ПРИРУЧНИК

О НАЧИНИМА УПРАВЉАЊА ЕЛЕКТРОНСКИМ УРЕЂАЈИМА, ЕЛЕКТРОНСКИМ ДОКАЗИМА И НОСАЧИМА ЕЛЕКТРОНСКИХ ДОКАЗА

Београд, 2024

#ЕУ ЗА ТЕБЕ

oebs Organizacija za evropsku bezbednost i saradnju
Misija u Srbiji

ПРИРУЧНИК

О НАЧИНИМА УПРАВЉАЊА ЕЛЕКТРОНСКИМ УРЕЂАЈИМА, ЕЛЕКТРОНСКИМ ДОКАЗИМА И НОСАЧИМА ЕЛЕКТРОНСКИХ ДОКАЗА

Београд, 2024

Приручник о начинима управљања електронским уређајима, електронским доказима и носачима електронских доказа

Приредило:
Министарство унутрашњих послова

Аутори:

Владимир Вујић, Служба за борбу против високотехнолошког криминала, Министарство унутрашњих послова

Мирјана Ђорђевић, Служба за борбу против високотехнолошког криминала, Министарство унутрашњих послова

Предраг Корач, Национални центар за криминалистичку форензику, Министарство унутрашњих послова

Милан Пејчић, Одељење за борбу против корупције, Министарство унутрашњих послова

Милош Цалић, Одељење за борбу против корупције, Министарство унутрашњих послова

Миливоје Лазић, Одељење за борбу против корупције, Министарство унутрашњих послова

Издавачи:
Мисија ОЕБС-а у Србији и пројекат „Подршка јачању владавине права у Републици Србији“, који заједнички финансирају ЕУ и Немачко савезно министарство за економску сарадњу и развој, а спроводи ГИЗ (Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ).

Лектура и коректура:
Јасмина Алибеговић

Дизајн и прелом:
Диа-Арт

Штампа:
Диа-Арт

Тираж: 500 примерака

Београд 2024. године

Штампање ове публикације подржали су Мисија ОЕБС-а у Србији и пројекат „Подршка јачању владавине права у Републици Србији“, који заједнички финансирају ЕУ и Немачко савезно министарство за економску сарадњу и развој, а спроводи ГИЗ (Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ)).

САДРЖАЈ

Увод

Приручник је направљен у сарадњи Министарства унутрашњих послова (у даљем тексту: МУП) Републике Србије, Мисије ОЕБС-а у Србији и пројекта „Подршка јачању владавине права у Републици Србији", који заједнички финансирају ЕУ и Немачко савезно министарство за економску сарадњу и развој, а спроводи ГИЗ, и намењен је за потребе Одељења за борбу против корупције МУП-а Републике Србије, другим организационим јединицама МУП-а које у току рада прикупљају електронске доказе, као и тужиоцима и судијама као помоћ у решавању процесних и техничких питања везаних за употребу савремених технологија.

У изради приручника коришћене су и смернице за поступање са електронским доказима које су дефинисали Интерпол[1] и Савет Европе[2] у својим приручницима, а коришћена је и најбоља пракса и искуство у случајевима Службе за борбу против високотехнолошког криминала и Националног центра за криминалистичку форензику МУП-а Републике Србије. У одређеним случајевима поступајући службеник би требало да користи и интернет (ради вршења одређених провера) и сходно томе у Приручнику су остављени линкови који помажу да се квалитетно провере подаци битни у поступању са неким електронским доказима.

1 Guidelines_to_Digital_Forensics_First_Responders_V7.pdf.

2 https://shorturl.at/W8GzO.

Скраћенице (акроними), појмовник и графички симболи

АНДРОИД	оперативни систем
ВТК	високотехнолошки криминал
ГПС	глобални навигациони сателитски систем
ЕСИМ	виртуелна мобилна картица (енг. Electronic Subscriber Identity Module)
ЗКП	Законик о кривичном поступку
ИМЕИ	јединствени нумерички идентификатор за сваки електронски уређај који га поседује
ИОС	мобилни оперативни систем америчке фирме Епл (енг. IOS, Apple)[3]
КУ	кривични уписник
МУП	Министарство унутрашњих послова
НФЦ	комуникација кратког поља (енг. Near Field Communication)[4]
СИМ	мобилна картица (енг. Subscriber Identity Module)
СД картица	меморијска картица
УСБ меморија	преносива меморија за складиштење дигиталних података

Под *авио модом* или *режимом летења* паметног телефона или таблета, подразумева се подешавање уређаја којим се блокирају сви бежични адаптери да емитују сигнал ради спречавања прављења конекције са другим уређајима који су компатибилни за повезивање и размену података.

Блутут је технологија помоћу које се врши бежични пренос података између уређаја који поседују исту технологију.

Вај-фај (енг. Wi-Fi) је бежична локална рачунарска мрежа. Сви уређаји који су повезани на ову мрежу су у близини (пар десетина метара) антене (уређаја) која прима и предаје потребне сигнале.

Виртуелна приватна мрежа (енг. virtual private network - VPN) је приватна комуникациона мрежа која се користи за комуникацију у оквиру јавне мреже. Транспорт ВПН пакета података одвија се преко јавне мреже (нпр. интернет) коришћењем стандардних комуникационих протокола. ВПН омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију као и да мењају геолокацију одакле њихови подаци излазе на некриптован интернет.

3 ИОС је име за мобилни оперативни систем који је развила америчка фирма Епл за ајфон, али данас се овај оперативни систем користи и за друге производе као: ајпед, Епл ТВ и ајпод тач.

4 НФЦ је скраћеница од Near Field Communication (енг. комуникација кратког поља) и представља скуп стандарда за паметне телефоне и остале мобилне уређаје којима се успоставља радио веза између њих, обично кратким прислањањем једног уређаја на други. Углавном се користи раздаљина од свега пар центиметара.

Под *атрибутом* електронског доказа се подразумевају информације које системи чувају о фајлу, а обично су подржани следећи: име, локација, величина, време креирања, последње модификације и последњег приступа, идентификатор власника фајла и права приступа.

Електронски подаци представљају електронске записе података погодне за електронску обраду и пренос путем средстава електронске комуникације.[5]

Електронски уређај представља уређај који може да креира, трајно или привремено чува и/или шаље и прима електронске податке.

Под *енкрипцијом* се подразумева процес у криптографији којим се врши измена података тако да се подаци, или поруке, учине нечитљивим за особе које не поседују одређено знање (кључ).

ИМЕИ је скраћеница од енглеске сложенице International MOBile Equipment Identity и представља јединствени број (15 знаковни број или 16 знаковни број) који је додељен сваком мобилном или сателитском телефону.

ИП камера је мрежна ЛАН камера.

Криптовалута је облик дигиталне имовине која се користи као средство размене вредности користећи криптографију као начин обезбеђивања сигурности трансакција, контроле стварања додатних новчаних јединица и ради потврде трансфера валуте.

QR код је матрични код или дводимензионални бар-код.

Лајтинг адаптер се користи за повезивање производа фирме Епл, пре свега ајфона, ајпед и ајпод тач са рачунарима, екстерним мониторима, камерама, екстерним пуњачима и другим периферним уређајима.

НОД представља суштински новчаник за биткоин који има само део блокчејна и да би ажурирао податке за трансакцију мора да се повеже путем интернет мреже на Фул НОД.

Фул НОД је софтвер за рачунар (Биткоин кор) који локално (на локалној меморији) похрањује целокупан блокчејн (све трансакције) и сходно томе учествује у верификацији трансакција на биткоин мрежи.

ОБД конектор постављен је у сваки аутомобил новије генерације, како би сервисери имали приступ софтверском делу компјутера аутомобила.

Облак (енгл. cloud) представља испоруку рачунарских ресурса и складишних капацитета као услугу за хетерогену групу крајњих корисника. Крајњи корисници приступају апликацијама у облаку преко веб прегледача или десктоп апликације на мобилном телефону, док се софтвер и кориснички подаци налазе на серверима на удаљеној локацији.

RAM - (енг. random-access memory — „меморија са случајним приступом”), означава врсту меморије која је директно адресибилна и њеном садржају се може приступити по произвољној локацији, а не само редом (секвенцијално, као код трака). Код других медијума, попут тврдих дискова, CD-a, DVD-a и магнетних трака, као и примитивних типова меморија

5 Члан 2 Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању, https://shorturl.at/JbhrX https://www.paragraf.rs/propisi/zakon-o-elektronskom-dokumentu-elektronskoj-identifikaciji-i-uslugama-od-poverenja-u-elektronskom-poslovanju.html.

попут добош меморије, подаци се записују у предодређеном реду, узастопно, због ограничења механичког дизајна.

СИД фраза је скуп одређених, тачно дефинисаних, речи (12-24) енглеског алфабета који служи за генерисање и бекап приватних кључева код софтверских и хардверских новчаника криптовалута.

ССД диск нема покретне механичке компоненте. То их разликује од традиционалних електромеханичких дискова као што су тврди дискови (HDD) или флопи дискови, који садрже диск који се окреће и покретну читајућу/уписну главу. У поређењу са електромеханичким дисковима, ССД дискови су обично отпорнији на физички удар, тише раде, имају мање време приступа и мање кашњење.

Trusted Platform Module (TPM) је међународни стандард за сигурни крипто процесор, наменски микроконтролер дизајниран за заштиту хардвера уз помоћ интегрисаних криптографских кључева. Појам се такође може односити на чип који је у складу са стандардом.

Фарадејева врећа - антистатичка торба која формира ефекат „индукционог штита" за све производе осетљиве на електростатику.

Форматирање диска је процес припреме уређаја за складиштење података као што су хард диск, ССД, флопи за прву употребу.

Под *хеширањем* се подразумева мапирање података произвољне величине у вредност фиксне величине тако да одређена улазна вредност мора увек да генерише исту излазну (хеш) вредност.

WLAN је бежична локална рачунарска мрежа коју чине два или више уређаја, бежично повезаних у локалну мрежу (LAN), унутар ограниченог простора. Најчешће, корисници се могу слободно кретати унутар тог простора, без прекида везе.

У приручнику ће се користити графички симболи који визуелно дају смернице о каквом садржају текста се конкретно ради:

	Означава део који садржи основне информације
	Означава део који указује на напредни садржај
	Означава део који указује на специјализована знања
	Означава информативни део поглавља
	Означава део који садржи важне информације
	Означава део који садржи техничке информације

ДИГИТАЛНА ФОРЕНЗИКА И ПРАВНИ ОСНОВ ЗА ПОСТУПАЊЕ СА ЕЛЕКТРОНСКИМ ДОКАЗИМА

1. Дигитална форензика и правни основ за поступање са електронским доказима

Дигитална форензика је поступак очувања, идентификације, издвајања и документовања електронских доказа који се могу користити на суду. То је наука проналажења доказа из дигиталних медија попут рачунара, мобилног телефона, сервера, серверских мрежа или других носилаца меморијског садржаја. Дигитална форензика обухвата низ метода, алата и поступака који омогућавају решавање великог броја кривичних дела.

Основни задатак дигиталне форензике јесте опоравак, анализа и очување електронских доказа на такав начин да ти исти докази буду употребљиви на суду, затим проналажење начина прикупљања доказа на месту догађаја на начин који ће очувати интегритет доказа. Аквизиција (изузимање) података, валидација (потврђивање) и репликација (копирање) доказа су основ сваког поступања у области дигиталне форензике. Такође, изузетно битна је и израда форензичког записника (вештачења) који на адекватан начин пружа увид у прикупљене доказе, као и на сам процес анализе.

След активности у области дигиталне форензике је следећи: идентификација, чување, анализа, документовање и представљање доказа.

Привремено одузимање електронских уређаја је у већини случајева резултат претресања стана и других просторија у складу са Закоником о кривичном поступку. Основ за привремено одузимање електронских уређаја дефинисан је у Законику о кривичном поступку. Осим Законика о кривичном поступку, Министарство унутрашњих послова усвојило је Стандардну оперативну процедуру за поступање са електронским доказима која детаљније дефинише начин паковања, складиштења и транспорта електронских уређаја које је такође обавезујуће.[6]

Пре самог чина привременог одузимања орган поступка, у складу са законом, има право да оствари увид у предмет који ће се привремено одузети. Мада, често користан, овакав увид може да произведе низ нежељених ефеката, посебно ако се узме у обзир реална неопходност самог увида, имајући у виду да основи сумње за извршење кривичног дела најчешће већ постоје. Наиме, с обзиром да увид, по правилу, подразумева преглед садржаја електронског уређаја на начин који је идентичан свакодневном коришћењу уређаја, постоји објективни ризик од измене података који ће касније пружити погрешну слику. На пример, увидом у садржај, рецимо, мобилног телефона и прегледом СМС порука, особа која остварује увид може да отвори и прочита поруку која је до тада била непрочитана. Касније анализа показаће да је конкретна порука прочитана, што орган поступка доводи у заблуду. Намеће се закључак да, уколико је остваривање увида у садржај електронског уређаја неопходно, та радња мора бити адекватно и детаљно документована како би докази који се касније пронађу као резултат анализа задржали форензичку исправност.

