Математички факултет

Семинарски рад
из техничког и научног писања

Дигитална форензика и анализа трагова у сајбер безбедности

Студент
Стефан Павловић
(67/2025)

Професор
др Јелена Граовац

Београд, 20. јануар 2026.

Садржај

Сажетак

У овом тексту су приказане основе дигиталне форензике, њене гране и процес истраге. Обрађена је и тема анализе трагова у сајбербезбедности, као и примене дигиталне форензике у истрагама високотехнолошког криминала и истрагама осталих кривичних дела.

1 Увод

Наглим развојем личних рачунара раних осамдесетих година прошлог века појављује се дигитална форензика, односно наука дигиталне форензике. Има много значаја за технолошке фирме, у случајевима разних облика сајбер напада, али још више код органа реда. Органи реда је користе у истрагама високотехнолошког криминала, али и истрагама осталих кривичних дела с обзиром на то да су рачунари постали део свакодневног живота већине светског становништва. Дигитална форензика обухвата процес сакупљања и обраде дигиталних доказа, тако да буду очувани и признати на суду. Њен значај баш лежи у томе што се ти докази третирају као и сви други докази неког кривичног дела. Она је грана форензичке науке. Истражитељи који примењују дигиталну форензику током прикупљања дигиталних доказа прате строге процедуре, као и други истражитељи, да докази не би били оштећени ради њиховог признавања на суду. Дигитална форензика обухвата прикупљање доказа са било којег дигиталног уређаја, а рачунарска форензика је грана која обухвата рачунаре [1].

2 Дигитална форензика

2.1 Историја дигиталне форензике

Неки од раних случајева високотехнолошког криминала су били приступи другим рачунарима преко телефонске мреже, хаковање телефонских система како би избегли плаћање телефонских позива. Ова кривична дела су извршавали људи који су се већ раније бавили другим облицима криминала. Млађа популација која се добро сналазила са технологијом је употребљавала своје вештине да добије неовлашћени приступ, тада доста скупом, плаћеном софтверу. На почетку истражитељи нису имали много алата за потребе истраге, користили су неке алате које су сами развили, а касније и комерцијалне алате који су помагали у отварању обрисаних датотека. Свакако проблематичан детаљ је био да су и најважније, највеће јединице органа реда имале мало ресурса за бављење дигиталном форензиком. С обзиром на то да дигитална форензика уопште није била развијена као наука, о лабораторијама дигиталне форензике није било ни речи. Све се своди на то да је у том периоду међу предводницима јединица органа реда владала велика незаинтересованост на тему таквих истрага.

Убрзан развој дигиталне форензике свакако прати убрзан развој и нагло повећану доступност личних рачунара, мобилних телефона,

и осталих сличних уређаја касних деведесетих и раних двехиљадитих година. У том периоду мање-више сви органи реда широм света развијају одељења, али и процедуре, за дигиталну форензику. Број случајева који се сада могу решити употребом дигиталне форензике расте. Развој технологије доводи до раста разних облика високотехнолошког криминала, ти случајеви се решавају применом дигиталне форензике. Помаже и у разним случајевима као што су убиства, крађе и друга кривична дела која се сада могу решити због неког мејла, објаве на друштвеним мрежама или слике направљене мобилним телефоном. Развијају се стандардизовани системи за чување дигиталних доказа, ради избегавања манипулације и/или подметања доказа. Развој дигиталне форензике захтева људе школоване да се њоме баве и зато академске институције широм света развијају курсеве који се баве дигиталном форензиком [2].

2.2 Гране дигиталне форензике

Дигитална форензика има разне гране које се примењују у зависности од тога каква је истрага у питању и који су подаци потребни. Неке од најзначајнијих грана су:

1. Рачунарска форензика - Прикупљање дигиталних доказа са рачунара
2. Форензика база података - Анализа база података ради откривања цурења података и других облика високотехнолошког криминала
3. Мрежна форензика - Анализирање података на компјутерским мрежама као што су приступи страницама и комуникација између уређаја
4. Меморијска форензика - Анализирање података пронађених у радној *(RAM - Random Access Memory)* меморији рачунара

Наведене гране дигиталне форензике представљају основу савремене истраге дигиталних трагова и међусобно се надовезују у комплексним случајевима. Рачунарска форензика служи као основа за анализу локалних уређаја, док форензика база података омогућава дубинско истраживање структурираних података и откривање манипулација. Заједно, све гране дигиталне форензике омогућавају комплетну реконструкцију догађаја, идентификацију индикатора компромитовања и очување доказа у складу са судским стандардима. Све то заједно чини дигиталну форензику ефикасним алатом у борби против високотехнолошког криминала и осталих кривичних дела.

