio 3.3.1[4], implementação dos emuladores Android e realização de todos os procedimentos de aquisição e análise forense possuia as seguintes especificações: Sistema operacional Windows 10, processador Intel Core i5-4460 com clock de 3.2GHz, 8GB de memória RAM e 1TB de disco.

3.4. Processo de aquisição de dados

O processo de aquisição de dados dos emuladores foi feito para dados não voláteis armazenados em disco e para dados voláteis armazenados em memória. Todas as etapas realizadas em cada um destes processos é descrita nesta seção.

1. Aquisição de Disco: Para aquisição lógica dos dados armazenados em disco nos emuladores foi utilizado o utilitário dd, nativo na imagem de emuladores Android. A partir da própria estação forense foi primeiramente estabelecido um *shell* com cada emulador utilizando o Android Debug Bridge (ADB). Neste *shell* Linux foi feita a coleta da imagem de disco executando o dd e redirecionando a sua saída para a estação forense através de uma conexão de rede fazendo uso combinado com o utilitário Netcat. Em cada um dos três testes a aquisição de imagens do disco se deu nos seguintes momentos em cada emulador:
   (a) Após a instalação e inicialização do emulador;
   (b) Após a instalação do aplicativo de carteira no emulador;
   (c) Após a inicialização do endereço de carteira Litecoin;
   (d) Após a confirmação de todas as transações na carteira do emulador.
2. Aquisição de Memória: Para aquisição de memória optou-se pela utilização do utilitário Lime [5]. A escolha foi baseada no fato de que os módulos carregáveis no

[3]https://developer.android.com/ndk/guides/abis.html?hl=pt-brgc
[4]https://developer.android.com/studio
[5]https://github.com/504ensicsLabs/LiME

Kernel como o Lime tem maiores privilégios para acesso ao hardware. O seu uso é recomendado visto que a partir da versão 2.6 do *kernel* do Linux os utilitários como dd passaram a ter restrições de acesso à memória. [van de Ven 2018]. Para uso da ferramenta Lime nos emuladores implementados foi necessário compilar o binário da mesma para o Android 7.0. Com a ferramenta compilada, a aquisição de memória dos emuladores Android ocorreu de forma semelhante a aquisição de discos. O módulo Lime foi primeiramente copiado para dentro do Android utilizando novamente o ADB e depois carregado no *kernel* do emulador para que fosse então extraído um *dump* da memória. A saída foi redirecionada para a estação forense que estava aguardando a conexão com o Netcat. A aquisição de memória foi realizada em um único instante, ou seja, após a realização e confirmação de todas as transações envolvendo a carteira instalada no emulador analisado.

3.5. Processo de análise de dados

Para a análise dos dados coletados foram utilizadas várias ferramentas entre elas: FTK Imager 4.2.1[6], Diff [7], Autopsy 4.11 [8], Strings e Grep. Os emuladores Android foram analisados do ponto de vista forense para cada um dos três testes de transações seguindo as etapas abaixo:

1. Análise de disco
   (a) Uso da ferramenta FTK Imager para extração da lista de *hashes* das 4 imagens da partição "/data" obtidas na etapa de aquisição de disco;
   (b) Uso da ferramenta Diff para comparação das listas de *hashes* extraídas anteriormente e identificação dos arquivos que foram alterados entre cada imagem;
   (c) Uso da ferramenta Autopsy para análise lógica somente dos arquivos que foram alterados em cada imagem da partição "/data" segundo informações da ferramenta Diff;
2. Análise de memória
   (a) Uso do utilitário Volatility para geração de um novo *dump* de somente com os dados gravados pelo aplicativo de carteira analisado.
   (b) Uso do utilitário Strings e Grep do Linux para aquisição de evidências buscando por palavras chaves dentro do *dump* de memória gerado pelo Volatility.

4. RESULTADOS

Nessa seção serão apresentados os resultados subdivididos de acordo com cada um dos três testes realizados. Com base nos resultados obtidos em cada teste é determinado se o objetivo da pesquisa foi atingido.

4.1. Teste 1: Coinomi x Freewallet

Ao analisar os arquivos de imagem da partição "/data" dos emuladores 1 e 2 com o Autopsy não foram encontradas em disco evidências relacionadas à transações de criptomoedas. Em contrapartida, a análise dos *dumps* de memória apresentou um resultado rápido

[6]https://accessdata.com/product-download/ftk-imager-version-4.2.1
[7]https://www.diffchecker.com/
[8]https://github.com/sleuthkit/autopsy/releases/download/autopsy-4.11.0

e relevante buscando pelas *strings* “hash” e “ltc” apenas para o *dump* de memória do emulador-2 onde estava instalada a carteira Freewallet. Neste *dump* foram encontrados várias *strings* JSON serializados com informações das transações realizadas pelo aplicativo, portanto apresentando dados estruturados e sequênciais na memória. Na Tabela 2 são apresentadas as três transações de pagamento filtradas das *strings* JSON para o único endereço da carteira Freewallet.

Tabela 2. Transações da Freewallet no *dump* do emulador-2

Hash	Amount	Type	Recipient Address
041f389c2a21ab0f6a037310b1a651237524ae0360bb04b92fadde408bf48ed1	0.0006	payin	LV13mjVwKViiX4FMm36Y3UUNNJHWSrMS6
41592097be1a82215c64385931fccaeedc5d35ce1409968ca994f77ec93fb47b	0.0006	payin	LV13mjVwKViiX4FMm36Y3UUNNJHWSrMS6
9d84141bf613c66f00d2c66d4d1d4706da3bfe706e26f010673f408a1498860d	0.0006	payin	LV13mjVwKViiX4FMm36Y3UUNNJHWSrMS6

O desafio da análise forense estava agora em encontrar quais destas transações correspondia a TX 4 originada pela carteira A, a Coinomi, instalada no emulador-1. Ao realizar a procura das *strings* “hash” e “ltc” no *dump* de memória do emulador-1 não foram encontradas quaisquer informações relacionadas à transações de criptomedas. No entanto, realizando a pesquisa por cada um dos três endereços de *hash* das transações coletadas no *dump* de memória do emulador-2, obteve-se evidências somente do endereço de *hash*:“9d84141bf613c66f00d2c66d4d1d4706da3bfe706e26f010673 f408a1498860d”. Esta evidência provou que a transação identificada por este *hash* foi utilizada para realizar um pagamento para a carteira Freewallet a partir da Carteira Coinomi conforme aponta Figura 2.

Figura 2. Informações da TX 4 na memória do emulador-1

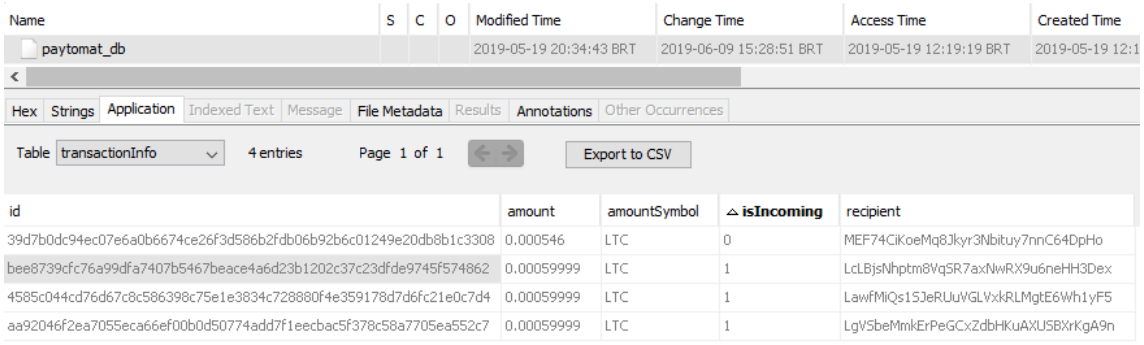
```
1537776  [0]createDataConnection() X id=0 dc={DC-1: State=DcInactiveState mApnSetting=null RefCount=0 mCid=-1
         mCreateTime=-1 mLastastFailTime=-1 mLastFailCause=NONE mTag=1 mLinkProperties={LinkAddresses: []  Routes: []
         DnsAddresses: [] Domains: null MTU: 0} linkCapabilities=[ Transports: CELLULAR Capabilities:
         NOT_RESTRICTED&TRUSTED&NOT_VPN LinkUpBandwidth>=51200Kbps LinkDnBandwidth>=102400Kbps Specifier: <1>]
         mApnContexts={}}
1537777  TransactionCreator
1537778   completed:  9d84141bf613c66f00d2c66d4d1d4706da3bfe706e26f010673f408a1498860d
1537779    in  <no scriptSig> 0.00079712 BTC
1537780       outpoint:8a961a15893ef67d9cd9fc756b2d9d638aed3131964b59b423b1b6cc91bf9f30:1
1537781    out  DUP HASH160 PUSHDATA(20)[6b4072f158d06dbb9109f516331bf10dcfaefd05] EQUALVERIFY CHECKSIG 0.0006 BTC
1537782    fee  0.00231905 BTC/kB, 0.00019712 BTC for 85 bytes
1537783    prps USER_PAYMENT
```

4.2. Teste 2: Coinomi x Paytomat

Ao analisar os arquivos do *dump* da partição “/data” do emulador-1 com o Autopsy novamente não foram encontradas em disco evidências de transações de criptomoedas. No entanto na pasta privada do aplicativo Paytomat em “/data/com.paytomat”, instalado no emulador-2, foi encontrada uma base de dados SQLIte com uma tabela chamada *transactioninfo* apresentando informações relevantes conforme destaque na Figura 3.

De posse dos *hashes* de transações obtidos na base de dados da carteira Paytomat foi realizada a pesquisa no *dump* de memória do emulador-1. Ao realizar a busca pelo *hash*: “bee8739cfc76a99dfa7407b5467beace4a6d23b1202c37c23dfde9745f574862” obteve-se a comprovação de que a carteira Coinomi realizou o pagamento à carteira Paytomat através desta transação.

Figura 3. Informações de transações na base de dados do aplicativo Paytomat



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
paytomat_db				2019-05-19 20:34:43 BRT	2019-06-09 15:28:51 BRT	2019-05-19 12:19:19 BRT	2019-05-19 12:1

Hex | Strings | Application | Indexed Text | Message | File Metadata | Results | Annotations | Other Occurrences

Table: transactionInfo — 4 entries — Page 1 of 1 — Export to CSV

id	amount	amountSymbol	isIncoming	recipient
39d7b0dc94ec07e6a0b6674ce26f3d586b2fdb06b92b6c01249e20db8b1c3308	0.000546	LTC	0	MEF74CiKoeMq8Jkyr3Nbituy7nnC64DpHo
bee8739cfc76a99dfa7407b5467beace4a6d23b1202c37c23dfde9745f574862	0.00059999	LTC	1	LcLBjsNhptm8VqSR7axNwRX9u6neHH3Dex
4585c044cd76d67c8c586398c75e1e3834c728880f4e359178d7d6fc21e0c7d4	0.00059999	LTC	1	LawfMiQs15JeRUuVGLVxkRLMgtE6Wh1yF5
aa92046f2ea7055eca66ef00b0d50774add7f1eecbac5f378c58a7705ea552c7	0.00059999	LTC	1	LgVSbeMmkErPeGCxZdbHKuAXUSBXrKgA9n

4.3. Teste 3: Paytomat x Freewallet

Observou-se novamente o formato JSON produzido pela carteira Freewallet na memória do emulador-2, portanto confirmando que este é um comportamento padrão da implementação deste aplicativo. Já a análise forense em disco no emulador-1 nos trouxe novamente, assim como no teste 1, uma base de dados SQLite na pasta da aplicação Paytomat contendo todas as informações de transações realizadas pelo aplicativo de carteira. Foi relativamente fácil a partir do *hash* da transação ou do endereço de pagamento da carteira Freewallet do emulador-2, comprovar a relação de pagamento entre as duas carteiras. Foi encontrada na base de dados do aplicativo Paytomat, a transação com *hash*: "104354e3fee0ae6d08711482c7c110f4ec686090c3246aa270266ae2b8e37 2af" com destino para o endereço "LdmrpR3YNhMPGq8rjbi bW8bJaVmgHsDHja" correspondente ao endereço utilizado pela carteira Freewallet.

4.4. Limitações dos testes

O escopo dos testes realizados foi limitado a carteiras móveis de criptomoedas para a plataforma de emulação Android. Não foi considerado nos objetivos da pesquisa realizar testes e comparações com carteiras móveis em outras plataformas de dispositivos móveis, bem como a comparação com outras criptomoedas. Também não foi contemplado nesta pesquisa a realização de testes em dispositivos reais visto que o objetivo foi inicialmente compreender o comportamento dos aplicativos de carteira móveis para Android com relação a produção de evidências de transações em emuladores onde se torna mais prático a replicação de testes, e a partir destes resultados concluir se é viável a realização de futuros testes com dispositivos reais para confirmar a aplicação prática do método.

5. CONSIDERAÇÕES FINAIS

Com base nos resultados obtidos pôde-se provar que é possível através de análise forense em dispositivos Android obter evidências de transações de carteiras móveis de criptomoedas e a partir destas informações estabelecer uma relação de pagamento entre duas carteira. É importante destacar que não há necessidade de ter conhecimento dos endereços das carteiras para realizar a investigação, visto que a relação de pagamento pôde ser comprovada através da obtenção do registro de *hash* referente a mesma transação em ambos dispositivos Android. Podemos afirmar também, com base nos resultados, que os aplicativos de carteira móvel produzem evidências das suas transações em memória e disco,

dependendo da implementação. Durante os testes foi observado que dois dos três aplicativos testados não apresentaram evidências das transações em disco, uma forte indicação que foi utilizada uma estrutura em nuvem e por isso não foram encontradas bases de dados nas pastas dos aplicativos. No geral, os resultados sugerem que os procedimentos de análise forense podem ser utilizados para auxiliar nas investigações relacionadas a crimes que envolvam pagamentos com criptomoedas.

Para trabalhos futuros se deseja avaliar a busca por evidências através da elaboração e testes com expressões regulares, visando criar um procedimento padrão de análise forense para os diversos aplicativos de carteiras móveis e criptomoedas existentes. É também do interesse do autor reproduzir os testes em dispositivos smartphones reais para verificar a viabilidade da aplicação do método descrito nesta pesquisa em ambientes reais.

Referências

Ablon, L., Libicki, M. C., and Golay, A. A. (2014). Markets for cybercrime tools and stolen data. Rand National Security Research Division.

Antonopoulos, A. M. (2017). *Mastering Bitcoin 2th edition*. OReilly Media Inc, Gravenstein Highway North, Sebastool, CA 95472.

Barysevich, A. and Solad, A. (2018). Litecoin emerges as the next dominant dark web currency. Recorded Future.

Ding, X. and Zou, H. (2011). Time based data forensic and cross-reference analysis. *Symposium on Applied Computing*, pages 185–190.

JUNIPER RESEARCH (2015). Cybercrime will cost businesses over $2 trillion by 2019. Technical report, Juniper Research.

Kim, D., Lee, Y., and Lee, S. (2017). Mobile forensic reference set (mfres) and mobile forensic investigation for android devices. *The Journal of Supercomputing*, pages 1–15.

Marturana, F. et al. (2011). A quantitative approach to triaging in mobile forensics. *International Conference on Trust, Security and Privacy in Computing and Communications*, pages 582–588.

McGuire, M. (2018). Into the web of profit. Technical report, Bromium.

Meiklejohn, S. et al. (2013). A fistful of bitcoins: Characterizing payments among men with no names. *Internet measurement conference*, pages 127–140.

Portnoff, R. S. et al. (2017). Backpage and bitcoin: Uncovering human traffickers. *ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 1595–1604.

van de Ven, A. (2018). x86: introduce /dev/mem restrictions with a config option.

Wang, M. et al. (2018). Lightweight and manageable digital evidence preservation system on bitcoin. *Journal of Computer Science and Technology*, 33:568–586.