Увид у сам уређај се може остварити у случајевима када је уређај који је предмет одузимања већ покренут из разлога адекватног документовања активног садржаја који је од значаја за поступак доказивања извршења кривичног дела, као и у случајевима већ откључаних/покренутих система за енкрипцију на рачунарима, као што је нпр. bitlocker у циљу прикупљања података тј. кључева из RAM меморије на форензички исправан начин (memorydump), без којих би евентуална касније анализа садржаја била онемогућена.

6 Збирка прописа из надлежности криминалистичке полиције, МУП РС, 2022.

У пракси Службе за сузбијање високотехнолошког криминала, када се врши увид у упаљени рачунар или мобилни телефон, полицијски службеници поступају у складу са чланом 135 ЗКП који дефинише Увиђај ствари. Суштински, ту се не ради о претресању уређаја за аутоматску обраду података него о увиђају на ствари извршеном у смислу ове одредбе ЗКП, а снимљене фотографије представљају део форензичке документације која је доказни материјал у списима предмета. Сходно томе, надлежни јавни тужилац, који руководи преткривичним поступком и који је поверио полицији процесну радњу претресања, може затражити помоћ стручног лица ради увида у садржај упаљеног уређаја сходно одредбама чланова 133 и 135 ЗКП. На основу тога, стручно лице остварује увид у упаљени уређај и о садржини истог сачињава извешај.

2. Основна начела и поступци приликом првог реаговања на електронске доказе

Сви кривични поступци зависе од доказа за одлучивање о кривици или невиности оптуженог у поступку. Традиционално и историјски, докази су били у физичком облику (као што су документи, фотографије, итд.) или усмено сведочење лица.

Електронски докази су изведени из електронских уређаја као што су рачунари и њихови периферни уређаји, апарати, рачунарске мреже, мобилни телефони, дигитални фото-апарати и друга преносива опрема (укључујући уређаје за складиштење података), као и са интернета.

Сам назив електронског доказа подразумева информацију коју систем чува у фајлу а обично садржи податке као што су име, локација, величина, време креирања, последње модификације и последњег приступа.

1. Карактеристике електронских доказа:
2. Аутентичност – да одговара оригиналном извору;
3. Потпуност - да је у складу са свим другим чињеницама, без обзира да ли иду или не у корист осумњиченом;
4. Поузданост - да не постоји ништа што би довело у сумњу аутентичност или истинитост;
5. Кредибилитет – морају бити убедљиви да их суд у поступку прихвати као истину;
6. Пропорционалност – да методе које се користе при обезбеђивању електронских доказа морају да буду у сразмери са интересима правде.

Нпр. Уколико је полицијски службеник приликом претресања стана и других просторија, супротно правилима, упалио рачунар и на њему пронашао електронски доказ који потврђује кривично-правну радњу осумњиченог, без обзира што није мењао атрибуте фајла (датум, време, тип фајла) нити садржину фајла, овако прибављен електронски доказ има карактеристике аутентичности, потпуности, кредибилитета и пропорционалности, али не и поузданости због начина којим се до њега дошло (видети дијаграм поступања приликом претресања – слика 2).

2.1. Припремне радње које претходе претресању

Пре предузимања процесних радњи које могу да доведу и до првог реаговања на електронске доказе, потребно је извршити одређене радње како би се олакшало поступање полицијских службеника на самом лицу места. Нпр. ако очекујемо да ћемо приликом предузимања процесне радње претресање стана пронаћи криптовалуте које треба одузети, потребно је да претходно припремимо новчаник за одузимање криптовалута. Такође, ако знамо да осумњичени има посебна знања везана за информационе технологије и да можемо очекивати да користи енкрипцију уређаја онда морамо предвидети и стручњака дигиталне форензике приликом претресања.

Припремне радње би требало да обухвате:

1. Прикупљање података из отворених извора на интернету о осумњиченом (друштвене мреже, форуми и сл.);
2. Планирање датума и времена претресања како би рачунар или други уређаји били упаљени, односно, у најбољем случају, осумњичени затечен како ради на њима;
3. Планирање полицијских службеника који ће учествовати (уколико су потребна специјализована знања о нпр. дигиталној форензици, криптовалутама и сл.);
4. Прецизирање опреме која је потребна за претресање.

Сходно Упутству о стандардним оперативним процедурама поступања са електронским уређајима и подацима МУП-а Републике Србије, предвиђена је обавезна и пожељна опрема:

Обавезна опрема:

1. Рукавице за једнократну употребу;
2. Налепнице;
3. Амбалажа за паковање доказног материјала;
4. Папирне кесе за доказни материјал и селотејп траке;
5. Трака за печаћење;
6. Коверте;
7. Сет одвијача и батеријска лампа.

Пожељна опрема:

1. Фото-апарат и/или камера за снимање лица места и информација на екрану уређаја;
2. Екстерне батерије;
3. Антистатичке кесе;
4. Фарадејеве вреће или друго адекватно паковање;
5. Водоотпорни маркери;
6. Папирни новчаник за криптовалуте и/или хардверски новчаних за криптовалуте;
7. Екстерни медији за складиштење података;
8. Уређај за спречавање уписивања података на складиштену меморију која је предмет истраге;
9. Уређај са одговарајућим алатима.

Напомена: Веома је важно да полицијски службеник фотографисање не врши својим мобилним телефоном, зато што се такав материјал код савремених паметних телефона аутоматски шаље на клауд – удаљену локацију на интернету. Такође се врши и анализа, од стране компанија Гугл и Епл, да ли се на телефону налази недозвољен и штетан садржај. Ово је нарочито важно ако се ради о материјалу насталом злоупотребом деце у порнографске сврхе на интернету. Овако пронађен материјал никако не треба фотографисати сопственим мобилним телефоном већ искључиво адекватним уређајем који нема интернет конекцију (фото-апарат).

2.2. Долазак на лице места првог реаговања на електронске доказе (претресање)

Приликом доласка на место догађаја или током претресања просторија где постоји могућност да се налазе електронски уређаји и подаци, полицијски службеник је дужан да обезбеди просторију и електронски уређај. Такође, свим неовлашћеним лицима приликом доласка на место претресања обавезно ограничити приступ уређајима и подацима. Лица морају бити одвојена од компјутера, мобилних телефона, хард дискова као и уређаја који служе за напајање.

Битно је да се осумњичени одмах приликом уласка у просторије које се претресају одвоји од рачунара и других уређаја које користи (паметних телефона, конзола и сл.) како не би покушао да их угаси или уништи.

Након тога, потребно је да се лоцирају битни предмети и уређаји као што су: компјутери, рутери, мобилни телефони, хард дискови, УСБ меморије, меморијске картице, дигитални фото-апарати и сл. Поготово је битно да се лоцирају они уређаји који су повезани на интернет како би се спречила могућност губитка података.

Привремено одузимање електронских уређаја је први контакт са предметом који орган поступка остварује, самим тим од изузетног је значаја да наведена радња буде адекватно спроведена. Привремено одузимање предмета чија се законитост може довести у питање, у великој мери може довести у питање и целокупно поступање. Имајући у виду наведено, ради очувања доказивости, изузетно је важно да први корак у поступању буде правовремен и спроведен на јасно дефинисан начин (видети дијаграм поступања приликом претресања – слика 2).

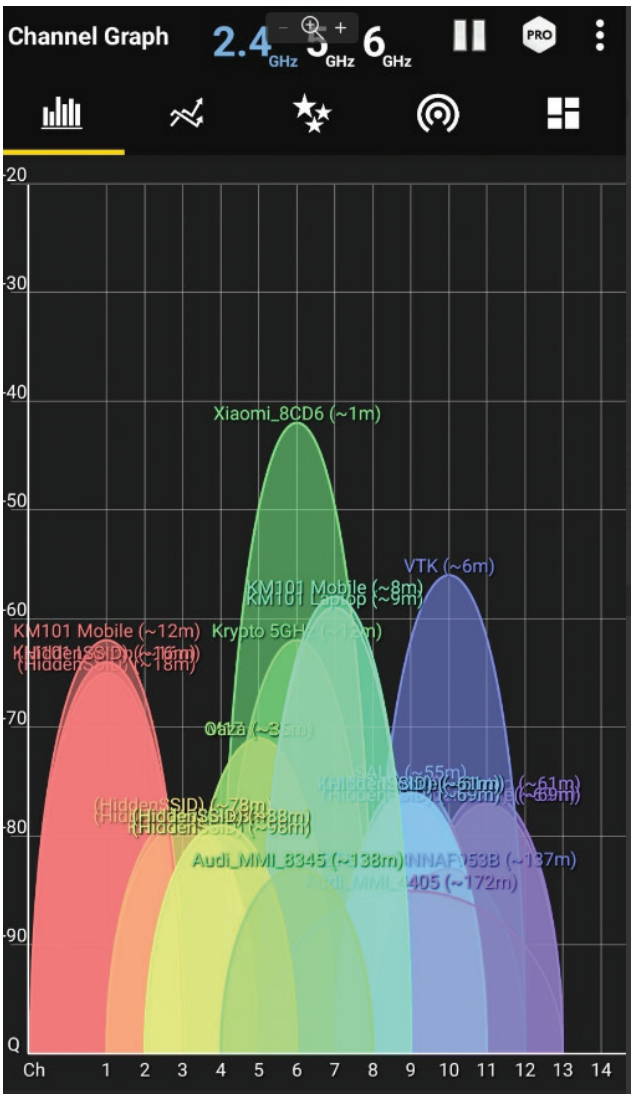
2.3. Тријажа

Пре одузимања електронских уређаја, по правилу, се врши тријажа. Тријажа електронских уређаја представља процес одлучивања који ће се уређаји привремено одузети из скупа пронађених уређаја. Имајући у виду да у приручницима најбоље праксе за област дигиталне форензике, тријажа електронских уређаја представља неизоставан део, зачуђује чињеница да се она релативно ретко спроводи у нашој пракси. Наиме, изостављањем тријаже привремено ће се одузети уређаји који не могу садржати податке који се могу довести у везу са извршењем кривичног дела. Као пример, навешћемо мобилне телефоне старе више од десетак година којима притом недостају поједине компоненте попут батерије и уређаје које користе деца осумњиченог лица, родитељи или у неким случајевима чак и лица која заједно са осумњиченима деле пословни простор. Привремено одузимање оваквих уређаја неминовно води ка вештачењу уређаја, које је, по правилу, компликованије и дуготрајније у односу на друга вештачења, с обзиром на то да је неопходно прво надоместити недостајуће компоненте и одговарајуће изворе напајања. Затим, као резултат вештачења, предмет који орган поступка води биће безразложно оптерећен подацима који немају никакве везе са извршењем кривичног дела.

Такође, међу уређајима које не треба одузимати су носачи СИМ картица, штампачи, скенери, тастатуре, мишеви и други уређаји који не могу бити носиоци меморије и самим тим на основу истих се не могу утврдити чињенице у вези са решавањем кривичног дела уз употребе дигиталне форензике, а у многоме оптерећују радње које се спроведе приликом вештачења.

Тријажу уређаја треба спроводити и приликом дефинисања наредби за претресање, односно вештачење, а посебно у случајевима када треба брзо одговорити на исте и када није потребна анализа свих уређаја и проналажење свих података, већ када се зна или очекује да се постојање одређеног садржаја налази у само једном уређају или неколико њих, а не у свим привремено одузетим уређајима.

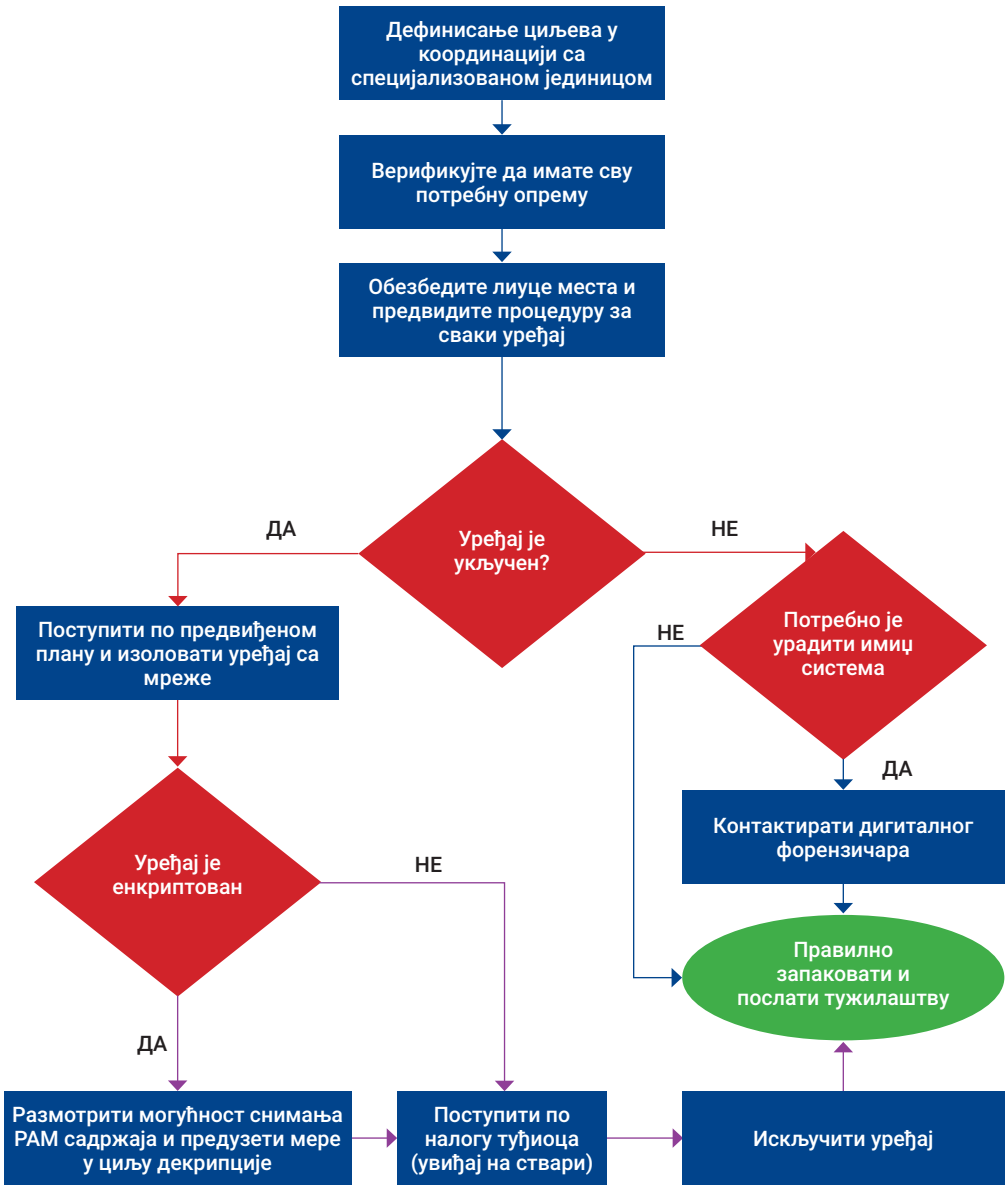
Прво је потребно, на лицу места, проверити и регистровати бежичну мрежу која се користи, као и чињеницу да ли је иста откључана или закључана. За то се може користити апликација за паметне телефоне „Wi-Fi analyser" https://rb.gy/73uj6c. На слици испод дат је пример скениране бежичне мреже (слика 1) где највиши пик одговара најближем рутеру који је удаљен од мобилног телефона којим се врши скенирање.



Слика 1

Након обезбеђења просторије пожељно је фотографисати распоред уређаја који се у простору налазе, да би се документовало где се исти налазе и у каквом су стању. Даље поступање зависи од природе предмета по којем се поступа, као и од претходно дефинисаних циљева и задатака приликом припреме за претресање.

Следећи дијаграм (слика 2) приказује генерално поступање са електронским уређајима приликом претресања. Обухваћене су најчешће дилеме везане за поступање са уређајима када су укључени или не. Посебности приликом поступања са рачунарима и мобилним телефонима дати су у посебним одељцима.



Слика 2

2.4. Прикупљање података о електронским уређајима

Приликом привременог одузимања електронских уређаја, неопходно је једнозначно идентификовати уређај утврђујући марку, модел, серијски број или другу идентификациону ознаку. Уколико уређаји који се привремено одузимају нису правилно идентификовани у записнику о вештачењу, као финалном производу вештачења, не могу се правилно означитии што значи да се потенцијално не могу довести у везу са лицем од кога су одузети.

Информације о уређају као што су примењени системи заштите података, уочене модификације оперативног система и приступне лозинке су често од виталног значаја за касније анализе, у погледу квалитета и квантитета података који се са уређаја могу преузети, те је приликом привременог одузимања неопходно прикупити и документовати такве информације, наравно ако је лице које их поседује вољно да их преда без физичког контакта са уређајем.

2.5. Паковање електронских уређаја

По правилу, привремено одузети уређаји се приликом одузимања пакују и паковање се печати на адекватан начин (углавном адекватном самолепљивом траком). Овом приликом нећемо улазити у посебно појашњење појма адекватног печаћења, с обзиром да то превазилази оквире дигиталне форензике. Рецимо само да печат треба да буде такав да јасно показује да је паковање отварано, уколико до тога дође. Само паковање треба да буде такво да обезбеди како заштиту уређаја од физичких оштећења, тако и заштиту интегритета података који се на уређају налазе.

Појам заштите уређаја од физичких оштећења је, мање-више, сам по себи јасан. Такође је јасно да је практично немогуће паковањем заштити електронски уређај од сваког могућег физичког утицаја. У том смислу, може се рећи да је електронски уређај адекватно заштићен од физичких оштећења када паковање, у коме се налази, обезбеђује заштиту од физичких утицаја које је могуће очекивати у планираном начину складиштења или транспорта.

Са друге стране, заштита интегритета података на уређају представља мало апстрактнији појам. Генерално гледано, интегритет података се може угрозити на три начина:

- Измена података непосредним руковањем уређајем представља измену, додавање или брисање података на начин сличан свакодневном коришћењу уређаја. Заштиту од оваквог вида угрожавања интегритета података пружа адекватно печаћење паковања о чему смо раније говорили.
- Измена података коришћењем специјализованих интернет сервиса најчешће представља или брисање података или постављање додатног слоја заштите података задавањем специфичне команде путем интернет сервиса који је, по правилу, у власништву произвођача уређаја. Најефикаснији начин за заштиту од оваквог вида угрожавања интегритета података јесте онемогућавање комуникације уређаја и интернет мреже, обавезно стављањем уређаја у авио мод и Фарадејеву врећу.
- Аутоматизована заштита података јесте посебан вид заштите података који врши аутоматско или брисање података или постављање додатног слоја заштите података уколико се испуне одређени, унапред дефинисани, услови. Велики проблем код оваквих заштита лежи у чињеници да, по правилу, представљају

део система заштите података на уређајима специјализованим за безбедну комуникацију, те да није могуће утврдити на који тачно начин заштита ради, и самим тим применити најбољи могући начин за, најпре заштиту интегритета а затим и аквизицију података. Нажалост, не постоји универзално применљив ефикасан начин борбе против оваквог вида заштите. Једноставно, разлике у примењеним решењима система заштите међу различитим произвођачима су сувише велике. Тако, идеално решење за један уређај је истовремено и потпуно погрешно решење за други. Оно што јесте заједничко за све уређаје јесте неопходност документовања уочених специфичности уређаја, чиме се у великој мери повећавају шансе да се дође до података са уређаја (видети пример активног програма за криптовање података Веракрипт).

Само паковање поред потписа лица од којег се уређај одузима и/или лица које уређај одузима, треба да носи и ознаку предмета у оквиру кога је предузето привремено одузимање, информације о идентификацији уређаја и података о лицу од кога се уређај привремено одузима. Из већ изнетих разлога, документи који садрже додатне информације о уређају, као и податке о предузетим радњама на уређају треба да прате уређај или у самом паковању или као прилог паковања.

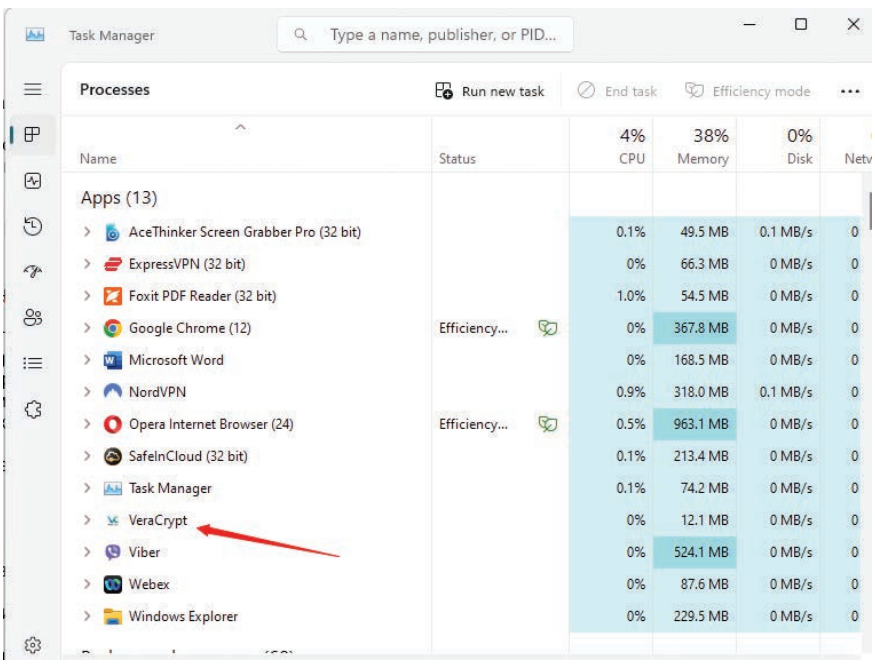
ПОСТУПАЊЕ СА РАЧУНАРИМА И РАЧУНАРСКОМ ОПРЕМОМ

3. Поступање са рачунарима и рачунарском опремом

Приликом поступања са рачунарима и лаптоповима потребно је поштовање одређених процедура, правила и поступака како би се обезбедили електронски докази на правно и технички ваљан начин.

Правило: Уколико је уређај укључен – НЕ ИСКЉУЧИВАТИ ГА

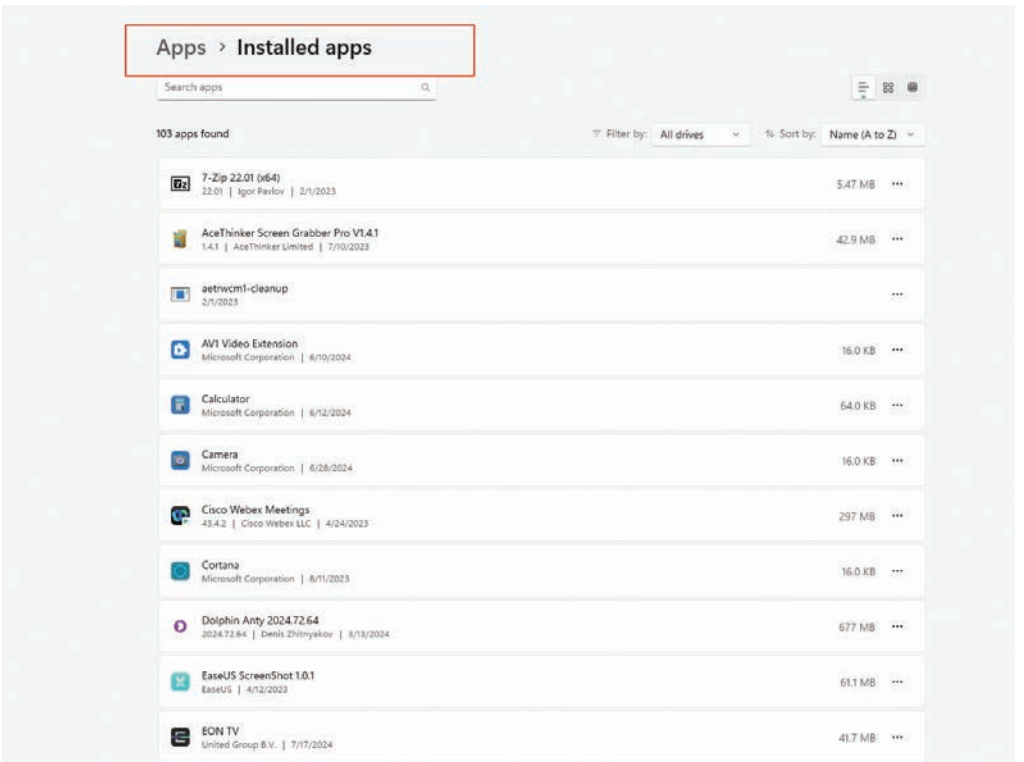
- Проверити да није укључен неки софтвер за брисање података локално или даљински (системска опција Windows Reset, софтвери Eraser, BitRaser и др.). Провера се може извршити на тај начин што се у Виндоус ОС притисну тастери „ctrl-alt-del“ којим се излиставају сви активни процеси у рачунару. Уколико јесте, ОДМАХ искључити уређај из напајања, односно извадити батерију из лаптопа.
- Изолујте уређај из мреже осим ако немате директан и ауторизован приступ меморији у облаку (клауд) са којим је уређај повезан.
- Искључите чувар екрана и закључавање рачунара (лаптопа) како уређај не би упао у мод хибернације, тј. аутоматски се закључао.
- Проверите да ли уређај има покренут неки софтвер за енкрипцију података (Битлокер, Веракрипт, ПГП диск и др.). Провера се може извршити на тај начин што се у Виндоус ОС притисну тастери „ctrl-alt-del“ којим се излиставају сви активни процеси у рачунару (слика 3).
- Ако је рачунар укључен, прибележити и фотографисати све тренутно отворене прозоре на десктопу. Водити рачуна да не дође до измене података и да се буде што је могуће мање инвазиван. Код укључених рачунара потребно је посебно обратити пажњу на скривене иконице у таскбару (програми за енкрипцију, антифорензик програми, Битлокер и сл.).



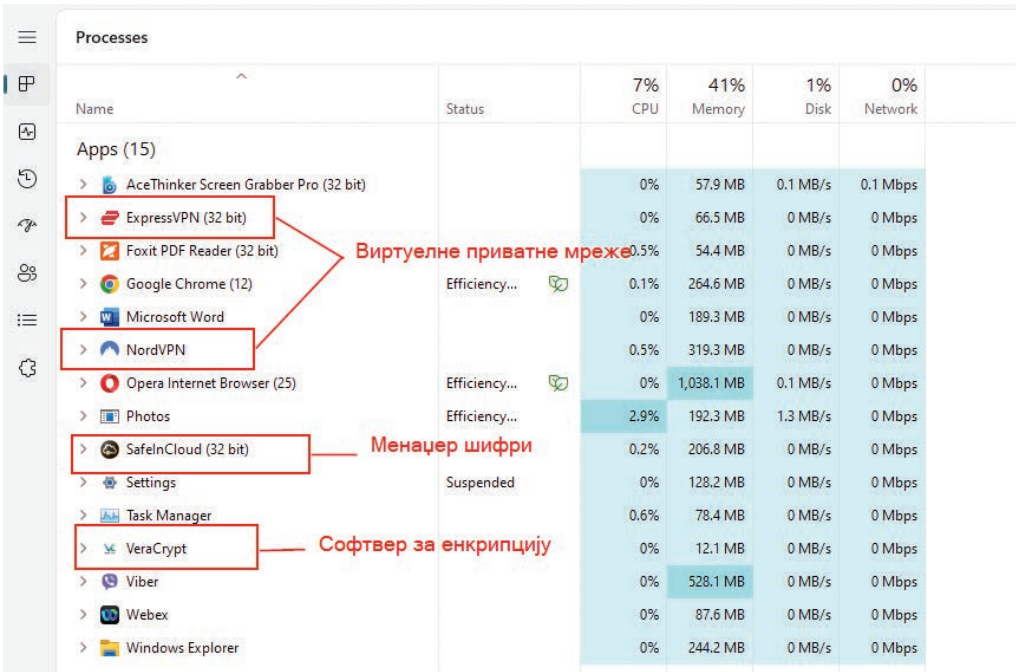
Слика 3

Уколико је активан неки програм за криптовање велика је вероватноћа да се шифра за тај програм може наћи у RAM меморији. Контактирати дигиталног форензичара или инспектора за ВТК, у складу са планом и дефинисаним циљевима који су претходили претресању!

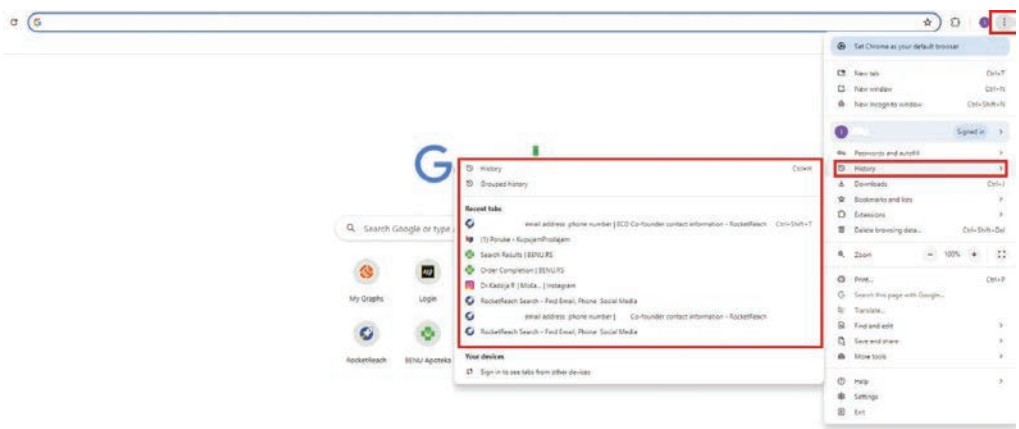
- У складу са постављеним циљевима и уз сагласност поступајућег тужиоца, извршити увиђај ствари (уређаја, рачунара) уз фотодокументовање криминалистичког техничара.
- Сходно постављеним циљевима претресања, могуће је да ће бити важно:
  - Пронаћи програме који су инсталирани на рачунару (код Виндоус ОС ићи на „search-add and remove programs“ да би добили листу инсталираних програма - слика 4).
  - Пронаћи активне клауд сервисе (One drive, Box, Dropbox, итд.), менаџере шифри (Keeper, Safe in Cloud, 1Pasword, итд.), ВПН програме (Nord VPN, Express VPN, Ghost VPN, итд.). Провера се може извршити на тај начин што се у Виндоус ОС притисну тастери „ctrl-alt-del“ којим се излиставају сви активни процеси у рачунару – слика 5).
  - Пронаћи историју претраживања на прегледачима типа Гугл хром, Опера, Мозила, итд. (код Гугл хром преглед историје претрага се врши на начин приказан на слици 6).
  - Пронаћи апликације за чување приватних кључева код криптовалута (објашњено у посебном поглављу).
  - Пронаћи галерије слика и фотографија (код Виндоус ОС ићи на „search-photos“).



Слика 4



Слика 5



Слика 6

По завршетку увиђаја на ствари и након уређене фотодокументације, уређај искључити и даље поступати као са искљученим уређајима (форензичка копија - прављење имиџа, паковање).

Искључивање укљученог рачунара може се спровести на неколико начина. Такозвано „нормално“ искључивање („start-power-shutdown“), затим искључивање преко тастера на кућишту, у случају да корисник нема дозволу да нормално угаси рачунар (нема дозволу администратора), или у случају када сте приметили да је покренут процес који може да уништи податке и не можете да га прекинете. Начин искључивања рачунара чупањем каблова, односно изненадним прекидом напајања може се применити само у крајњим ситуацијама, када је потребно спречити процесе који могу уништити податке, када је потребно спречити настанак квара и оштећења и сл. Напомињемо да се применом ове методе искључивања повећавају шансе за настанак фаталног квара рачунара.

Уколико се ради форензичка копија обавезно је да се уради хеширање имиџ фајла како би се могле упоређивати накнадне копије са оном која је урађена на лицу места (непромењеност електронског доказа).

Правило: Уколико је уређај искључен – НЕ УКЉУЧИВАТИ ГА

Потребно је потражити шифре или пинове записане на папирићима који се налазе у просторијама где се врши претресање, а уколико осумњичени добровољно дâ приступне параметре исте, на потврду о привремено одузетим предметима, одузети и констатовати службеном белешком. Чак и ако уређај није у потпуности криптован добро је узети приступне параметре, јер су можда закључани појединачни фајлови или делови диска, а могуће је да је осумњичени исте шифре користио и за друге системе.

У складу са постављеним циљевима пре претресања, уколико је потребно, узети клон-имиџ система у координацији са дигиталним форензичаром.

У складу са Упутством о стандардним оперативним процедурама поступања са електронским уређајима и подацима, полицијски службеник је дужан да потражи и одузме све повезане уређаје за складиштење електронских података. Сваки одузети предмет потребно је посебно упаковати. Рачунар је потребно упаковати у адекватну амбалажу која омогућава спречавање оштећења уређаја и измена података, облепити селотејп траком, а испод селотејп траке потребно је ставити бели папир. На овом папиру потребно је да се осумњичени потпише водоотпорним маркером, чиме потврђује стање у којем је предмет одузет. Мобилни телефон, хард/ССД диск, УСБ меморију, као и други електронски уређај који се одузима потребно је упаковати у коверту, облепити селотејп траком преко које осумњичени треба да се потпише водоотпорним маркером, чиме потврђује стање у којем је предмет одузет.

На сваком упакованом и одузетом предмету исписују се подаци о лицу од кога је предмет одузет, подаци о одузетом предмету – КУ, број предмета, редни број из потврде.

Сви одузети предмети треба да буду описани у потврди о привремено одузетим предметима.

Поред рачунара и рачунарске опреме, одузимају се и сви други уређаји за складиштење електронских података, приручници за употребу тих уређаја и белешке.

У зависности од процене, некада неће бити потребно одузимати цео рачунар већ ће бити довољно извадити хард диск или ССД диск из рачунара који је предмет претресања. Треба имати у виду и то да је у одређеним случајевима целисходније и правилније одузети цео рачунар, поготово ако је чврсти диск криптован неким системским програмом за енкрипцију, као што је Битлокер код Виндоус ОС. Код Виндоус ОС је битан ТПМ чип за енкрипцију, који служи за комуникацију између матичне плоче и хард диска и директно је одговоран за правилно функционисање Битлокера и детекцију приступа криптованом хард диску, па је у овом случају правилно одузети комплетан рачунар са кућиштем.

Остали уређаји, као што су мишеви, тастатуре, монитори и персонални штампачи (периферни) немају посебан значај за електронске доказе јер немају своју меморију или ако имају, она је ограниченог капацитета.

Код одузимања лаптопова примењују се иста правила као и код класичних десктоп рачунара уз одређене специфичности.

Код одузимања и паковања лаптопова прво уклањамо батерију (ако је могуће), а затим искључујемо кабл за напајање. Новији лаптопови имају батерију и меморијске дискове интегрисане са матичном плочом и у тим случајевима, уколико на лицу места нема полицијских службеника са специјализованим знањима, потребно је да се лаптоп одузме без уклањања батерије.

Такође, потребно је уз лаптоп који се одузима приложити и кабл за напајање.

Уређаје који у себи имају податке од значаја потребно је чувати на сигурном месту и у контролисаним условима - ниска влажност ваздуха, заштићеност од електричног пражњења (статички електрицитет), контролисана температура ваздуха, заштита од радио-таласа (посебно за мобилне телефоне, таблете и сл.) и заштита од механичког оштећења.

Када су у питању остали меморијски уређаји пронађени на лицу места, као што су преносиве меморије за складиштење дигиталних података (УСБ меморије - слика 7), меморијске картице, екстерни хард дискови, оптички дискови, са њима се поступа као са меморијама из рачунара и лаптопова. Сходно претходно дефинисаним циљевима, код оваквих уређаја се врши по потреби увиђај ствари, форензичка копија и одузимање и паковање. Највећи проблем је уочити овакве уређаје приликом претресања јер су годинама њихове димензије постајале све мање, а меморијски капацитети све већи и са различитим облицима израде.

Слика 7

ПОСТУПАЊЕ СА МОБИЛНИМ УРЕЂАЈИМА ЗА КОМУНИКАЦИЈУ

4. Поступање са мобилним уређајима за комуникацију

Под мобилним уређајима за комуникацију подразумевамо класичне мобилне телефоне, паметне телефоне и таблет уређаје. С обзиром на то да су паметни мобилни уређаји углавном са ОС Андроид и ИОС, специфичности тих оперативних система су посебно описане коришћењем дијаграма, док су процедуре које су универзалне за све мобилне уређаје за комуникацију дате у доле наведеном тексту.

Полицијски службеник не треба да укључује мобилни телефон или таблет рачунар који је искључен. Са искљученим мобилним телефоном или таблет рачунаром, полицијски службеник поступа као и са искљученим рачунаром и другом опремом, односно одузима их и пакује на исти начин као и рачунаре и лаптопове.

Уколико је мобилни уређај упаљен, а сам телефон или таблет рачунар закључан, и осумњичени добровољно хоће да дâ приступну шифру, потребно је да полицијски службеник искључи закључавање екрана преко поставке паметног телефона или таблет рачунара (енг. settings) и да то евидентира фотографијом и службеном белешком.

Уколико лице од кога се одузима мобилни телефон добровољно дâ приступну нумеричку лозинку или шаблон, потребно је исту написати (или нацртати шаблон) на амбалажу у коју се пакује уређај. Треба напоменути да се приликом одузимања мобилних телефона води рачуна о свим деловима и повезаним уређајима, јер готово увек у истима у одговарајућим слотовима постоје СИМ и/или СД картице, осим евентуално у случајевима када мобилни телефон има опцију еСИМ, које уколико се не наведу у потврди о одузетим предметима у каснијем поступку могу бити оспорене и као такве можда неће бити предмет радње претресања, односно вештачења.

У складу са постављеним циљевима, и уз сагласност поступајућег тужиоца, извршити увиђај ствари (уређаја, мобилног телефона, таблета) уз фотодокументовање криминалистичког техничара.

Поступак приликом одузимања мобилног телефона или таблет рачунара који је укључен:

1. Укључити авио мод ако је могуће (код већине мобилних телефона и таблет
2. рачунара је могуће укључити чак и када је екран закључан);
3. Проверити и ручно искључити, ако је неопходно, све бежичне конекције (вај-фај, блутут, НФЦ);
4. Повезати мобилни телефон или таблет са екстерном батеријом;
5. Уколико се одузима мобилни телефон или таблет рачунар са ИОС оперативним системом (Епл уређаји) убацити адаптер у уређај да би се спречио улазак у рестриктивни мод УСБ-а мобилног телефона, односно таблет рачунара;
6. Ставити мобилни телефон или таблет рачунар у Фарадејеву врећу (антистатичка торба која формира ефекат „индукционог штита“ за све производе осетљиве на електростатику), или на други адекватан начин обезбедити уређај, заједно са прикљученом екстерном батеријом (уколико полицијски службеник нема Фарадејеву врећу и батерију, запаковати мобилни телефон или таблет рачунар у адекватно паковање које ће, након тога, запечатити). Уколико полицијски службеник

не поседује Фарадејеву врећу, потребно је да телефон увије у алуминијумску фолију како би блокирао долазне и одлазне сигнале;

7. Обавестити надлежног јавног тужиоца о поступању.

Уколико је могуће, битно је да се тачно утврде ИМЕИ бројеви мобилног телефона или таблета (уколико има слот за СИМ картицу или еСИМ опцију). Подаци о ИМЕИ бројевима можемо добити укуцавањем *#06# кода на тастатури за позивање у телефону, односно таблету. На сликама доле (слике 8 и 9) имате приказ података који се добију приликом укуцавања кода *#06#.

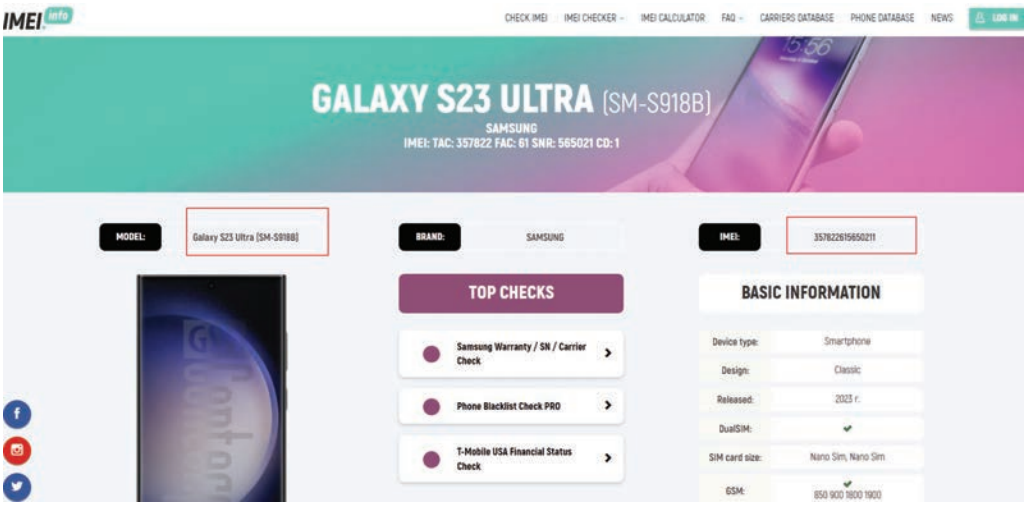
Слика 8

ИМЕИ бројеви (сваки слот за СИМ картицу их има) су 15 цифара које идентификационо повезују СИМ картицу са мобилним телефоном. Код старијих мобилних телефона (код којих је постојала могућност уклањања батерије) ИМЕИ бројеви су се налазили одштампани и на полеђини телефона (испод батерије).

Слика 9

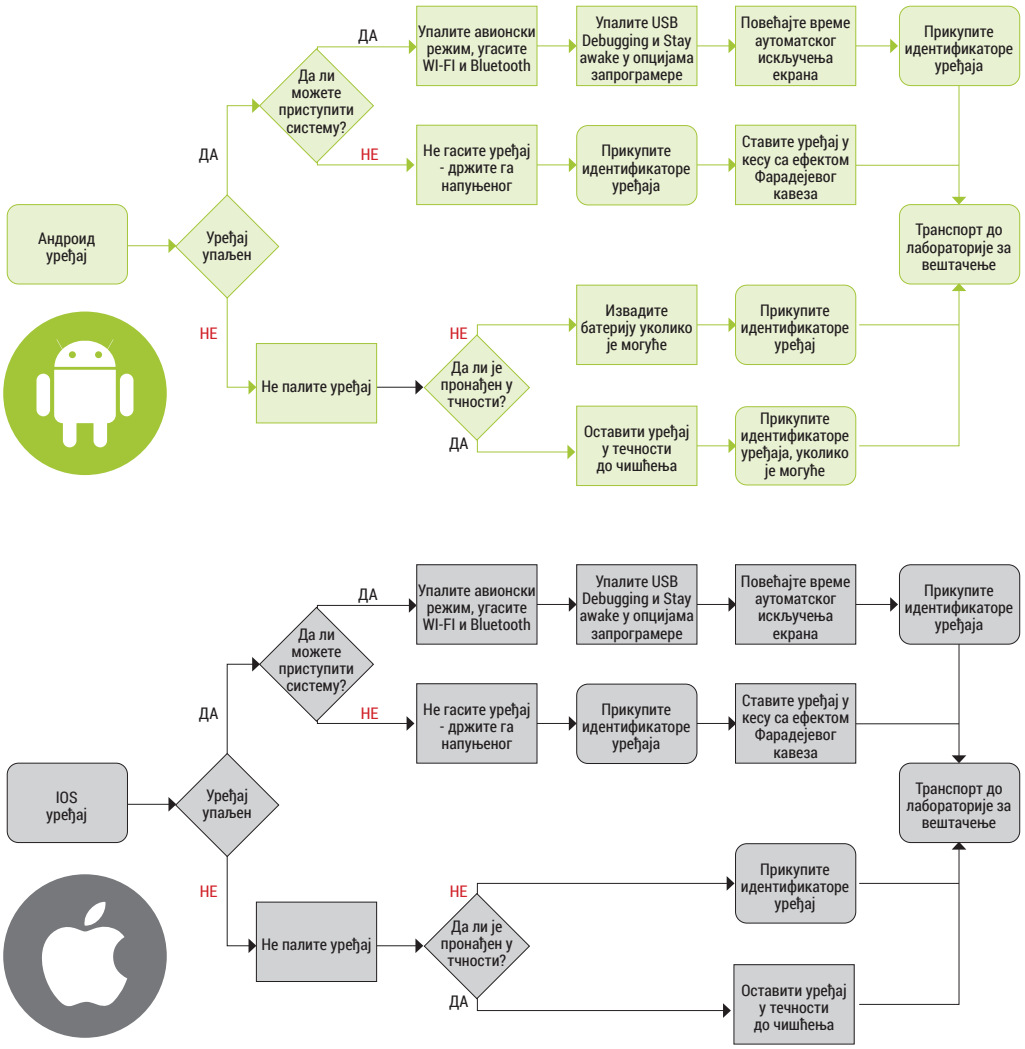
С обзиром да постоје софтверски алати за промену ИМЕИ броја увек је добро проверити да ли ИМЕИ број који смо пронашли на телефону одговара ИМЕИ броју произвођача. То се може проверити на интернет сајту https://rb.gy/c6wlzp (слика 10).

На доле приказаној слици имате резултате провере за претходно пронађене ИМЕИ бројеве код мобилног телефона Самсунг С23 ултра.



Слика 10

На дијаграмима доле (слика 11), дата су упутства како поступати са Андроид и ИОС мобилним уређајима у различитим ситуацијама (упаљени-угашени, потопљени у течност или не).



Слика 11

Омогућавање функција „debugging“ и „stay awake“ даје касније, дигиталним форензичарима у лабораторији, могућност за бољу и лакшу анализу садржаја на мобилном телефону. Више о начину омогућавања за ИОС на линку https://rb.gy/mrlk1z и Андроид на линку https://rb.gy/lckzrt. Уколико се активира функција „debugging“ и „stay awake“ (да екран стално буде у активном стању) потребно је да се то евидентира фотографисањем и службеном белешком.

Оба оперативна система (Андроид и ИОС) захтевају да корисници имају Гугл или Епл налог преко којих се врши бекап свих података са телефона,ȃ што треба имати у виду приликом увиђаја на ствари ако се исти ради на телефону. Уколико се тада не изврши увид, веома често се дешава да битни електронски докази остану и даље у облаку, односно недоступни за даљу форензичку анализу.

ПОСТУПАЊЕ СА ОСТАЛИМ УРЕЂАЈИМА КОЈИ У СЕБИ ИМАЈУ СКЛАДИШТЕЊЕ ЕЛЕКТРОНСКИХ ПОДАТАКА

5. Поступање са осталим уређајима који у себи имају складиштење електронских података

Под осталим уређајима подразумевамо дигиталне камере, глобални навигациони сателитски систем (ГПС навигације), паметне телевизоре, ИП камере, дронове, ауто камере, конзоле за видео игре, аутомобилске путне рачунаре и др.

Заједничка карактеристика им је да поред екстерне меморије (меморијске картице или другог меморијског модула) имају углавном и интерну меморију, најчешће мањег капацитета, али која може да садржи битне податке.

Процедура би обухватала следеће:

- По лоцирању уређаја исти фотографисати.
- Уређај се документује са идентификационим бројем (нпр. идентификациони број камере или ГПС навигације).
- Проверити да ли постоји екстерна меморија и уколико постоји извадити је и документовати.
- Урадити форензичку копију екстерне меморије.
- Уређај (камеру) би требало упалити и проверити интерну меморију.

Уколико постоји садржај који је битан и може се извући:

- Повезати уређај каблом и направити копију (немају сви уређаји ту могућност).
- Убацити нову меморијску картицу и копирати садржај (направити логичку копију интерне меморије).
- Уколико друге опције нису могуће фотографисати садржај интерне меморије.
- Документовати поставке уређаја: датум, време и временску зону.

Уколико се електронски докази налазе на уређају за видео надзор, потребно је да се упореди датум и време које се налази на уређају (да ли се поклапа са стварним датумом и временом) и то евидентирати и фотографисати. Такође, потребно је фотографисати екран, угасити рекордер да не би дошло до преписивања података, откачити каблове, идентификовати марку и модел уређаја за видео надзор.

Уколико се електронски докази налазе на дрону потребно је, уколико је дрон упаљен, фотографисати изглед и модел дрона као и контролни екран на дрону, угасити дрон, изоловати га од ГПС сателита и било каквих других бежичних сигнала (Фарадејевом врећом или на други начин) и потражити спољну меморију (меморијску картицу).

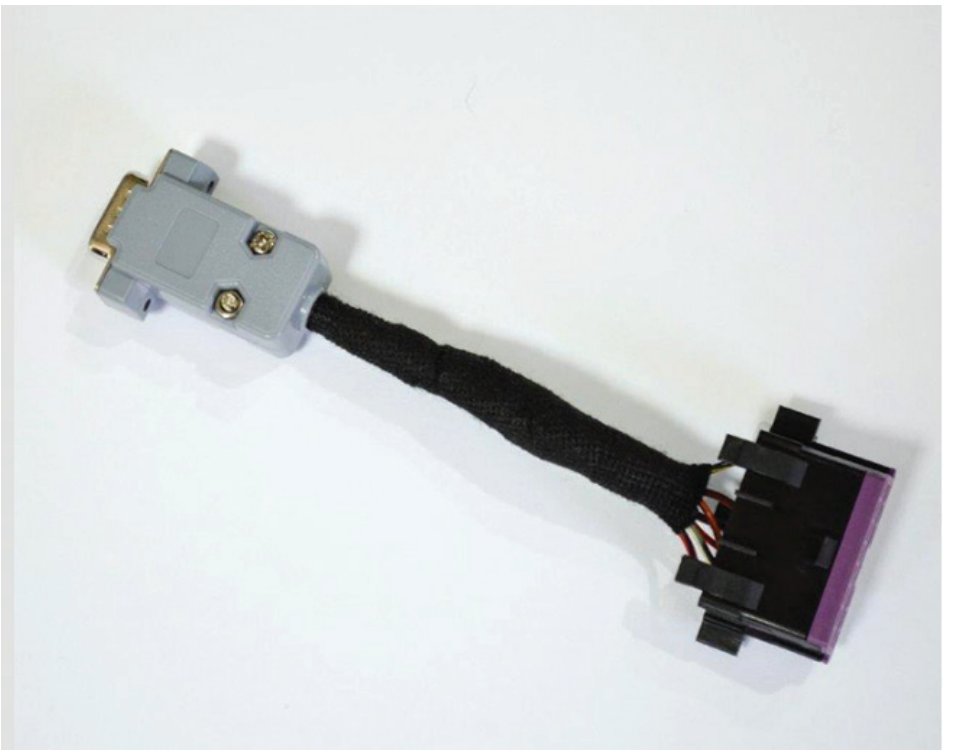
Аутомобилски паметни системи имају све већу заступљеност у модерним аутомобилима. Имају своју меморију и углавном чувају две врсте података:

- Информациони подаци о возилу и возачу (ГПС, блутут уређаји, повезани мобилни телефони, позиви, именици, поруке итд.).
- Системски подаци о возилу (стање мотора, сензор кочења, сензор дистанце, притисак гума, сервиси и сл.).

Сви ови подаци се налазе у логовима меморије путног рачунара возила. Битни подаци до којих је могуће доћи су:

- Навигациони подаци (ГПС, брзина, правац кретања, датум, време).
- Отварања врата и пртљажника.
- Коришћење предефинисаних подешавања седишта за корисника (нпр. аутомобили са више корисника код којих сâм систем препознаје ко је користио возило на основу кључа који је употребљен).
- Позиви, поруке и именици копирани са телефона.

Важно је напоменути да се код новијих возила најчешће ради измештање ОБД конектора (слика 12) због спречавања крађе аутомобила. ОБД заштита је заправо уклањање ОБД конектора из аутомобила и постављање на његово место нестандардног конектора, док власник возила добија адаптер којим овај нестандардни конектор поново враћа на ОБД. Тај конектор стоји ван возила и носи се приликом одласка у сервис, како би се сервисери могли конектовати. Свака ОБД заштита се прави насумичним одабиром пинова у конектору тако да ниједна није идентична другој, па је за анализу ових података, уколико је ОБД заштита активирана, потребно пронаћи измештени ОБД додатак како би се извршила адекватна форензичка анализа путног рачунара возила.



Слика 12

Када говоримо о преносивим уређајима (слика 13), постоји неколико типова таквих уређаја који укључују веома мале рачунарске системе интегрисане у одећу или додатке. Обично имају сет сензора (нпр. ГПС, жиро сензор, сензор откуцаја срца) и комуникацијске функције (нпр. WLAN, блутут, мобилна мрежа).

Слика 13

Такви уређаји могу да чувају поруке и додатне информације као што су адресари, заказани састанци, календари, активности корисника, географске информације и белешке. Они такође имају могућност синхронизације информација са паметним телефоном или рачунаром. Потенцијални докази за узети у разматрање укључују:

- Адресар
- Календаре заказивања
- Е-маил
- Информације о географској локацији
- Догађаје
- Напомене
- Бројеве телефона

Неки преносиви уређаји могу да садрже уређај за складиштење, као што је УСБ меморија, УСБ токен или чак и камера. Популарни примери носивих уређаја су паметни сатови и сатови за фитнес.

6. Поступање у пословној електронској мрежи

У случају да се електронски подаци и докази налазе у пословној мрежи или на серверу сложене инфраструктуре потребно је обезбедити место где се врши претресање, као и присуство систем администратора, а затим контактирати надлежног јавног тужиоца.

Уколико је претресање просторија у оквиру сложеније серверске инфраструктуре (фирме, интернет провајдера и сл.) део претходно дефинисаних циљева и задатака приликом припреме за претресање, потребно је предвидети и присуство дигиталног форензичара МУП-а.

Приликом припрема за претресање просторија где се налази серверска инфраструктура неке пословне мреже, потребно је одговорити на нека питања која су битна за правац у којем ће се само претресање одвијати.

Пре свега:

- Да ли је у реду да оставимо кориснике пословног сервера (који најчешће нису умешани у криминалну активност) без сервиса? Ово је веома битно, зато што су сервери основни делови функционисања сваке фирме.
- Да ли је потребно да одузимамо серверску опрему или је довољан увиђај ствари и/или форензичка копија?
- Да ли је потребна сарадња систем администратора?
- Уколико јесте, да ли му се може веровати, односно да ли постоји сумња да је и он укључен у криминалну активност?
- Да ли је јасно које су информације битне за документовање на серверу?
- Да ли нам је позната серверска инфраструктура, као и оперативни систем који је инсталиран на серверу?
- Да ли можемо сервер откачити са интернета, односно привремено изоловати да би се спречио даљински приступ и брисање података?

Углавном ће се процес узимања података са сервера сводити на прављење логичких копија сумњивих фолдера и фајлова али треба размотрити и потребу за прављењем копија логова догађаја, поставки активних директоријума, фолдера електронске поште, као и бекапа.

Приликом припремања претресања просторија сложене пословне инфраструктуре неопходно је предвидети улазак и обезбеђивање просторија и сервера од стране специјализованих (интервентних) јединица полиције, како би се брзом и муњевитом акцијом спречила могућност уништења постојеће инфраструктуре, као и физичко прекидање приступа интернету, односно прекидања конекције сервера са другим серверима и сервисима (нпр. у иностранству).

ПОСТУПАЊЕ СА ДИГИТАЛНОМ ИМОВИНОМ (КРИПТОВАЛУТЕ)

7. Поступање са дигиталном имовином (криптовалуте)

Према Упутству о стандардним оперативним процедурама поступања са електронским уређајима и подацима, у поглављу бр. XI, прописан је начин поступања са криптовалутама.

Према овом упутству, само онај полицијски службеник који има потребна знања за прво реаговање на електронске уређаје и податке може поступати у случају проналаска средстава у виду криптовалута. Он тада обавезно проверава јавну адресу криптовалуте преко интернет везе и кроз јавно повезани ланац блокова – блокчејн, као и СИД фразу, односно групу речи преко адекватног софтвера за анализу. Уколико пронађе да се на адреси налазе средства – криптовалуте, привремено их одузима пребацивањем на јавне адресе виртуелних (дигиталних новчаника) чији су приватни кључеви под контролом полицијског службеника који их одузима. Такође, неопходно је учешће два полицијска службеника приликом одузимања криптовалута, као и обавештавање надлежног јавног тужиоца, те да се пренос врши на дигитални новчаник који мора бити под њиховом заједничком контролом. Постоји и процедура у случају пребацивања са виртуелног на папирни (генерисани) новчаник, као и проверавања преноса средстава од стране полицијских службеника. Као додатак овом приручнику израђено је и упутство за прављење папирног новчаника за одузимање криптовалута.

Када је трансакција неповратно реализована, полицијски службеници ће у потврди о привремено одузетим предметима навести датум и време одузимања, количину и врсту криптовалуте, износ трошкова трансакције, јавну адресу/адресе криптовалуте са које/којих је трансакција извршена, јавну адресу криптовалуте где су криптовалуте пребачене, као и хеш вредност саме трансакције.

Након што су пребацили криптовалуте на папирни новчаник који је само под контролом полиције, полицијски службеници треба да га запакују у коверту или провидну фолију на којој се види само јавна адреса, тако да се без њеног цепања не може доћи до података о приватном кључу, и да ту коверту, односно провидну фолију, обезбеде селотејп траком преко које ће се потписати лице од којег се криптовалуте одузимају.

Полицијски службеници не смеју да копирају, фотографишу нити на други начин умножавају папирни новчаник на који су пребачене криптовалуте од осумњиченог.

Полицијски службеници који су непосредно учествовали у привременом одузимању криптовалута сачиниће након одузимања службену белешку у којој ће навести податке о извршеној трансакцији одузимања криптовалута и доставити је надлежном јавном тужиоцу.

Приликом одузимања криптовалута (биткоина) постоје основна питања на која треба одговорити:

Шта се одузима?

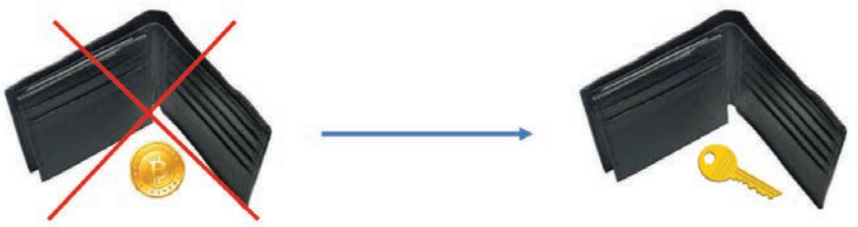
Где се одузима?

Како се одузима?

7.1. Шта се одузима?

Ако поставите ово питање неком ко није мало дубље у материји криптовалута, вероватно би вам одговорио да је логички да се одузима биткоин. Наравно да би такав одговор био погрешан. Биткоини као такви постоје на блокчејну и увек ће постојати. У време писања овог приручника у оптицају је било 19.716.450 биткоина.[7] Укупно ће бити у оптицају 21 милион биткоина и последњи ће бити изрударен негде 2140. године. Власништво над биткоинима потврђује се приватним кључевима. Хеширањем приватног кључа добија се јавни кључ а хеширањем јавног кључа јавна биткоин адреса. Обрнути поступак није могућ (да се од јавне адресе добије приватни кључ).

Дакле, **не одузимају се биткоини него посед (контрола) над биткоинима**. Посед над биткоинима се доказује власништвом над приватним кључем. Битно је напоменути и то да више лица у истом тренутку могу да буду у поседу биткоина са једне адресе (ако поседују исти приватни кључ). Зато се приватни кључ мора чувати у тајности јер је он кључ за „браву" биткоина (биткоин адресу).



Илустрација 1

Контрола над приватним кључевима се врши на три начина:

1. Новчаником инсталираним на рачунару, мобилном телефону или екстерном уређају (укључујући и хардверски новчаник);
2. Папирним новчаником (јавна адреса и приватни кључ су одштампани на папиру);
3. Од стране трећег ентитета: мењачница, берза, онлајн новчаници (приватне кључеве контролише трећи ентитет).

7 Извор https://coinmarketcap.com.

7.2. Где се одузима?

За одузимање контроле над приватним кључем потребно је, пре свега, лоцирати где се приватни кључ налази на хард диску рачунара или меморији телефона. Уколико је новчаник заштићен шифром или пин кодом биће потребна сарадња осумњиченог. Шифра може бити записана и на папиру, а у пракси се дешавало да је пин код, веома често, онај који се користи као приступ и ка другим апликацијама. Индиције за постојање новчаника са криптовалутама јесу софтверски новчаници и крипто мењачнице пронађене на рачунару или телефону (слике 14 и 15).

Слика 14

Слика 15

7.2.1. Врсте приватних кључева

Постоје 3 облика приватних кључева код биткоина:

1. У хексадецималном облику: нпр. *1E79423A4ED27608A15A2616A2B0E5E52CED330AC530EDCC32C8FFC6A520AED1*;
2. Класично похрањен у новчанику је увек дужи од јавне адресе и почиње цифром 5, нпр. *5J3hzQ41KoJX64H5YRTqS9YB9LVGacU2qusL37Ys1eVpJTgnr4u*;
3. Компресован приватни кључ који почиње са L или K, нпр. *KyoPrwwmvSZymMrJLRhePV6jTFFpGU6uMVLv5nQhkMM4dpDKaMgG*.

Проналаском приватног кључа могуће је поново конфигурисати новчаник од осумњиченог.

Код рачунара локација новчаника где се налазе приватни кључеви, уколико је подразумевано инсталиран новчаник (ако није промењена путања приликом инсталације), налази се на следећим локацијама:

- Код рачунара са Виндоус оперативним системом: (WinKey+R): *%APPDATA%\Bitcoin.*
- Код рачунара са Мекинтош оперативним системом: *~/Library/Application Support/Bitcoin/.*
- Код рачунара са Линукс оперативним системом: *~/.bitcoin/.*

7.2.2. Врсте новчаника код криптовалута

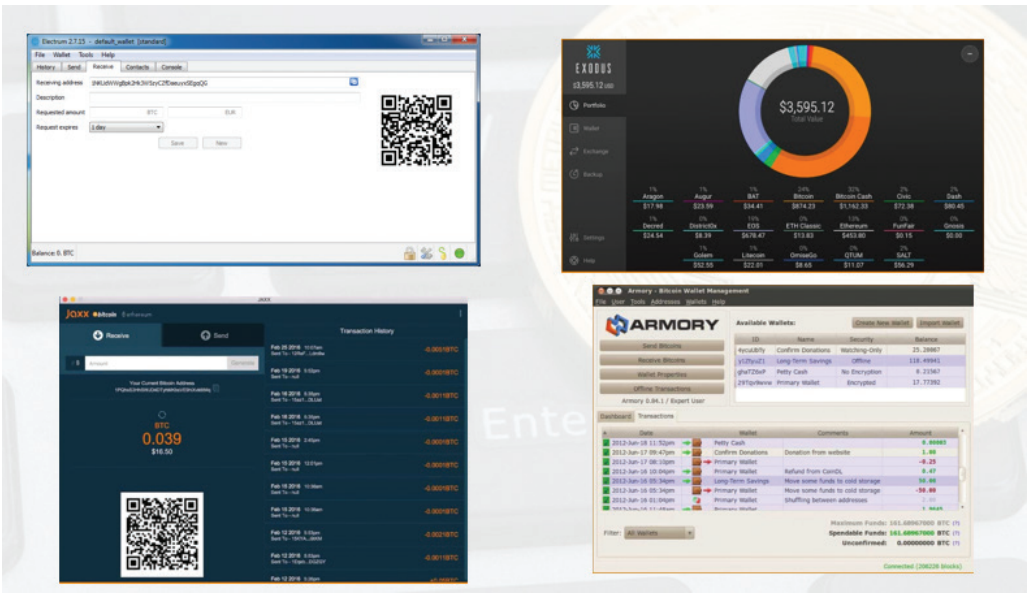
Постоје различите поделе новчаника код криптовалута, у зависности од различитих параметара њихове употребе. Тако, нпр. имамо поделу новчаника на оне код којих се приватни кључеви чувају од стране физичког лица (енг. „Non custodial“) и оне код којих се приватни кључеви чувају од стране треће стране (енг. „Custodial“). Такође имамо и поделу на вруће (енг. „Hot“) и хладне (енг. „Cold“) новчанике, према критеријуму да ли се код новчаника приватни кључеви експонирају или не на интернету.

Крипто новчанике, у односу на тип новчаника који се користи за чување приватних кључева, можемо поделити на:

1. Софтверски новчаници за рачунаре;
2. Новчаници за паметне телефоне;
3. Веб новчаници;
4. Папирни новчаници;
5. Детерминистички новчаници;
6. Хардверски новчаници.

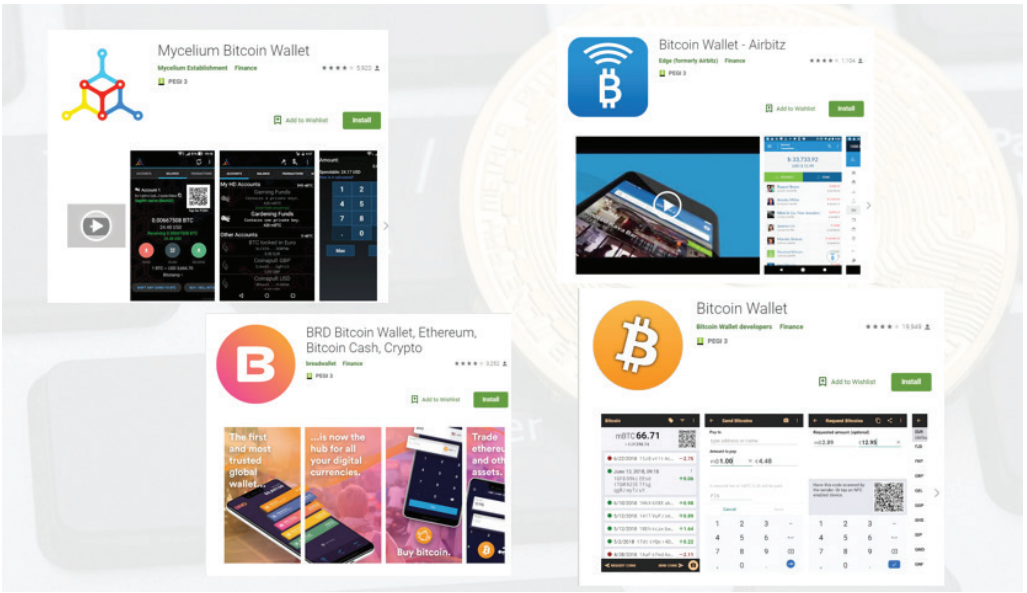
Софтверски новчаници за рачунаре су у ствари програми за персоналне рачунаре који генеришу приватне и јавне адресе у оквиру инсталације на персоналном рачунару и графичког су интерфејса. Нуде могућност бекаповања новчаника путем 12, 18, 20 или 24 речи (СИД фраза). Постоји Биткоин кор чијом инсталацијом се на меморији локалног рачунара меморише целокупан блокчејн са свим трансакцијама до тог тренутка (велика количина

података више од 700 GB). Много чешћи су лагани софтвери код којих не скида целокупан блокчејн, већ само софтвер који генерише приватне и јавне адресе а затим се конектује на најближи НОД како би ажурирао податке са блокчејна путем интернета. Ово су „Hot“ и „Non custodial“ новчаници и меморишу wallet.dat на локалном диску (садржи приватне и јавне адресе). Најпознатији су Electrum, Atomic, Exodus, Jaxx, Armory и др. (слика16). Подложни су хакерским нападима сходно рањивости оперативних система за персоналне рачунаре.

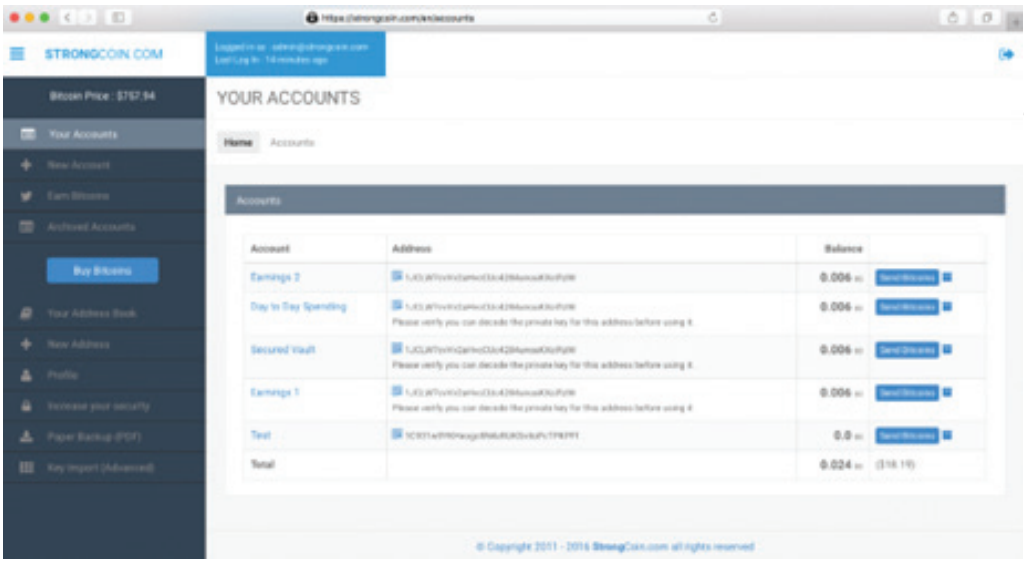


Слика 16

Новчаници за паметне телефоне су суштински апликације за најпознатије оперативне системе за паметне телефоне (ИОС и Андроид) у оквиру којих се генеришу новчаници са паровима приватних и јавних адреса. Нуде могућност бекаповања новчаника путем 12, 18, 20 или 24 речи (СИД фраза). Синхронизација са блокчејном се врши путем интернета и повезивањем на најближи Фул НОД (служи осталим корисницима мреже као карика дозвољавајући им да пренесу своје трансакције даље на блокчејн). Приступ је заштићен обично или пин кодом и/или биометријским подацима (отисак прста). Углавном се на паметним телефонима чувају мањи износи криптовалута јер је мобилни телефон лак за манипулацију и брза плаћања (QR код). Као и софтверски новчаници за рачунаре и новчаници за паметне телефоне су „Hot“ и „Non custodial“, што значи да се приватни кључеви генеришу локално на меморију телефона. Најпознатији су Mycelium, Airbitz, Breadwallet, Bitcoin Wallet (слика 17).



Слика 17



Слика 18

Папирни новчаници су новчаници код којих је приватни кључ одштампан заједно са јавном адресом (слика 19), односно ово су „Non custodial“ и „Cold“ новчаници. У време настанка биткоина честу су употребљавани за чување већих количина биткоина јер су отпорни на хаковање (немају додир са интернетом). У новије време бележе слабију употребу јер су их, у тој функцији, заменили хардверски новчаници. Карактеристика ових новчаника је да се лако могу убацити у већину софтверских новчаника. Иако су отпорни на хаковање нису отпорни на физичко уништење. Неке од онлајн адреса за генерисање папирних новчаника су https://rb.gy/nxzbik и https://walletgenerator.net.

Слика 19

Детерминистички новчаници могу бити софтверски или хардверски. Представљају систем деривације приватних и јавних кључева из СИД фразе. У оквиру BIP-39 протокола[8] предефинисано је укупно 2.048 речи енглеског алфабета које служе као фраза за бекап крипто новчаника[9]. Уколико се пронађу, записани на папиру или урезани у металу, могуће је у потпуности реконфигурисати крипто новчаник и зато се углавном чувају као бекап софтверских и хардверских крипто новчаника. Називају се и „brain wallets" уколико се само памте (без записивања).

Хардверски новчаници су специјализовани уређаји који су наменски направљени за заштићено чување приватних кључева код крипто новчаника (слика 20). Код хардверских новчаника, приликом иницијализације, генерише се СИД фраза од 24 речи (уз могућност додавања своје 25 фразе као додатна безбедносна мера). Такође се поставља и пин (4-8 цифара) за откључавање уређаја. Трансакција се потврђује на уређају тако што уређај прима иницијалну трансакцију, потписује је приватним кључем и тако потписану враћа у уређај (рачунар или мобилни телефон) и даље у блокчејн мрежу. Дакле, приватни кључ се никад не експонира и зато хардверски новчаници припадају „Cold" новчаницима, а такође су и „Non custodial" (приватни кључеви су у власништву лица). Уколико се три пута унесе погрешан пин код хардверски новчаник се ресетује на фабричка подешавања и поновна активација истог новчаника могућа је само уколико постоји СИД фраза. Најпознатији су Trezor, Ledger, KeepKey.

Слика 20

8 Извор https://rb.gy/9eqg8d.

9 Извор https://rb.gy/1ziwb8.

7.3. Како се одузима?

Одузимање криптовалута је процес који подразумева пребацивање криптовалута на крипто новчаник који је само и искључиво под контролом полиције и тужилаштва. У зависности од врсте новчаника и околности под којим је пронађен одузимамо на следећи начин:

- **Софтверски новчаници и новчаници за паметне телефоне:** уколико приватни кључеви могу да се извуку из крипто новчаника, убацивањем у софтверски (мобилни) новчаник и пребацивањем на претходно припремљен папирни, хардверски или софтверски новчаник чији су приватни кључеви под контролом полиције и тужилаштва. Уколико је сама апликација откључана могуће је и директно пребацивање на претходно припремљен крипто новчаник.
- **Веб новчаници:** Уколико се има приступ веб платформи, могуће је директно пребацивање крипта или скидање приватних кључева, конвертовање у софтверски (мобилни) новчаник и пребацивање на претходно припремљен папирни, хардверски или софтверски новчаник чији су приватни кључеви под контролом полиције и тужилаштва.
- **Папирни новчаници:** Уколико се пронађе папирни новчаник пребацивање криптовалута се врши класичним убацивањем у софтверски новчаник који је под контролом полиције и тужилаштва (тзв. „сваповање" једног новчаника у други).
- **Детерминистички новчаници:** Уколико се пронађе СИД фраза иста се убацује у софтверски новчаник и изврши се пребацивање у одговарајући, претходно припремљен, софтверски или хардверски новчаник чији приватни кључеви су под контролом полиције и тужилаштва. Овде треба обратити пажњу на могућност постојања додатне речи, јер уколико постоји она мења читаву конфигурацију новчаника.
- **Хардверски новчаници:** Уколико се пронађе пин код, пребацивање крипта се врши у одговарајући, претходно припремљен, софтверски или хардверски новчаник чији приватни кључеви су под контролом полиције и тужилаштва. Уколико се пронађе СИД фраза онда се поступа као са детерминистичким новчаницима.

Након иницирања пребацивања криптовалута у новчаник који је под контролом полиције и тужилаштва обавезно проверити да ли је трансакција прошла (сматра се да је прошла ако је потврђена од најмање 3 блока на блокчејну).

8. Планирање привременог одузимања криптовалута

Приликом планирања привременог одузимања криптовалута, када се претпоставља да ће се претресањем стана и других просторија пронаћи крипто новчаници, важно је сачинити прави план који представља основну тактичку претпоставку сваке мере и радње које се предузимају. План обухвата планирање активности које претходе самом акту одузимања, активности приликом самог одузимања и након истог.

Код планирања радње самог одузимања и пратећих активности неопходно је планирати начине и методе лоцирања приватних кључева и/или датотеке дигиталних новчаника, а потом начин и методе на који ће се они убацити на новчаник под контролом полиције и тужилаштва. Сходно наведеном, потребно је припремити новчаник који је под контролом полиције и тужилаштва, а поступак припреме папирног новчаника дат је као прилог овом приручнику.

Након самог одузимања, неопходно је планирати начине и методе потврђивања трансакције и само извештавање пре, у току и након самог одузимања.

АНЕКС

9. Анекс

Прављење новчаника за одузимање криптовалута

Приликом одузимања криптовалута (нпр. биткоина) потребно је да средства са новчаника осумњиченог пребацимо на раније припремљени новчаник (најбоље папирни). Описаћемо поступак најбоље праксе прављења новчаника за одузимање биткоина (слично се може применити и за остале криптовалуте). Резултат ће бити папирни новчаник који ће имати јавну и једну приватну адресу. Овакав новчаник имаће снагу новца у готовини и исти ће бити „хладни новчаник“ без приступа интернету.

За прављење папирног новчаника за одузимање криптовалута потребан је:

1. Рачунар са могућношћу повезивања на интернет;
2. Бутабилни Убунту лајв оперативни систем који се може преузети са линка: https://rb.gy/awon7a или свеже инсталиран ОС који никада није нити ће бити употребљен на интернету;
3. Форматиран УСБ меморијски уређај;
4. Штампач повезан локално (каблом на рачунар); и
5. Провидна најлон фолија за паковање новчаника.

Поступак прављења папирног новчаника за одузимање биткоина

Поступак обухвата више фаза:

1 корак:

Обезбедите да рачунар којим приступате интернету има последња ажурирања система и активну антивирус заштиту.

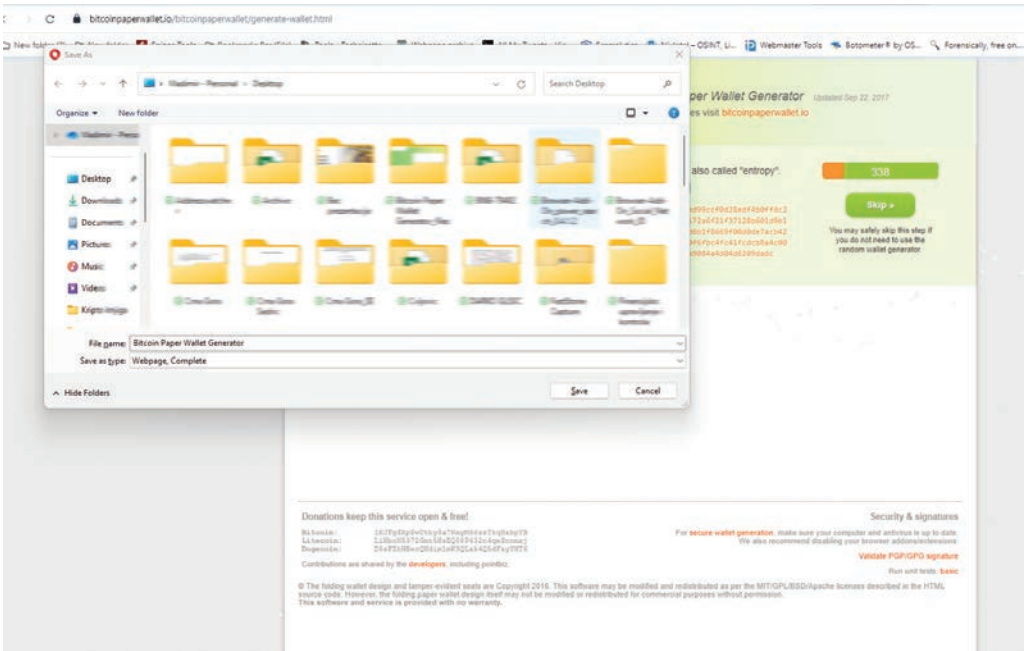
2 корак (слика 21):

- Идите на вебсајт https://rb.gy/jp39rm.
- Проверите да ли је криптована конекција (https://).
- Одаберите опцију „Create New Bitcoin Wallet“.

Слика 21

3 корак (слика 22):

- Притисните на тастатури контрол и тастер `c` у исто време („control +s“).



Слика 22

4 корак:

Сачувајте офлајн страницу под називом „Bitcoin Paper Wallet Generator“ на УСБ меморији.

5 корак:

- Покрените претходно скинут Убунту лајв оперативни систем или други ОС који ће служити само за израду папирних новчаника и који није нити ће бити конектован на интернет.
- Проверите да нема интернет преко жичне или бежичне конекције.
- Проверите да ли рачунар може да одштампа (има повезан штампач за директну штампу).

6 корак:

- Убаците УСБ меморију, покрените претходно сачувану офлајн страницу (фајл) под називом „Bitcoin Paper Wallet Generator“ и пратите упутства за прављење новчаника (слика 23).

Слика 23

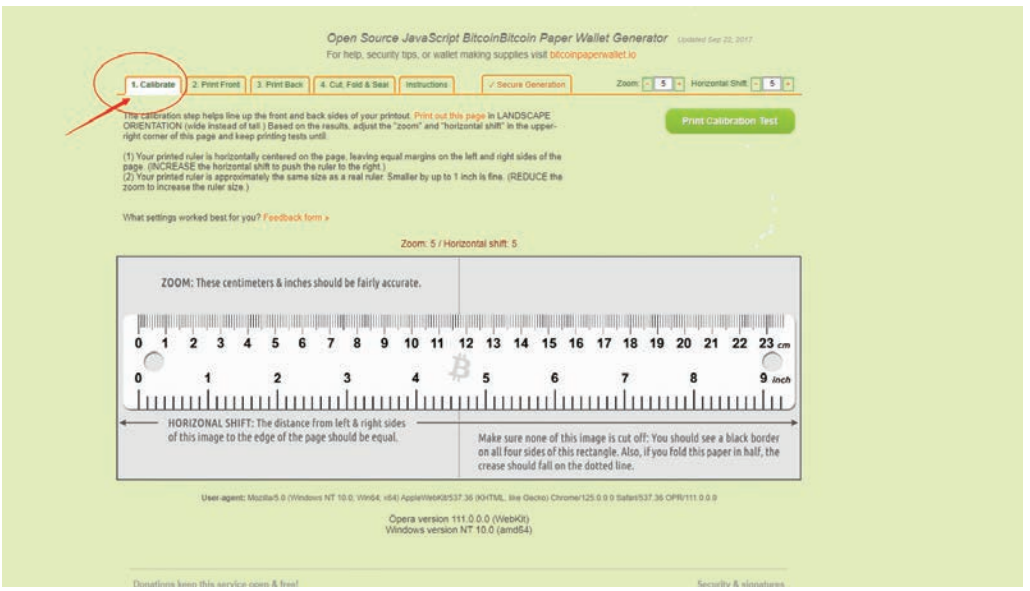
7 корак:

- Померањем миша прогрес бар ће доћи до краја и формирати биткоин новчаник (јавну и приватну биткоин адресу – слика 24).

Слика 24

8 корак:

- Идите на калибрацију папира и подесите новчаник за штампање (слика 25).

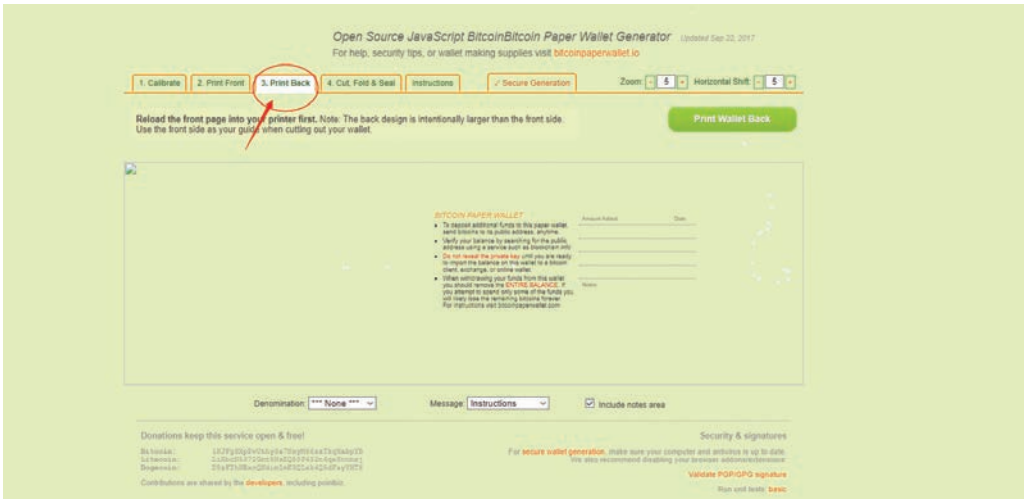


Слика 25

9 корак (слике 26 и 27):

- Одштампајте предњи и задњи део новчаника.

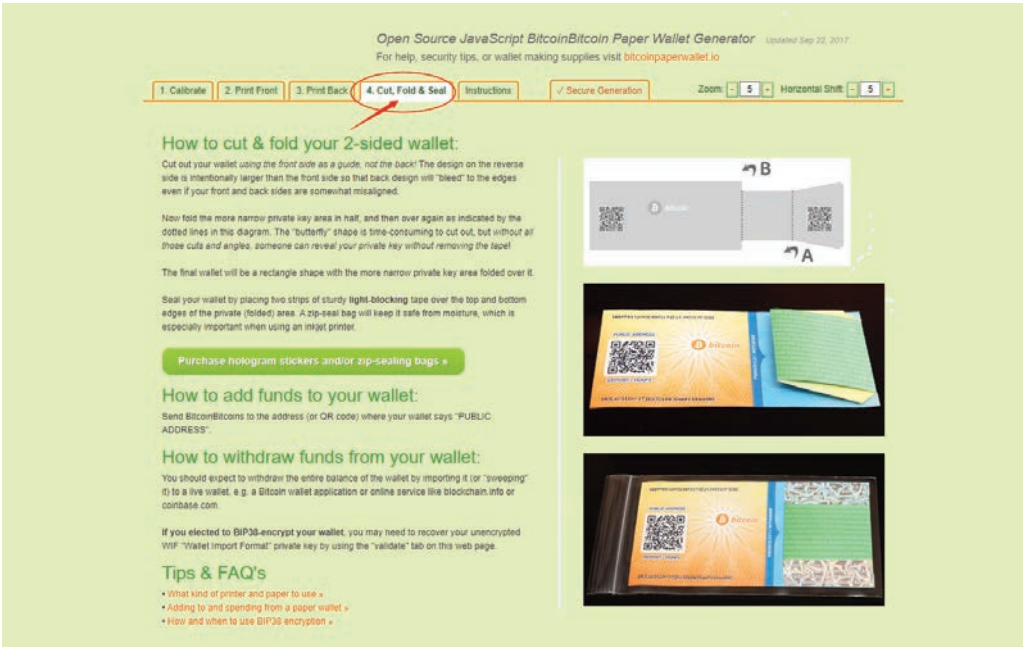
Слика 26



Слика 27

10 корак (слика 28):

- Пресавијте новчаник по инструкцијама.
- Ставите га у провидну најлон фолију тако да се види јавна адреса, али не и приватна.



Слика 28

11 корак:

Приликом одузимања на превојима отвора кесице потписаће се лице од којег се одузимају биткоини, као што је приказано на илустрацијама у наставку (слике 29 и 30).

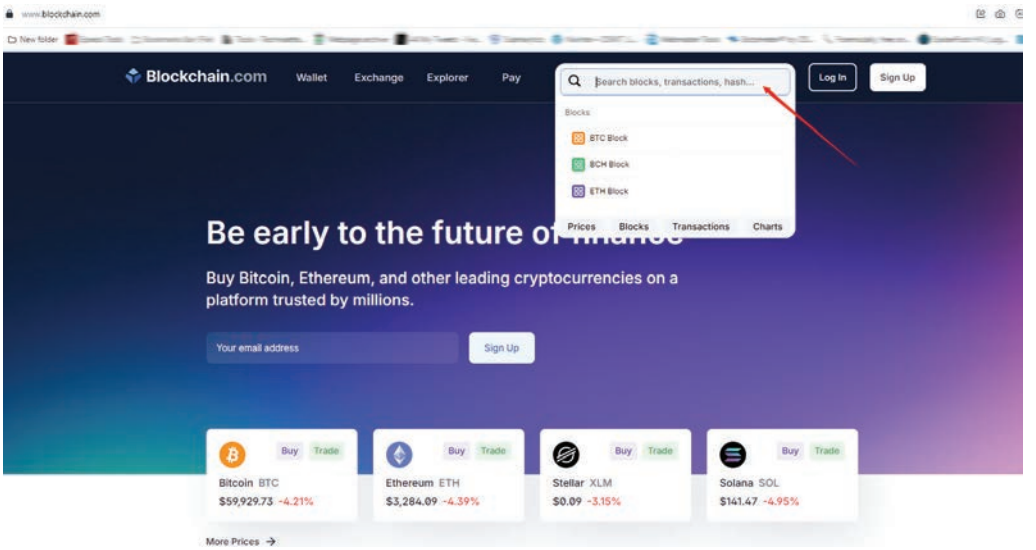
Слика 30

12 корак:

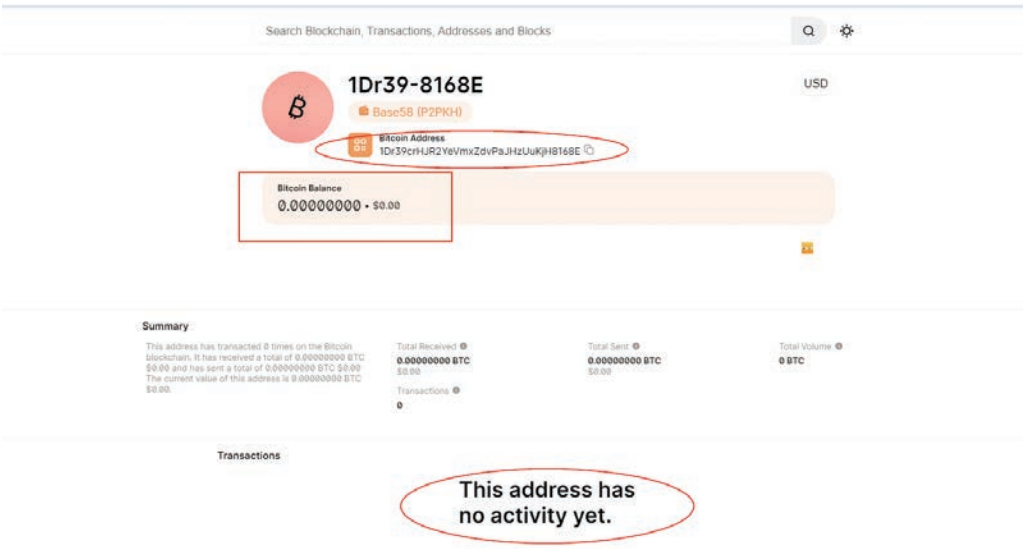
- Угасити рачунар који је служио за израду папирног новчаника.

13 корак:

- На рачунару са интернет конекцијом потврдити да је адреса направљена на тај начин што ћете на интернет сајту www.blockchain.info убацити јавну биткоин адресу у поље за претрагу (слике 31 и 32).



Слика 31



Слика 32

Биткоин новчаник је спреман за одузимање средстава.