2.3 Процес истраге

Процес истраге у дигиталној форензици може да варира, али у свету обично обухвата четири корака која дефинише Амерички наци-

онални институт стандарда и технологије (*NIST - National Institute of Standards and Technology*):

1. Прикупљање података
2. Преглед
3. Анализа трагова/података
4. Писање извештаја

Слика 1: Алат за форензичко клонирање диска

Кораци могу варирати у зависности од типа истраге, али ми ћемо покрити како генерално изгледа сваки корак. При прикупљању података важно је прикупити све изворе података релевантне истрази (хард дискове, уређаје, и слично). Овај корак у теорији изгледа доста једноставно, али у пракси долази до многих проблема. Ти проблеми су углавном случајеви када истражитељи немају право на прикупљање неког извора података који би могао да помогне у истрази. Да се у истрази не би ризиковао губитак података важних за истрагу, направи се клон диска, на пример алатом за форензичко клонирање диска. Један такав уређај можемо видети на слици 1

У току прегледа истражитељи прегледају све прикупљене податке везане за неки случај и траже податке који указују на неко кривично дело. У току прегледа, могу видети историје претрага, четова и друге податке на диску. Овај корак обухвата и дешифровање шифрованих података, обнову обрисаних података, преглед мета-информација података, и слично. Могу прегледати чак и податке из кеш меморије оперативног система.

Анализа података, односно трагова, је свакако можда и најзначајнији део процеса истраге у дигиталној форензици. Ту на основу прикупљених података закључују њихов смисао, повезаност и важност при истрази, односно случају. Користе се разни алати зарад откривања повезаности података који можда не буду најјаснији у самом процесу прегледа.

Након претходно набројаних корака, следи писање извештаја, који обухвата опис догађаја, узроке и евентуалну одговорност учесника.

Приликом састављања извештаја узимају се у обзир различити фактори: уколико недостају подаци и није могуће утврдити јасног кривца или узрок, наводе се алтернативна објашњења. Формат, структура и фокус извештаја прилагођавају се његовој намени и циљној публици, па се истичу различити детаљи у зависности од тога за кога је извештај намењен [4].

2.4 Анализа трагова у сајбер-безбедности

Анализа трагова у сајбер-безбедности је једна од најзначајнијих области дигиталне форензике. Она обухвата откривање, анализирање и разумевање активности које су се догодиле или се активно догађају у дигиталним системима, мрежама и сервисима. Трагови у овом контексту могу укључивати лог датотеке оперативних система, лог датотеке мрежних уређаја, податке са сервера, *cloud* сервиса, али и метаподатке који настају током комуникације унутар информационих система.

Један од најважнијих делова анализе трагова јесте идентификација индикатора компромитовања, као што су неуспели покушаји пријаве на неки систем или платформу, приступи подацима са сумњивих IP адреса, покушаји неовлашћеног приступа или неуобичајен проток саобраћаја (нпр. приступ великом броју података у кратком временском периоду). У оквиру сајбер-безбедности истражитељи се ослањају на различите алате за анализу лог датотека, разне системе, као и форензичке платформе које омогућавају систематску обраду и повезивање догађаја.

Анализа трагова игра кључну улогу у реконструкцији хронологије сајбер инцидента. На основу ових података могуће је утврдити како је нападач приступио систему, које акције је извршио, као и да ли је оставио малвер или неки други облик компромитованог кода. Осим тога, анализа трагова је важна и за превенцију будућих напада, јер се на основу добијених увида могу унапредити безбедносне праксе, конфигурације система и обезбеђење платформе.

3 Примена дигиталне форензике

Дигитална форензика има широку примену у истрагама кривичних дела, како у области високотехнолошког криминала тако и у истрагама осталих кривичних дела где дигитални трагови могу да постану кључни докази. Са порастом употребе дигиталних уређаја, готово свако кривично дело оставља неки дигитални траг (мејлови, поруке, GPS локације, друштвене мреже), што чини дигиталну форензику врло важном у савременим истрагама кривичних дела. У табели 1 можемо видети разлике између дигиталних и физичких доказа у форензичким истрагама.

