

Форензика социјалних мрежа

Ана Миленковић 1524

Универзитет у Нишу

Електронски факултет Ниш

Садржај

1. Увод.....	3
2.1 Закон.....	4
2.2 Законска ограничења.....	5
2.3 Техничка ограничења	7
2.4 Питања етике	8
2.4.1 Етика форензике социјалних мрежа	10
3. Процес истраге.....	13
4. Постојећи алати	16
4.1 EnCase Forensics	16
4.2 CacheBack 3	18
4.3 Internet Evidence Finder	19
4.4 Social Network Harvester	21
4.5 WebPreserver	23
4.6 Pipl Search.....	25
4.7 TinEye.....	26
4.8 TweetBeaver	28
Литература.....	29

1.Увод

Употреба социјалних мрежа се знатно повећала у протеклих неколико година. Истраживање обављено од стране фирме “Керіос” октобра 2022. године показало је да 4,74 милијарди људи користи друштвене мреже. То одговара 59,3% људске популације. Време које људи проводе на друштвеним мрежама такође достиже рекордне бројеве: свет потроши 10 милијарди сати на социјалним платформама сваког дана, што је скоро еквивалентно 1.2 милиона година. Неке од водећих и најпосећенијих друштвених мрежа су:

1. Facebook са **2.934 милијарде** месечних активних корисника
2. YouTube, са потенцијалним рекламним покрићем од **2.515 милијарде**
3. WhatsApp има најмање **2 милијарде** месечних активних корисника
4. Instagram са рекламним покрићем од **1.386 милијарде**
5. WeChat (inc. Weixin 微信) има **1.299 милијарде** месечних корисника
6. TikTok има **1 милијарду** месечних активних корисника

Израз “друштвене мреже” описује све комуникационе канале који се користе за интеракције у оквиру заједнице и дељење садржаја. Људи су активно укључени у дељење својих свакодневних активности на социјалним мрежама, као и у размени идеја и искустава. Ове мреже су иницијално и биле коришћене за то: промоцију пријатељстава. Међутим, како су умрежени рачунари и уређаји почели да се шире на начине који нису претходно очекивани, тако је и порасла учесталост криминалаца који користе друштвене мреже. Ово указује да мреже дају оквир за злоупотребу легитимног коришћења ових сервиса.

Као такве, постале су ново поље у области дигиталне форензике. Обзиром на њихов брзи раст и популарност, подаци које друштвене мреже генеришу такође расте, и то експоненцијално. Ти подаци се могу употребити како у добре, тако и у лоше сврхе. Сајбер-криминалци често користе погодности социјалних мрежа за ширење вируса, прибављање поверљивих информација, а мотиви, иако их има доста, углавном се свode на финансијску добит. Најчешћи проблеми нанети на овај начин су оштећена репутација, новчани губитци, као и угрожена приватност, интегритет, ширење информација, доступност података. Друштвене мреже се такође могу искористити и за утврђивање штетних планова и шема. Криминално понашање и докази о злочинима се могу наћи на друштвеним мрежама. Ови подаци се могу искористити за утврђивање намере када се користе као доказ у криминалним случајевима.

2.Закон, ограничења и етика

2.1 Закон

Агенције за провођење закона желе да податке прикупљене са друштвених мрежа искористе у сврхе сигурности и безбедности. На тај начин, друштвене мреже се могу користити као извор надгледања. Уз помоћ алата дигиталне форензике за преглед информација преузетих са друштвених мрежа, могу се донети закључци за неки конкретан догађај. Када је у питању анализа криминалних активности на друштвеним мрежама, једно од битнијих проблема је идентификација најугрожавнијих профила, такозваних “кључних играча”. Агенције за провођење закона су заинтересоване да нађу одговоре на 6 значајних питања: ко, шта, када, где, како, зашто.

Ово су традиционална питања приликом криминалне истраге и дигитална форензика у области друштвених мрежа овде може да помогне. Докази прикупљени са друштвених мрежа доносе прегршт информација о профилима потенцијалних осумњичених или о профилима жртава које се могу набавити у реалном времену. Контакти, поруке, геолокацијски подаци, слике, и генерално њихова активност се закону достављају у хронолошком реду. Метаподаци и мрежни подаци имају адекватан потенцијал да помогну у криминалним истраживањима и да аутентификују доказе са онлајн социјалних мрежа.

У садашњости, у великом броју криминалних случајева се легално захтева да се набаве и истраже дигитални уређаји жртава и осумњичених. Подаци са ових уређаја помажу у проналажењу трагова злочина или историје дигиталне активности од стране корисника. Неки примери улога доказа са друштвених мрежа:

- Документована комуникација се користи за приступ и увид у ментално стање особе
- Дневна онлајн активност се користи као доказ о присуству или одсуству особе у одређено време или на одређеном месту
- Фотографије стила живота приказују навике трошења новца, приходе или физичко здравље
- Фотографије такође дају доказ о томе где и са ким нека особа проводи време
- Онлајн понашање оставља трагове сајбернасиља, сајберкриминала, узнемиравања и слично
- Онлајн профили дају доказе о крађи идентитета
- Профили на друштвеним мрежама се такође користе за позадинске провере потенцијалних осумњичених или жртава

2.2 Законска ограничења

Напредак у дигиталној комуникацији омогућује разноврсне позитивне прилике за појединце. На жалост, такође омогућава и безбројне прилике криминалцима за почињавање злочина. Они веома лако приступају подацима њихових жртава путем друштвених мрежа. Коришћење друштвених мрежа у виду доказа на суду је све чешће.

Велики број криминалних случајева сада се рутински обрађују и бране кроз доказе добијене онлајн. Тужилаштво, одбрана и адвокати подједнако користе информације са социјалних мрежа у правним поступцима.

Ипак, адвокати одбране имају већи број препрека, као на пример тражење налога и судског позива компанијама које воде друштвене мреже ради приступа заштићеним подацима.

Још једно од законских ограничења са којима је могуће сусрести се јесте аутентикација електронских уређаја, поготову социјалних мрежа. Било ко може направити лажан профил и претварати се да је неко други и деловати под туђим именом. Такође је могуће манипулисати садржајем туђих података, уколико прибаве корисничко име и шифру. Постоје два главна критеријума прихватљивости података са социјалних мрежа као доказе. Прво, потребно је аутентификовати ауторство доказа. Друго, од великог значаја је обезбедити доказе о интегритету матерјала који се доноси на суд. Део аутентикације се такође бави проблемима чувања и права поседа доказа. Суд често одбацује доказе у облику једноставне штампе или усликаних екрана (screenshots) јер их је лако изменити. Традиционални методи екстракције података и њиховог чувања нису погодни за форензику социјалних мрежа. Ова ограничења аутентикације захтевају напредне алате, који су специјализовани за сакупљање, претрагу, индексирање, чување и аутентикацију доказа са социјалних мрежа.

У криминалним случајевима, агенције за провођење закона набављају податке о осумњиченима од провајдера друштвених мрежа путем налога за претрагу и владиних судских позива. Од интернет провајдера се такође могу набавити неки корисни подаци, као што су информације о претплати, датуми конектовања, IP адресе и слично. Међутим, компаније друштвених мрежа нису спремне да уступе на рачун приватности својих корисника тако што би њихове информације доставиле закону. Проблем се овде додатно компликује са појавом глобалних сукоба надлежности, када се криминална активност јавља у оквиру једне надлежности, а компанија друштвене мреже у другој. Због различитих закона, правне агенције се суочавају са проблемима надлежности за очување и приступ подацима које држе компаније у другим земљама. Неке легалне процедуре захтевају да истражитељи раде са компанијама које хостују податке и да осигурају да се процес колекције обавља по свим уставним правима и захтевима, као и да прате услове коришћења. Ова колаборација је непрактична уколико су надлежности

различите. Због тога је потребно креирати конзистентан, интернационални правни оквир, који би омогућио глобални приступ доказима са социјалних мрежа, независно од надлежности.

2.3 Техничка ограничења

Истраживања су показала да адвокати и истражиоци наилазе на проблеме када обрађују и раде са подацима из дигиталне форензике. Главни проблем је што у току једне истраге социјалних мрежа, неки елементи података се сматрају ван контекста и не узимају се у обзир. Надаље, компоненте података који се сматрају важним се чувају одвојено. Сви фрагментирани и неструктурирани подаци, иако можда делује од мањег значаја, би били веома корисни уколико би имали кохерентни приказ и ако би били хронолошки поређани. Поред тога, обзиром да се подаци чувају на различитим местима, анализа података је ограничена на претрагу по кључним речима, која је неадекватна за форензичку истрагу.

Други изазов је у области развоја софтвера и алата дигиталне форензике социјалних мрежа и односи се на хетерогеност различитих платформи. Наиме, различите друштвене мреже на различите начине чувају податке и њихова обрада није униформна. Решење за ово било би хомогенизовати податке. Оквир усмерен ка безбедности би допустио и чување, као и претрагу и формирање корелација, и то све уз аутоматизоване алате за анализу података и визуализацију.

Предлаже се формирање новог процеса анализе података са друштвених мрежа који би обухватао три корака: праћење, припрему, и анализу података са више медијских извора. Праћење би се обављало путем АПИ-ја специфичних за конкретну друштвену мрежу (Facebook, Twitter, LinkedIn имају своје посебне АПИ-је). Након тога уследила би фаза припреме која уводи нову онтологију која би осликавала данашње стање социјалних мрежа. Да би се лакше увео овај цео процес, креирали би се посебни додаци (plugins) за неке сајтове друштвених мрежа. Сваки додатак би узимао као улаз податке специфичне за ту друштвену мрежу. Нова онтологија би детаљно описивала како се ти подаци чувају у граф бази. Означавала би лабеле чворова, њихове особине и њихове везе које би описивале односе између чворова. Подаци би били обрађени на начин који одговара сваком сајту понаособ и прибављали би се само они који су заједнички за новоуведену онтологију, и мапирани би се по њој. Као такви, уписују се у граф базу. Да би се интеракције између профила детаљно анализирале, постојао би

механизам закључивања који би креирао директну везу између профила који комуницирају, уколико та веза већ није експлицитно дефинисана.

У фази анализе, дефинишу се упити који прибављају податке и везе између ентитета и профила. Ови упити би могли узимати аргументе крајњих корисника као улаз. Може бити и предефинисаних упита који би давали увид у структуру мреже и октирвали најбитније профиле које правне агенције на даље могу обрађивати. Аутоматска хомогенизација података, чување и анализа би у великој мери смањила трошкове истраге.

2.4 Питања етике

У данашње време, директно или индиректно, пораст злочина повезаних са рачунарима и дигиталним уређајима, као и реалност ове појаве, постали су велики повод за бригу у друштву. Овај феномен је утицао на нормалан процес истраге и нови израз “Дигитална Форензика” је почео да носи већу тежину на суду. Дигитална форензика је такође постала и алат у превенцији злочина, али и један од пожељнијих видова доказа на суду.

Зато је веома битно да у току истраге злочина, постоји експерт дигиталне форензике који презентује научне доказе, пратећи систематску процедуру која је правно доказана и научно утемељена. Упркос свему овоме, данас постоји јако мало етичких стандарда за експерте у области дигиталне форензике. Иако постоје закони, ти закони се не баве етичким питањима, нити дефинишу етичке смернице. Проблем је тај, што се постојећи закони баве само правним питањима, док су моралне дилеме запостављене у закону.

Шта је заправо “етичко питање”? То означава нешто што је морално исправно, часно. Идеја етике је била наглашавана у индустрији рачунарства и открића етичких питања у рачунарству су постала честа. Док се те идеје етике баве индивидуалним корисницима рачунара, идеја етике у дигиталној форензици је усмерена ка људима који истражују те кориснике, да би постигли резултате у истрази. Због природе посла, ови експерти се носе са много неморалних акција крајњих корисника, а да притом

задрже највиши стандард транспарентности и професионализма за време трајања истраге.

Извештај о истрази који долази од експерта дигиталне форензике је постао од круцијалног значаја и најтраженији извор информација у правним поступцима. Како је у питању веома осетљив материјал, експерти дигиталне форензике могу понекад да почине неке неморалне акције, чак и илегалне активности попут кривоклетства, а све у корист својих клијената. Етика у дигиталној форензици није само битна због проналаска доказа сакривених у рачунарима, мрежама, дигиталним медијумима, већ има и одговорност према јавности да обезбеди и подигне ниво свести о дигиталној форензици у области осигурања информација.

Постоји много етичких дилема у истрази коју обавља дигитална форензика. То је због тога што се закон спорије мења од технологије, и нашег виђења неких значења и промена са временом. На пример, значење “бити за осуду” се у једној генерацији може разликовати од онога што је за осуду у следећих пар година. Због природе посла, постоји знатан број етичких дилема у овом пољу. Неке од чешћих етичких питања укључују: интегритет, комплетност истраге, потенцијал за корупцију или загађеност дигиталних података, игнорисање или промену доказа, непраћење стандардне процедуре, мито, као и емоционална укљученост у криминалне случајеве. Када дође до ситуација попут “истина против оданости”, “индивидуалност против заједнице”, “кратак рок против дугог”, “правда против милости”, експерти дигиталне форензике ће бити суочени са етичким дилемама. Било би потребно дефинисати одговарајући интернационални етички стандард за истраге у дигиталној форензици, као и за интеракцију са релевантним областима закона. Ово би у великој мери допринело нашем друштву при разјашњавању суштинске истине, што може умањити такозвана “сива поља” у дигиталној форензици.

2.4.1 Етика форензике социјалних мрежа

Када је у питању конкретно етика у форензици социјалних мрежа, оне су у огромној мери утицале на дигиталну форензику. Социјалне мреже су у потпуности измениле начин на који људи комуницирају. Сврха друштвених мрежа је добровољна размена информација у комуникацији, и овакве информације понекад могу бити изузетно приватне и могу се видети само од стране одређене групе људи или пријатеља. Такви постови и историја порука садржи корисне информације у распону од правних истрага, открића и парница. Активности на друштвеним мрежама се чувају онлајн и садрже лична понашања, локацију и остале приватне информације, које се могу открити у току дигиталне истраге. Ово може имати озбиљне последице, и зато одавде произлази велики број забрињавајућих етичких питања. Да би се обавила успешна истрага друштвених мрежа, постоје неки етички проблеми којима се треба посветити.

Једно од питања које прво падне на памет је приватност. Многе друштвене мреже допуштају, чак и захтевају од корисника да унесе своје личне податке, попут пуног имена, датума рођења, телефонског броја, кућне адресе приликом креирања профила. Иако корисници имају контролу над својим конекцијама и свој профил чине видљивим само одређеним људима, те информације се и даље могу прибавити и видети од стране експерата дигиталне форензике за време истраге. Тако се долази до питања: шта ако дође до открића поверљивих података, али који нису од значаја за криминални случај. На експертима је да такве приватне информације задрже за себе и да остану поверљиве информације, недоступне другима за увид.

Проблем поштења, искрености и интегритета података је још једно велико етичко питање у области дигиталне форензике. Признати грешку је део етичких принципа за форензичара. Ипак, људи углавном веома тешко прихватају и признају своје грешке, поготову ако себе сматрају за професионалца у својој струци. Како расте број корисника друштвених мрежа, тако расте и криминална активност, а сходно томе и дигитални форензичари морају научити нове алате и оформити нове истражне процесе како би истрага била коректна и тачна. Како је ово релативно нова грана у области форензике, јавља се проблем стандардизације, или њеног мањка. Понекад, форензичари раде под притиском и у кратким временским роковима се очекује да доставе резултате. То, заједно са жељом да задовоље своје клијенте, као и ради одржавања своје репутације, често форензичаре излаже стресу. То може довести до тога да недовољно детаљно прегледају доказе, или да предају извештај о истрази са недовољном анализом. Можда су им потребни додатни алати или апликације за прикупљање података са друштвених мрежа, обзиром да је ово нова и неразвијена грана форензике. Могуће је да немају довољан буџет за куповину неког алата специјализованог за форензику друштвених мрежа и уместо њега, користе општи алат за, на пример, форензику медијума за складиштење података. Тренутно нема много софтверских пакета који су специфично намењени и дизајнирани за истраге друштвених мрежа, па се онда поставља питање колико је фер користити податке који нису набављени на “исправан” начин. Колико су ти подаци заправо валидни? Ово може бити од пресудног значаја у криминалном случају у судници.

Дигитални форензичар треба да декларише своје квалификације и искуства у току информисања. Постоји много реалних случајева где су форензичари лажно представљали себе и своје умеће. На пример, 2008. године у Британији, експерт дигиталне форензике дао је лажну изјаву суду и добио суспензију у трајању од шест месеци. Поред тога, судија је изјавио да је његова каријера дигиталног форензичара завршена. Ово је послужило као одличан пример колико је професионална етика важна у овом послу. Због озбиљне природе посла, очекује се да истражитељи обезбеде прикладне квалификације и документа о припадности професионалној организацији. Како је ипак ово поље релативно ново, не тако велики број људи заиста и поседује потребне сертификате и квалификације.

Иако неке компаније обезбеђују тренинге и сертификоване курсеве за алате у области дигиталне форензике социјалних мрежа, јако је битно да се знање из ове области константно надограђује. Функционалности и могућности друштвених мрежа се веома брзо мењају. Уколико форензичари не раде на томе да буду ажурни и не прате брзе промене технологија, наћи ће се у ситуацији да њихове вештине и квалификације буду застареле и имаће потешкоћа у прикупљању и анализирању података и доказа који долазе из најновијих технологија. По том питању, од значаја је, и део професионалне етике за све дигиталне форензичаре да буду ажурни и да прате технолошке промене, да би знали на исправан начин да доказе представе на суду.

Поред етике која се односи конкретно на форензичаре и људе који прикупљају податке, не треба занемарити и етику оних који креирају алате који омогућавају екстракцију тих информација. Када развијају софтвер за истрагу података са друштвених мрежа, може се десити да занемаре неке етичке принципе, попут заштите приватности. Улога етике у развоју софтвера има повећани значај у новије време. Томсон и Шомолд су 2001. године изјавили “Разунарски софтвер лежи у срцу модерног процеса доношења одлука, укључујући чување података и њихову манипулацију, доступност података и алтернативне формулације и селекције”. Они су даље наглашавали да сва софтверска решења треба да буду прегледана и критикована у току самог развоја јер то може имати утицаја на људе и њихове културе. Јако је важно да креирани софтвер буде исправан, коректан, тачан, јер у супротном, штета коју лош софтвер потенцијално може нанети, не може се измерити.

3. Процес истраге

Процес истраге у области дигиталне форензике социјалних мрежа своди се на три главна корака, а то су:

1. Прикупљање и чување података
2. Анализа података
3. Презентација и визуелизација резултата

1. Прикупљање стабилних форензичких података је од круцијалног значаја. Подаци генерисани на друштвеним мрежама долазе у различитим форматима, али процес прикупљања у суштини остаје исти. Могући типови података који се сакупљају, као и њихове локације, су следећи:

- Интернет историја - истражити и сакупити историју са *web browser-a*; кориснички фолдери, локална подешавања, привремени интернет фајлови
- Web кеш - кеширани подаци са *web browser-a*; иста локација као и за историју
- Колачићи и сесија - информације о сесији и колачићи са *web browser-a*; налазе се у Firefox профилним фолдерима, привременим интернет фајловима, *pagefile.sys/ hiberfil.sys* фајловима, у неалоцираним кластерима, *places.sqlite* фајловима ако је у питању Firefox
- Фотографије - у корисничким фолдерима, локалним подешавањима, привременим интернет фајловима, неалоцираном простору
- Видео снимци - исте локације као и за фотографије
- Коментари и одговори - у кеш фајловима претраживача, корисничким фолдерима, неалоцираном простору, *pagefile.sys/ hiberfil.sys* фајловима
- Постови “на зиду” и статуси - прикуљани подаци укључују идентификатор корисника и име особе која поставља пост/статус, садржај, локацију; може се извући из привремених интернет фајлова, *pagefile.sys/ hiberfil.sys* фајлова, неалоцираних кластера

- Локација - у кешу претраживача, неалоцираном простору, pagefile.sys/ hiberfil.sys фајловима
- Чет - послате и примљене поруке, идентификатор корисника који је слао, као и корисника који је примао поруке, време када су поруке послате; ови подаци налазе се у привременим интернет фајловима, празном датотечном простору, неалоцираним кластерима, pagefile.sys/ hiberfil.sys фајловима
- Мејлови - примљени или послати мејлови преко друштвене мреже, а укључује и тему мејла, примаоца, време последњег ажурирања, идентификатор и име корисника, додатне фајлове, линкове, слике, као и сам садржај мејла; подаци се проналазе у привременим интернет фајловима, pagefile.sys/ hiberfil.sys фајловима, неалоцираним кластерима, профилним подацима са Outlook-а

Иако су подаци прикуљени са различитих друштвених мрежа, кораци за њихово прикуљање су исти. Тачност извора се такође мора утврдити, а затим се подаци чувају на форензички безбедан начин, бивају документовани, и потом их треба оценити као значајне и релевантне за истрагу. Подаци са социјалних мрежа, као и било који подаци са интернета, се могу наћи на бројним локацијама. Углавном се чувају на серверима самих социјалних мрежа, где су подаци креирани и постављени. Још један чест извор ових података је рачунар овлашћен за приступ друштвеним мрежама.

Пошто су подаци са социјалних мрежа динамички, они могу бити измењени или обрисани. Да би се проверио интегритет прикупљених података, користи се хеширање. Иницијално се прикупе сви доступни подаци, који се потом хеширају и хеширана вредност се чува. Ако у било ком тренутку, након новог хеширања, хеш вредности буду различите, значи да је дошло до промена и да је угрожен интегритет података.

2. Анализа

Први корак у анализи података је провера валидности и тачности података. Након што су подаци накупљени, спроводи се аналитичка истраживања која испитују значења података прикуљених са друштвених мрежа. Најчешћи подаци који се добијају анализом су : ко је поставио садржај, када је поставио, место одакле је садржај креиран, коме је садржај упућен (на пример, ако је у питању размена порука, чет).

Следећи корак у анализи било би поређење података и уочавање веза и релација међу њима. Подаци сами по себи ретко када могу дати довољно потребних информација. Закључци који потичу из узајамних веза међу подацима су ти који дају значење претходно прикупљеним подацима. На пример, уколико се истражује учесталост порука које одређени корисник шаље у току дана, могу се пребројати све поруке које се шаљу сваког дана и груписати се по данима у недељи. Даљом визуализацијом и презентацијом података, могу се извући одређени закључци који би били корисни у истрази. Што доводи то последњег, трећег корака у процесу истраге а то је презентација и визуелизација резултата.

3. Презентација и визуелизација резултата

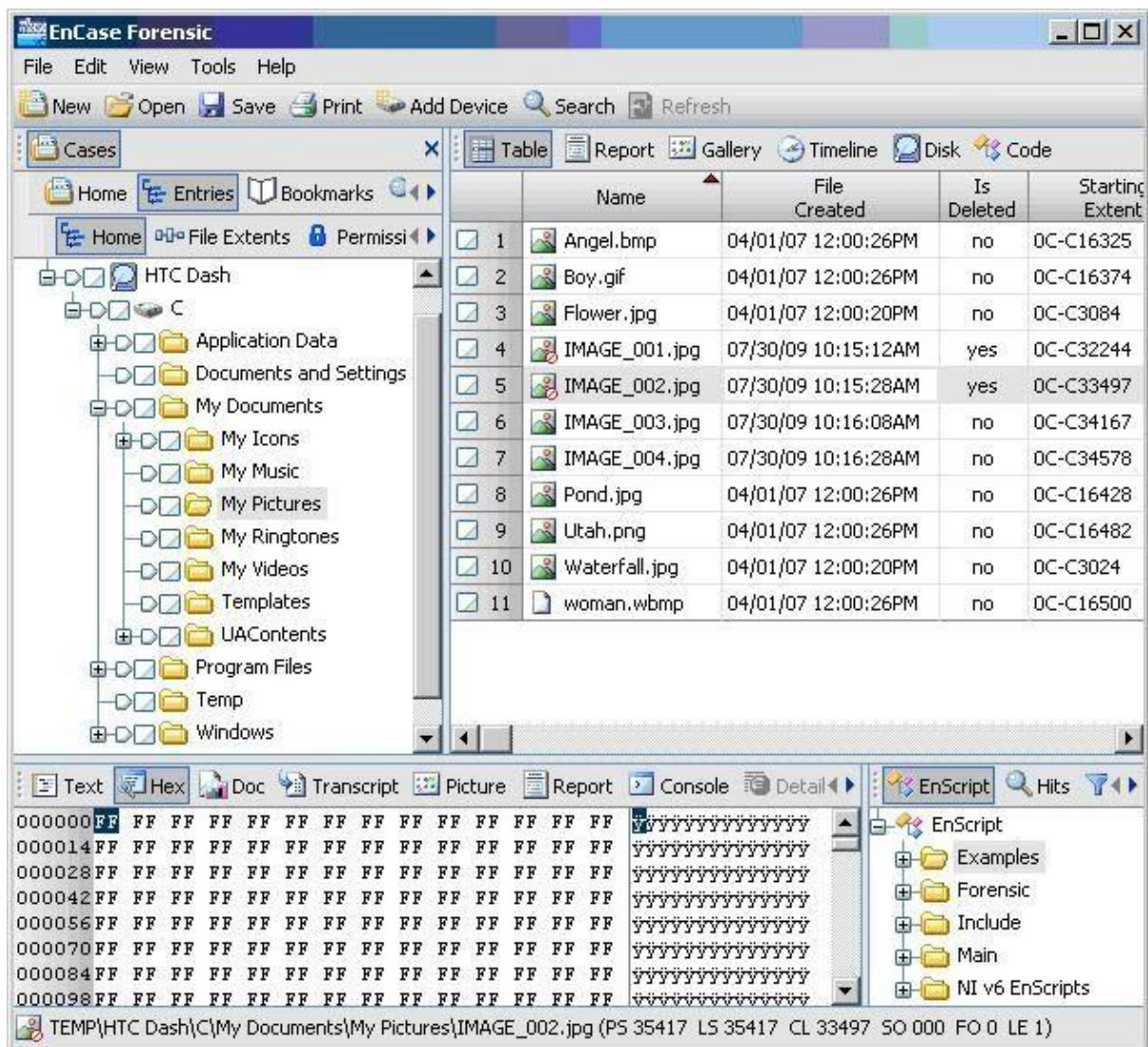
На самом крају истраге, претходно прикупљени и анализирани подаци се приказују на начин разумљив човеку. Подаци се групишу по потребама и условима истраге, тако да приказују релевантне закључке и доказе. Подаци могу бити приказани у различитим облицима, на пример путем графова, графикона, стабала, пита-графика, календара, линијских графика, табеларно, путем слајдова. Могу се посматрати у различитим аспектима, на пример у временском аспект, локацијском аспект, фреквентном аспект. Закључци који произлазе из ових репрезентација прикупљених података могу знатно утицати на истрагу. На пример, ако се уочи да је на дан злочина осумњичени послао јако велики број претећих порука жртви, то може бити додатни доказ о емотивном и менталном стању осумњиченог и припомоћи при доношењу коначне пресуде.

4. Постојећи алати

Упркос чињеници да је ова област релативно нова, на тржишту постоје алати и апликације за прикупљање података потребних у једној истрази. Неки од таквих алата су: *EnCase Forensics*, *CacheBack 3*, *Internet Evidence Finder*, *Social Network Harvester*, *Web Preserver*, *Pipl Search*, *TinEye*, *TweetBeaver*. Неки од ових алата су општег карактера и могу се користити у разне сврхе, док су неки уско специјализовани само за једну категорију (на пример, само за одређену друштвену мрежу, или само за неки тип података).

4.1 EnCase Forensics

EnCase Forensics апликација је комерцијални алат и једна од најпопуларнијих апликација у дигиталној форензици. Проналази дигиталне доказе без обзира на то где се крију и помаже органима за спровођење закона и владиним организацијама у смањењу засталих случајева, бржем затварању случајева и побољшава јавну безбедност. За више од 20 година, истражитељи, адвокати и судије широм света се ослањају на EnCase као пионира у софтверу за дигиталну форензику да достави поуздане резултате. Овај алат је решење индустријског стандарда за форензичаре који желе да спроведу ефикасно, форензички исправно сакупљање података користећи поновљиви и безбедан процес. Апликација је доказано моћна и допушта истражитељима да прибаве податке из широког спектра уређаја, као и да открију потенцијалне доказе на нивоу диска са форензичком анализом. Омогућава и креирање обимних извештаја на основу проналазака, и то све док чува интегритет самих података и доказа.



Слика 4.1.1 Кориснички интерфејс апликације EnCase

EnCase Forensics се може искористити за тражење доказа на различитим оперативним системима, као што су Windows, Linux, Mac OS. Може процесовати доказе до 75% брже од сличних алата, доказано тестовима уз коришћење стварних података. Фајл формати доказа, као и интегритет дигиталних доказа је прихваћен и показао се као поуздан стандард на суду свугде у свету. Моћ овог алата се може додатно проширити са комплетним API-јем који даје прилику да се аутоматизују процеси и побољша ефикасност анализа. Између осталог, EnCase има следеће могућности:

- Прибављање података из скоро било којих извора - то укључује RAM меморију, слике, мејлове, интернет артефакте, интернет историју и кеш, реконструкцију HTML страница, чет сесије, компресоване фајлове, бекап фајлове
- Прибављање како локалних, тако и података на облаку са Facebook-a, Twitter-a, Insatgram-a, Google-a, iCloud-a, WhatsApp-a и LinkedIn-a
- Прибављање података на форензички безбедан начин - креирање потпуно истог бинарног дупликата оригиналног медијума
- Подршка за вештачку интелигенцију и машинско учење - аутоматски препознаје садржај и фотографије које садрже неки одређени интерес, као што су, на пример, психоактивне супстанце, оружја, експлицинти садржај
- Оптичко препознавање карактера - могућност екстракције текстуалних доказа из PDF фајлова, слика и скенираних докумената који се могу признати као критични докази
- Подршка за AFF4 доказе - фајл формат за доказе је отвореног стандарда и може у себи “прогутати” друге фајл формате како би омогућио шире и разумљивије закључивање
- Напредна анализа прибављених података
- Даје програмерске могућности форензичарима и истраживачима, и на тај начин им допушта да креирају персоналне програме који им помажу да аутоматизују задатке који би иначе одузимали много времена, уколико би се радили ручно
- Доставља аутоматизовани алат за креирање извештаја

4.2 CacheBack 3

CacheBack је алат дигиталне форензике који служи да поново изгради кеширане интернет странице и да претражи интернет историју и активности на сајтовима социјалних мрежа. Подржава све познатије и популарније интернет претраживаче (Edge, Firefox, Google Chrome, Opera, Safari). Кеширане странице и слике се могу прегледати у једној уједињеној галерији слика, тако да је лако уочити артефакте који су од интереса.

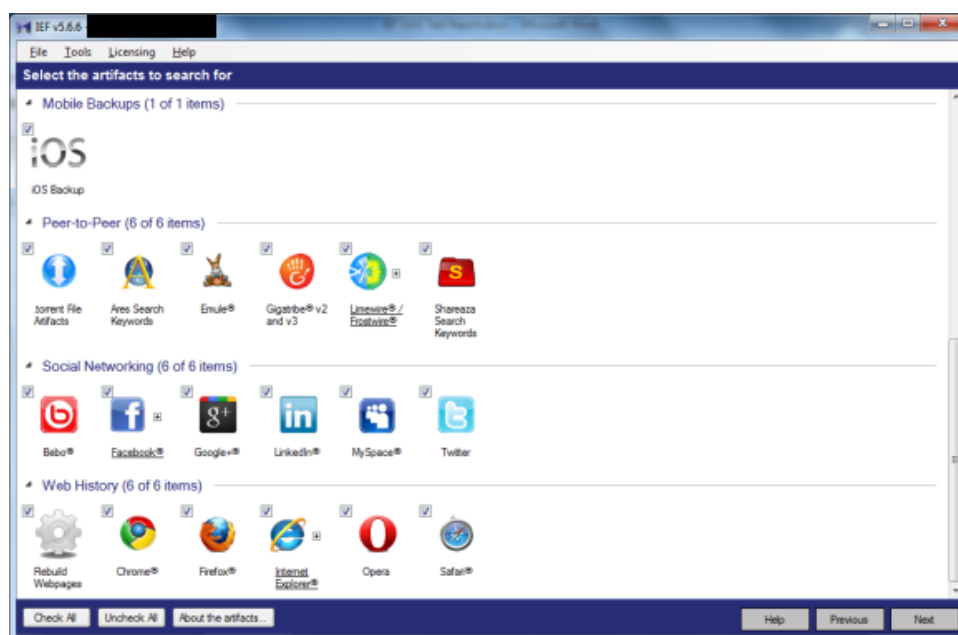
Слике и снимци се могу импортовати директно са хард диска коришћењем алата за мајновање података. Омогућава категоризацију, груписање, обележавање и укључивање/искључивање било које количине слика или филмова из случаја. Може елиминисати стотине и хиљаде слика из анализе, за само пар секунди, захваљујући филтрирајућој технологији и диференцијалном алгоритму за однос ширине и висине фотографија. На слици 4.2.1 се може видети како изгледа кориснички интерфејс апликације CacheBack.



Слика 4.2.1 Кориснички интерфејс апликације CacheBack

4.3 Internet Evidence Finder

Internet Evidence Finder је апликација која може да претражује хард дискове или фајлове за артефакте генерисане у онлајн окружењима и специфично је дизајниран истражитеље у области дигиталне форензике. Дизајн софтвера је интуитиван за коришћење, и захтева минималан тренинг особља. Претражени медијуми укључују избрани драјв, фолдере (и опционо подфолдере), фајлове (*memory dumps*, *pagefile.sys*, *hiberfi.sys*), а резултати се враћају у виду Интернет Артефакта. Фолдер за случај бива креиран и у себи садржи артефакте, а резултати се могу видети кроз “Report Viewer”. Овде је могуће креирати нове извештаје и експортирати податке у различите формате.



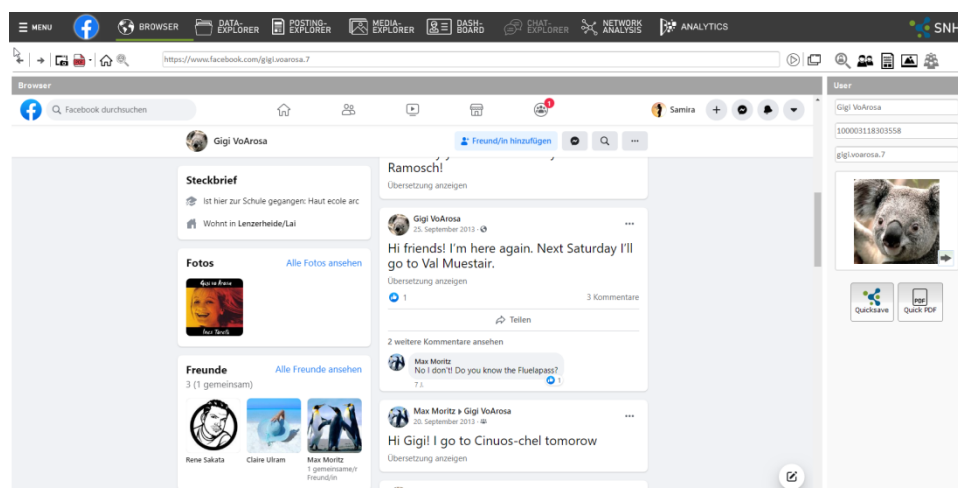
Слика 4.3.1 Интерфејс *Internet Evidence Finder-a*

Од акција које може извршити, постоје и неке које се односе конкретно на социјалне мреже:

- Претрага *Facebook* чета уживо - прикупља поруке послате и примљене коришћењем *Facebook live chat-a*; ове информације укључују идентификатор профила који је слао/примао поруке, имена пошиљаоца и примаоца, као и време када је порука послата
- Конвертовање *Facebook Unicode* текста
- Претрагу *Windows Live Messenger-a*
- Прибављање фрагмената *Facebook* страница - може прибавити странице везане за *Facebook*, укључујући Inbox страницу, фото галерију, групе, и слично. Већина прибављених ствару ће бити фрагментисана и неће формирати читаву страницу, али у току су покушаји да се прибави цела страница.
- Постоји и преносива верзија овог алата која се може покренути на *live* системима
- Парсирање лог фајлова који потичу са *Yahoo Messenger-a*, који се могу парсирати без потребе уноса корисничког назива
- Валидација *Yahoo Messenger* лога чета

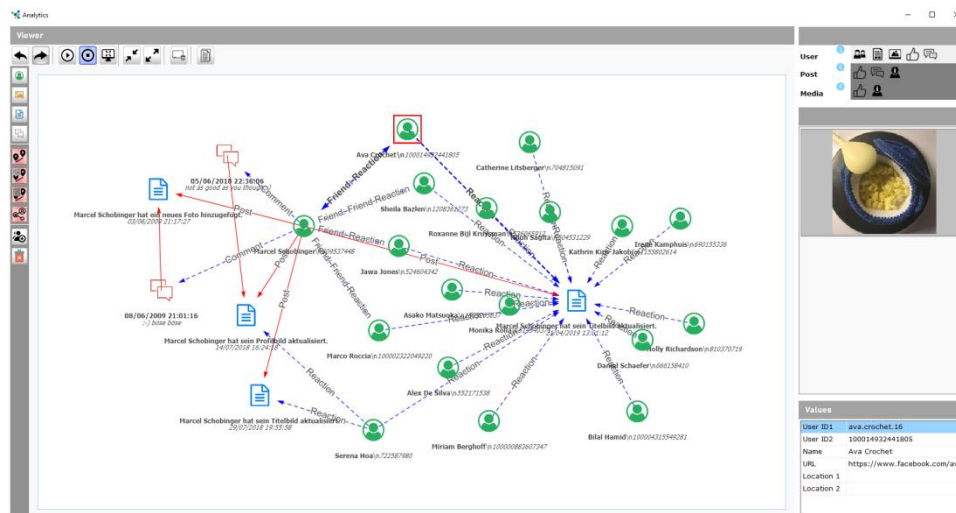
4.4 Social Network Harvester

Открити како су људи повезани је од виталног значаја за већину форензичких истрага, и социјалне мреже обезбеђују истражитељима нове могућности и изазове у праћењу социјалних конекција. Специјализовани софтверски алат *Social Network Harvester* (скраћено SNH) који је креирала немачка компанија “Freezingdata” помаже форензичким истражитељима склопе информације дистрибуиране преко широког медијског простора. SNH је осмишљен да адресира прилике и изазове асоциране са задацима сакупљања, анализирања, и визуелизације информација са социјалних мрежа.



Слика 4.4.1 Интерфејс *Social Network Harvester* -а

SNH је аутоматизовано, истраживачко решење за агенције за спровођење закона, консултанте за менаџмент, правне фирме, детективске агенције или друге који сакупљају и процењују податке са друштвених мрежа. SNH темељно анализира и визуализује везе између пријатељстава, постова, фотографија, снимака, коментара и лајкова и поседује кориснички интерфејс који је лак за коришћење. Лако се могу уочити групе и пресеци скупова. SNH штеди време и ресурсе захваљујући брзом и аутоматизованом сакупљању података. Садржи интегрисану визуелизацију која омогућава директни и брзи преглед. Уколико је потребно, могуће је експортирати целу мрежу, или само делове, за даљу обраду.



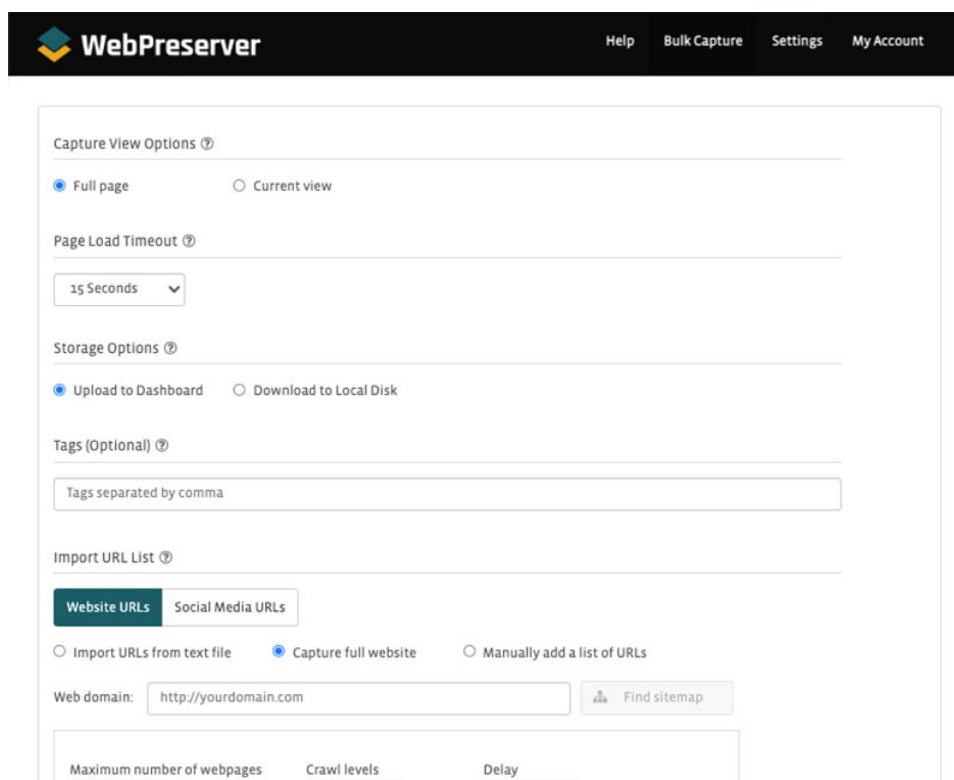
Слика 4.4.2 Визуелизација података у *Social Network Harvester* -у

Главне особине SNH алата су следеће:

- Чува јавне листе контаката
- Чува чланове група
- Установљава међусобне пријатеље
- Чува албуме фотографија, укључујући и видео снимке
- Чува временску линију
- Одређује идентификаторе корисника, укључујући и претрагу корисника
- Детектује релевантне профиле
- Истражује податке
- Открива заједнице
- Преглед мреже контаката
- Репрезентација целовите и индивидуалне под-мреже
- Пријатељи се листају као табеле
- Приказ контактних мрежа кроз графове
- Експортовање за друге алате

4.5 WebPreserver

Web Preserver је алат који служи за колекцију и презервацију садржаја са друштвених мрежа и другог онлајн садржаја. Обезбеђује поуздану, аутоматизовану претрагу и чување података. Докази се могу сакупити у два клика. Коришћењем Web Preserver додатка за Chrome, могу се сачувати интернет странице и профили на друштвеним мрежама. У том случају, садржај се чува на локалном рачунару, у форми форензичког дигиталног доказа. Web Preserver штеди време тако што аутоматски проширује дуге, сакривене постове, коментаре и одговоре и на тај начин осигурава да је цео садржај уснимљен, без потребе да се ручно проширују претходно поменуте секције. Овај алат такође генерише доказе у различитим форматима: OCR, PDF, MHTML, WARC. Прва три формата обезбеђују целокупан контекст и потпуно су претраживи.



The screenshot displays the WebPreserver web interface. At the top, there is a dark header with the WebPreserver logo on the left and navigation links for 'Help', 'Bulk Capture', 'Settings', and 'My Account' on the right. The main content area is a light gray box containing several sections of settings:

- Capture View Options**: Two radio buttons, 'Full page' (selected) and 'Current view'.
- Page Load Timeout**: A dropdown menu currently set to '15 Seconds'.
- Storage Options**: Two radio buttons, 'Upload to Dashboard' (selected) and 'Download to Local Disk'.
- Tags (Optional)**: A text input field with the placeholder 'Tags separated by comma'.
- Import URL List**: Two tabs, 'Website URLs' (active) and 'Social Media URLs'. Below the tabs are three radio buttons: 'Import URLs from text file', 'Capture full website' (selected), and 'Manually add a list of URLs'.
- Web domain**: A text input field containing 'http://yourdomain.com' and a 'Find sitemap' button.
- Advanced Settings**: Three input fields for 'Maximum number of webpages', 'Crawl levels', and 'Delay'.

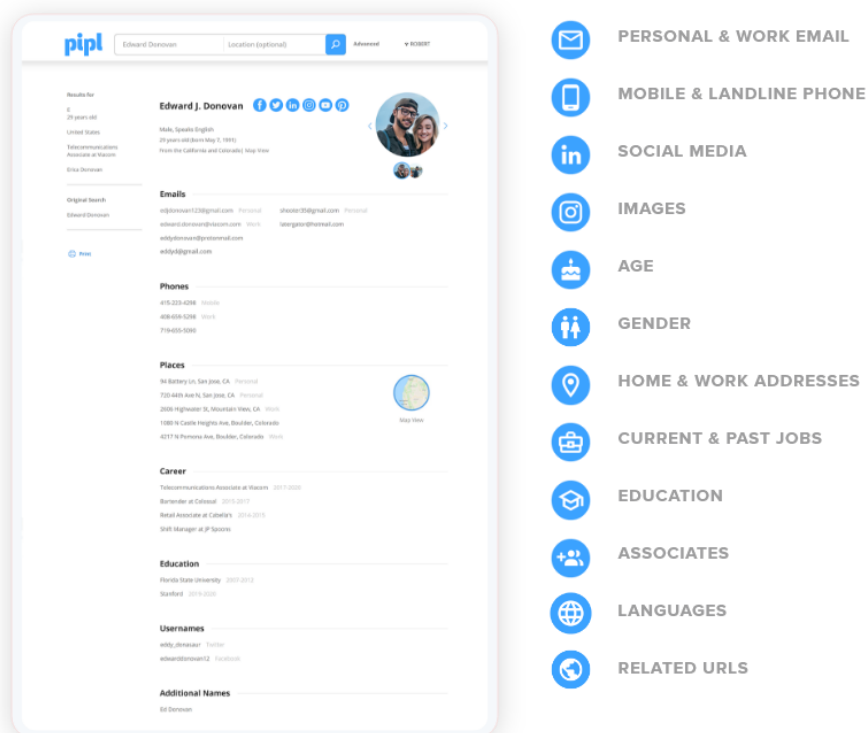
Слика 4.5.1 Интерфејс Web Preserver алата

Кључни аспекти Web Preserver алата су следећи:

- Прикупљање података са Facebook-a, Twitter-a, Instagram-a, Youtube-a, TikTok-a и многих других - Web Preserver може претворити било који профил на социјалним мрежама у аутентификоване доказе. Довољно је отићи на жељени профил и поставити параметре за чување у падајућем менију. Може се изабрати цео профил, или само подаци од значаја, и тај садржај се касније екпортује у формат који се може презентовати на суду
- Чување комплетних интернет сајтова - Web Preserver може чувати целе интернет сајтове, без типичних JavaScript препрека које се иначе срећу код већине интернет ботова. Такође омогућава и масовно чување (*bulk capture*)
- Аутоматизовано снимање видеа - аутоматски чува интегрисани видео садржај као форензички доказ. Web Preserver ће сакупити све снимке са специфициране локације и области, и омогућити њихово преузимање.
- Тренутно сакупљање доказа - социјалне мреже и постови на њима се могу веома брзо и лако променити. Уколико је потребно чекати да прође цео поступак снимања, може се десити да се неке информације промене или изгубе. Web Preserver додаток дозвољава чување онлајн доказа истог тренутка, и тиме у великој мери смањује шансе да ће докази бити нетачни или нерелевантни.
- Аутоматизовани процес сакупљања - истражитељи често приговарају да чување података са социјалних мрежа траје веома дуго и да је то фрустрирајући посао. У великом броју случајева, уахтева да истражитељ ручно пролази кроз садржај и проширује све постове, коментаре и одговоре. Једна временска линија од 500 страна на Facebook-у може се претворити у 3000 страна након проширења свог садржаја. Ово траје сатима, чак и данима, ако се ради ручно. Зато Web Preserver аутоматизује овај процес у потпуности: истражитељи се могу фокусирати на остале задатке док овај алат врши експанзију и прикупљање.
- Без сумњиве активности - приликом коришћења Facebook API-ја, често се дешава да се налози истражитеља означе као “сумњиви” и бивају закључани. Код система чувања који имплементира Web Preserver, ово се не дешава: нема означених налога, нема препоручених пријатеља, трагова IP адреса, закључаних налога, и нема активности које се могу повезати за истражитељима.
- Лака интеграција - Web Preserver не захтева инсталацију или конфигурацију, довољно је само учитати додаток за Google Chrome претраживач

4.6 Pipl Search

Pipl Search је алат за идентификовање личних, професионалних и социјалних информација онлајн. Ово је један од најсофистициранијих енџина за претрагу људи доступан истражитељима. Pipl сакупља податке са Интернет извора као што су јавне евиденције, листинзи, директоријуми и онлајн архиве, али поседује и своје приватне ексклузивне изворе. Pipl има глобално покриће, са преко 3 милијарди онлајн идентитета и 25 милијарди индивидуалних података. Све што је потребно је један податак (попут имена, броја телефона, или мејл адресе) и Pipl Search ће брзо обезбедити све информације доступне о тој особи.



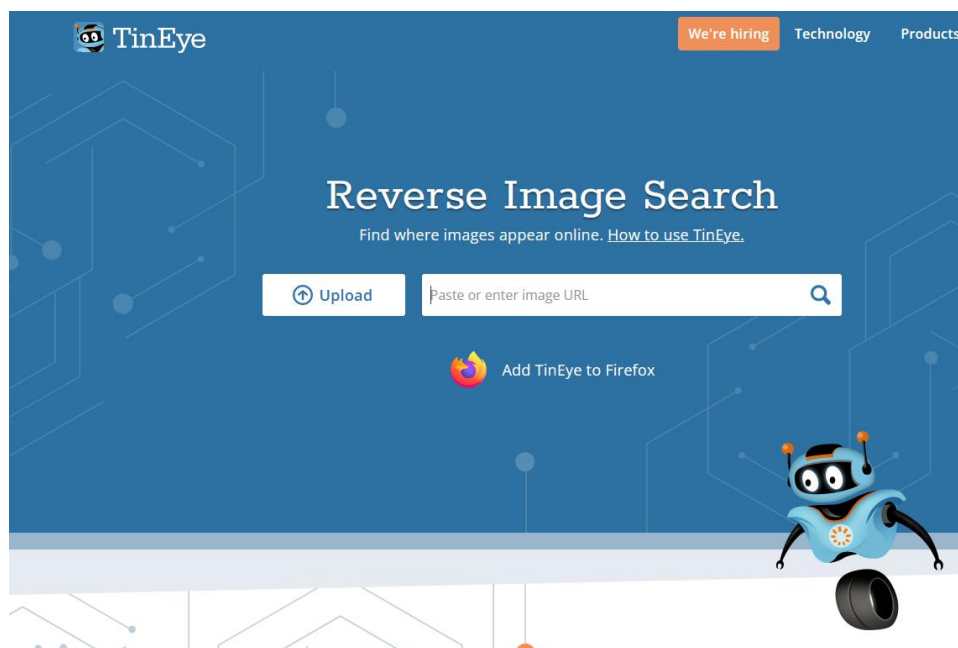
Слика 4.6.1 Интерфејс Pipl Search алата

Између осталог, Pipl Search нуди:

- Лоцирање и контактирање - проналази алтернативне контакт информације, контакт информације родбине или познаника, и лоцира укључене и умешане странке са минималном количином потребних информација за проналазак
- Умањује трошкове губитака и превара - открива доказе о преувеличаним или лажним изјавама брже захваљујући тренутном приступу провереног идентитета, експортује те информације за глатку интеграцију са системима за менаџмент случајева, детектује шаблоне и креира везе ка професионалним и организованим преварама
- Повезује контакт информације са личним информацијама - открива налоге на друштвеним мрежама чак и када су корисничка имена двосмислена, линкује директно на странице са сликама, скорашњим активностима, везама и многе друге
- Приступа метаподацима - информације о извору, времена првог или последњег виђења

4.7 TinEye

TinEye је алат за претрагу извора неке слике. Алат је веома једноставан за коришћење, али веома користан и моћан. Довољно је само убацити слику, а резултат претраге даће сва места онлајн на којима се та слика користи и појављује. Пример случаја коришћења био би: имате слику која је асоцирана са неким Facebook профилем и желите да откријете на којим још друштвеним мрежама се та слика користи.



Слика 4.7.1 TinEye алат

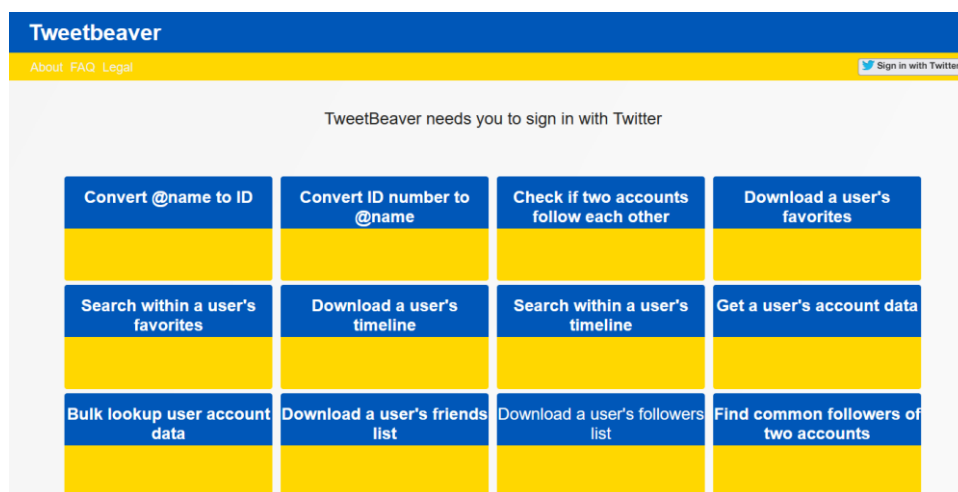
Функционалности које TinEyeу пружа су:

- Напредна идентификација слика - користи препознавање слика за моделирање садржаја и детекцију превара
- Праћење фотографија - прати где и како се нечије слике користе онлајн
- Препознавање мобилних слика - повезује физички свет са дигиталним коришћењем енцина за препознавање слика
- Подударање лабела - Инетгрише брзо и тачно подударање лабела за индустрију пића
- Верификација слика - Верификује слике, проналази где се слика појављује, уз поштовање ауторских права
- Претрага боја - обезбеђује један од најбољих, ако не и најбољи алат за претрагу боја

4.8 TweetBeaver

TweetBeaver је једноставан, али изненађујуће моћан алат који омогућава брзо сакупљање велике количине информација са било ког јавног Tweeter налога. Неке од могућности које нуди TweetBeaver су:

- конвертовање корисничког имена (@name) у ID,
- конвертовање ID у корисничко име,
- провера да ли се два налога међусобно прате,
- прибавити омиљене ставке корисника,
- претрага по омиљеним ставкама,
- преузети корисничку временску линију, њена претрага,
- прибавити податке о налогу,
- прибављање листе пријатеља корисника,
- прибављање листе пратиоца корисника
- проналазак заједничких пратиоца за два налога
- прибављање разговора између два налога
- пронаћи првих 25 налога која су запратила корисника
- пронаћи првих 25 налога које је корисник запратио



Слика 4.8.1 Изглед TweetBeaver сајта

Литература

Muhammad Firdaus, “Forensic Analysis of Social Media Data : Research Challenges and Directions”

JUNG SON , “Social Network Forensics: Evidence Extraction Tool Capabilities”

EnCase Forensics: <https://www.opentext.com/products/encase-forensic>

Social Network Harvester: https://digitalintelligence.com/solutions/social_networks

Web Preserver: <https://www.pagefreezer.com/webpreserver/>

PiplSearch: <https://pipl.com/resources/library/investigation-for-insurance>

TinEye: <https://tineye.com/>

Tweetbeaver: <https://tweetbeaver.com/index.php>