Табела 1: Поређење физичких и дигиталних доказа у форензичким истрагама

Особина	**Физички докази**	**Дигитални докази**
Облик доказа	Материјални (оружје, отисци, ДНК)	Нематеријални (фајлови, логови, метаподаци)
Начин прикупљања	Физичко изузимање са места догађаја	Клонирање уређаја, копирање података
Потреба за специјалним алатима	Лабораторијска опрема	Форензички софтвер и хардвер
Ланац чувања доказа	Физичко обезбеђење и документација	Криптографски хешеви и документација

3.1 Примена дигиталне форензике у истрагама високотехнолошког криминала

Високотехнолошки (сајбер) криминал обухвата дела као што су хаковање, крађа идентитета, ransomware напади (напади којима се украду или закључају неки подаци и извршилац кривичног дела тражи одређену количину новца зарад очувања података), финансијске преваре и дистрибуција малвера. Дигитална форензика овде игра централну улогу у идентификацији нападача, реконструкцији инцидента и прикупљању доказа за суд.

Примери примене:

- Анализа малвера и индикатора компромитовања ради утврђивања начина уласка нападача у систем (нпр. *phishing* мејлови или експлоатација слабих тачака система).
- Мрежна форензика за праћење саобраћаја и идентификацију *IP* адреса или командних сервера.
- Реконструкција сајбер инцидента у корпоративном окружењу, што омогућава не само кривично гоњење већ и превенцију будућих напада (*DFIR - Digital Forensics and Incident Response*).
- Истраге криптовалутних превара или *dark web* трансакција, где се прате, између осталог, *blockchain* трансакције.

Ова примена је кључна за органе реда и приватне компаније, јер омогућава откривање нападача (повезивање са конкретним починиоцима) и очување доказа који ће бити прихваћени на суду.

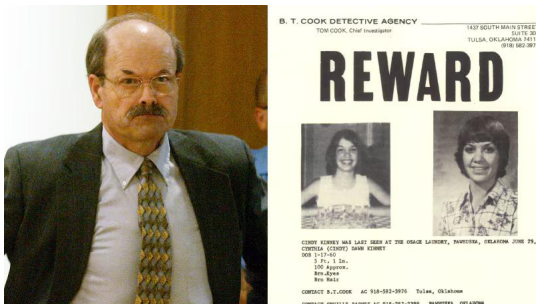
3.2 Примена дигиталне форензике у истрагама осталих кривичних дела

Дигитална форензика се све више користи у истрагама осталих кривичних дела, где дигитални уређаји пружају индиректне доказе о

мотиву, алибију, локацији или комуникацији извршиоца или осумњиченог за кривично дело.

Примери примене:

- У истрагама убистава или напада: анализа мобилних телефона за *SMS* поруке, позиве, *GPS* локације или фотографије (нпр. случај *BTK* серијског убице, којег можемо видети на слици 2, решен 2005. преко метаподатака на флопи диску) [3].
- Крађе и пљачке: Преглед камера, друштвених мрежа или објава које указују на то да је осумњичени извршио кривично дело.
- Трговина дрогом или тероризам: праћење комуникације преко апликација (WhatsApp, Telegram), друштвених мрежа, али и боље шифрованих платформи за комуникацију (*Signal*, такозвани *скај* телефони).
- Насиље у породици или злостављање: анализа историје претраге, мејлова или обрисаних порука ради утврђивања претњи.



Слика 2: *BTK* серијски убица, случај кривичног дела невезаног за технологију решеног употребом дигиталне форензике

У овим случајевима, дигитални докази се третирају као и физички - са строгим поштовањем ланца чувања *(chain of custody)* да би били признати на суду.

У будућности, са развојем *IoT уређаја* и вештачке интелигенције, примена ће се проширити на анализу података са паметних кућа, возила и историје ћаскања са чет-ботовима вештачке интелигенције.

4 Закључак

Наука дигиталне форензике има широк спектар примена, веома интересантну историју, али и још важнију будућност. Дигитална форензика је помогла великом броју оштећених људи при разним кривичним истрагама невезаним за технологију, али је и кључни део садашњости и будућности технологије. С обзиром на све већу улогу дигиталних технологија у свакодневном животу, дигитална форензика

представља неизоставан алат савремених истрага, који повезује технолошки развој, правни оквир и заштиту друштва од свих облика криминала.

Литература

[1] What is digital forensics? - IBM - Annie Badman, Amber Forrest: https://www.ibm.com/think/topics/digital-forensics/.

[2] Pollitt, M. (2010). A History of Digital Forensics. In: Chow, KP., Shenoi, S. (eds) Advances in Digital Forensics VI. DigitalForensics 2010. IFIP Advances in Information and Communication Technology, vol 337. Springer, Berlin, Heidelberg.

[3] Girard, J.E. Criminalistics: Forensic Science, Crime, and Terrorism 9781449691806 - страница 417

[4] Guide to Integrating Forensic Techniques into Incident Response - Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf