Др *Драган РАНЂЕЛОВИЋ*
Криминалистичко-полицијска академија,
др *Дамир ДЕЛИЈА*
Загреб,
мр *Бранкица ПОПОВИЋ*
Криминалистичко-полицијска академија, Београд

EnCase форензички алат

UDK: 343.9:004.4

Апстракт: *Компјутерска или дигитална форензика се дефинише као процес прикупљања, очувања, анализе и презентовања дигиталних доказа, који су дигитални подаци и који могу потврдити да ли је почињено криминално дело, као и везу између криминала и починиоца. Користи форензичке hardware и software алате, као и научне методе за откривање, идентификацију, валидацију, извлачење, опоравак и анализу дигиталних података.*

Ново је поље науке а заинтересованост за проблематику којом се бави огледа се у чињеници да тренутно постоји више десетина колеџа и универзитета који само у Америци обављају едукацију у овој научној дисциплини.

Овај рад се бави једним од форензичких алата, EnCase фирме Guidance, који представља стандард у судској пракси САД и земљама ЕУ.

Кључне речи: *дигитална форензика, форензички hardware и software алати.*

Увод

Под дигиталном форензиком (ДФ) подразумева се примена научних метода за идентификацију, сакупљање, вредновање, анализу, интерпретацију, документовање, вештачење, чување и руковање дигиталним подацима уз очување интегритета оригиналног дигиталног доказа. У суштини, ДФ представља примену компјутерске истраге и техника анализе, у циљу утврђивања потенцијалних доказа (Casey, 2004; McClure, Scambray, Kurtz, 2006; Howard, Lipner, 2006; Jones, Shema, Johnson, 2003; Pastore, Dulaney, 2007).

Таксономија ДФ

Таксономија ДФ се може дати посматрајући различите аспекте:

1. Са аспекта области примене:
   - Званична (Јавна): *истрага, доказивање, хапшење, суђење;*
   - Корпорацијска (Приватна): *истрага, доказивање, ...,(суђење).*
2. Са аспекта типа процеса*:*
   - претраживање/истрага физичког/дигиталног места кривичног дела;
   - аквизиција дигиталних података/доказа;
   - анализа дигиталних података/доказа;
   - сведочење/вештачење дигиталних доказа.
3. Са аспекта објеката аквизиције/анализе:
   - ДФ рачунара или Компјутерска форензика;
   - анализа физичких медија;
   - анализа фајл система;
   - анализа апликативног слоја апстракције;
   - ДФ софтвера – Софтверска форензика: програмског, апликативног, малициозног;
   - ДФ рачунарске мреже укључујући и Интернет или Кибернетичку форензику.

Терминологија ДФ

Поступак ДФ истраге подразумева следећу терминологију:

1. Физичко место је соба са рачунарским средствима осумњиченог.
2. Физички докази су физички објекти који:
   - могу потврдити да је криминално дело почињено;
   - омогућавају повезивање криминалца и жртве;
   - омогућавају везу између криминалног дела и кривице криминалца.
3. Дигитално место је рачунар осумњиченог, као и сва остала рачунарска средства.
4. Дигитални доказ је дигитални податак који:
   - може потврдити да је почињено криминално дело,
   - може омогућити везу између криминала и починиоца.

Методологија ДФ

ДФ истраживања су јако сложена. Форензички истражитељ мора јако много да зна о грађи и функционисању оперативног система рачунарских средстава над којима се врши истрага, како не би током саме истраге дошло до уништавања дигиталних доказа. Зато је неопходно стручно ос-

пособљавање истражитеља како за коришћење рачунарских форензичких алата, тако и за саму методологију ДФ.

Код форензичких истрага додатни проблем може да представља начин презентације дигиталних доказа пред судовима. Судови у земљама ЕУ, као и судови у САД, врло су осетљиви на егзактно поштовање методологије рачунарске форензике. Није редак случај да судови одбију понуђене дигиталне доказе искључиво због непоштовања методологије рачунарске форензике.

Оквирна методологија рачунарских форензичких истрага одвија се према корацима наведеним у следећем пасусу. Ову методологију би требало схватити као врло начелну, имајући у виду да свака форензичка истрага садржи одређене специфичности које се морају уважавати.

Кораци рачунарских форензичких истрага су:

1. одредити рачунаре који су предмет истраге;
2. сачувати оригиналне медије и тиме спречити било какве измене садржаја медија;
3. ако је рачунар укључен, преузети садржај RAM (оперативне меморије);
4. искључити рачунар редовним путем или, ако тако није могуће, онда применити искључивање напајања;
5. направити копију свих битних медија рачунарских средстава над којим се врши истрага, и
6. Обавити форензичку анализу на направљеним копијама медија.

Дигитални доказ

Под дигиталним доказом се подразумева свака информација у дигиталном облику која има доказујућу вредност, а која је или ускладиштена, или пренесена у таквом облику. При томе, дигитални доказ може да буде било какав низ битова и бајтова на диску рачунара, без обзира какву репрезентацију према оперативном систему тај низ има, да ли је то документ, слика, музика, база података или нешто друго. Такође би требало нагласити да криминалци увек покушавају да за собом уклоне трагове, па су зато најквалитетнији дигитални докази, по правилу, увек невидљиви алатима самог оперативног система (Bishop, 2003; Đorđević, Pleskonjić, Maček, 2006; Tanenbaum, Woodhull, 1997; Tanenbaum, 2005).

Дигитални докази укључују:

- компјутерски ускладиштене и компјутерски генерисане доказе,
- дигиталне аудио и видео доказне податке,
- податке са дигиталног мобилног телефона,
- податке са свих других дигиталних уређаја.

Аквизиција дигиталних података

По дефиницији, аквизиција дигиталних података је прва главна фаза дигиталне форензике која применом строго научних метода обухвата процесе откривања, идентификације, валидације и извлачења дигиталних података, са циљем сакупљања физичих и дигиталних доказа узимањем физичке копије (слике, копије бит-по-бит) дискова рачунара HD, CD, FD, DVD, USB, итд.

Процедура аквизиције дигиталних података подразумева:

- фиксирање места кривичног дела – формална процедура;
- документовање физичког и дигиталног места;
- заштиту осумњиченог рачунарског средства од измене стања/података;
- искључивање рачунарског средства;
- узимање физичке слике диска и свих других медија, или привремено одузимање рачунарског средства (алтернативно);
- означавање и паковање свих компоненти рачунарског средства;
- пренос рачунарског средства у форензичку лабораторију за анализу;
- заштиту рачунара и прављење радне и референтне слике (имица);
- откривање на имицу свих података и садржаја;
- опорављање свих, или што је могуће више избрисаних фајлова;
- откривање скривеног садржаја: swap, нелоцираних и slack фајлова;
- приступ садржају заштићених и шифрованих фајлова;
- анализу, разврставање и сакупљање свих релевантних дигиталних доказа;
- извештавање о резултатима анализе;
- реконструкцију догађаја/напада, и
- обезбеђивање експертског мишљења/вештачење.

Технологија дигиталне форензике

Зашто користити форензичке алате?

Ово је питање са којим се често сусрећемо. Коришћење алата оперативног система за претраживање рачунара се, на први поглед, чини врло једноставним и сврсисходним, а пре свега са крајње добрим учинком, међутим стварна ситуација је потпуно другачија из два основна разлога:

1. први разлог је што се код рачунарских форензичких истраживања може применити принцип „леденог брега“: само мали део дигиталних доказа је могуће открити помоћу алата оперативног система, док се велика већина дигиталних доказа налази сакривена у различитим

привременим датотекама, swap датотекама, slack фајловима, обрисаним партицијама диска, обрисаним датотекама електронске поште и на свим сличним местима која су невидљива таквим алатима;

2. други разлог је што управо коришћење алата оперативног система уписује јако пуно информација у привремене датотеке. Како је величина привремених датотека увек ограничена, оперативни систем ће приликом уписивања нових информација пребрисати старе информације из привремених датотека. Интензивно коришћење алата оперативног система за обављање форензичких истраживања тако, у основи, уништава доказе, при чему доказ представљају информације у привременим датотекама (Tanenbaum, Woodhull, 1997).

Форензички алати

Под форензичким алатом у ДФ се може подразумевати техничко средство, као и програм којим се омогућава ефикасно прикупљање, чување, анализа и презентовање дигиталних доказа. Избор и подешавање тог алата пре његове конкретне употребе кључно је за његову ефикасност. Они се, у основи, могу поделити на мултифункционалне и специјализоване алате, а генерално омогућавају:

- инспекцију и превенцију,
- детекцију инцидента,
- истраживање и одговор,
- поправку система.

Технике и алати ДФ могу бити хардверски (hw) и софтверски (sw):

- успостављени су као стандарди,
- обезбеђују компетентно вођење.
- Захтева се да:
  - користе форензички стерилне медије,
  - сачувају интегритет оргиналних дигиталних података,
  - означе резултате истраге и анализе, копије дигиталних доказа, штампани материјали, ...
  - контролишу, документују и чувају дигитални доказ за даљи ток поступка.

Историјски развој форензичких алата може се дати кроз три генерације:

- прва генерација:
  разни алати за: Image, Document, Search, Recover, Report;
- друга генерација:
  посебни дизајнирани и развијени форензички алати: EnCase и други;
- трећа генерација:
  Network Forensics: тренутна, сигурна, ефикасна форензика рачунара

путем LAN-а (McClure, Scambray, Kurtz, 2006; Tanenbaum, 2005; Pleskonjić, Đorđević, Maček, Carić, 2006; Jones, Shema, Johnson, 2003).

EnCase алат

EnCase алат (произвођач Guidance Software) сматра се водећим комерцијалним алатом за рачунарску форензику (http://www.encase.com, 2009). Он је прихваћен као стандардни алат у правосуђу САД и ЕУ и велики је број судских пресуда и поступака у којима је овај алат кориштен у доказном поступку (http://www.insig2.hr/racunalna-forenzika/encase/, 2009).

За правилну употребу овог алата корисник не мора бити експерт у рачунарству да би провео стандардну рачунарску истрагу, тј. није потребно познавање детаља о меморијским јединицама нити структурама података. User-friendly кориснички графички интерфејс ослобађа корисника мучног писања командних линија и омогућава угодан рад.

EnCase је врло чест алат на рачунарима истражитеља. Статистике (на територији САД) казују да 90% истражитеља користи управо EnCase за обављање форензичких истрага. Наравно, ова статистика није случајност. Током година развоја, стручњаци фирме Guidance software, већином и сами бивши форензички истражитељи, уградили су властита најбоља искуства у EnCase, како по питању методологије истраге, тако и по питању врста потребних претраживања које алат мора подржавати (Security, info, 2006; http://www.insig2.hr, 2009).

Основне карактеристике (и предности) EnCase форензичког алата су да је :

- неинвазивни алат за форензичке истраге;
- прилагођен форензичким истраживањима на великим количинама података;
- опремљен подршком за FAT, FAT32, NTFS, Apple, Unix, Linux оперативне системе;
- способан за обављање свих нужних форензичких истраживања;
- модуларан и укључује и програмски језик EnScript за аутоматизацију појединих истраживања, и
- верификован, тј. извештаји генерисани овим алатом потврђени су и прихваћени од стране правосудних органа ЕУ и САД.

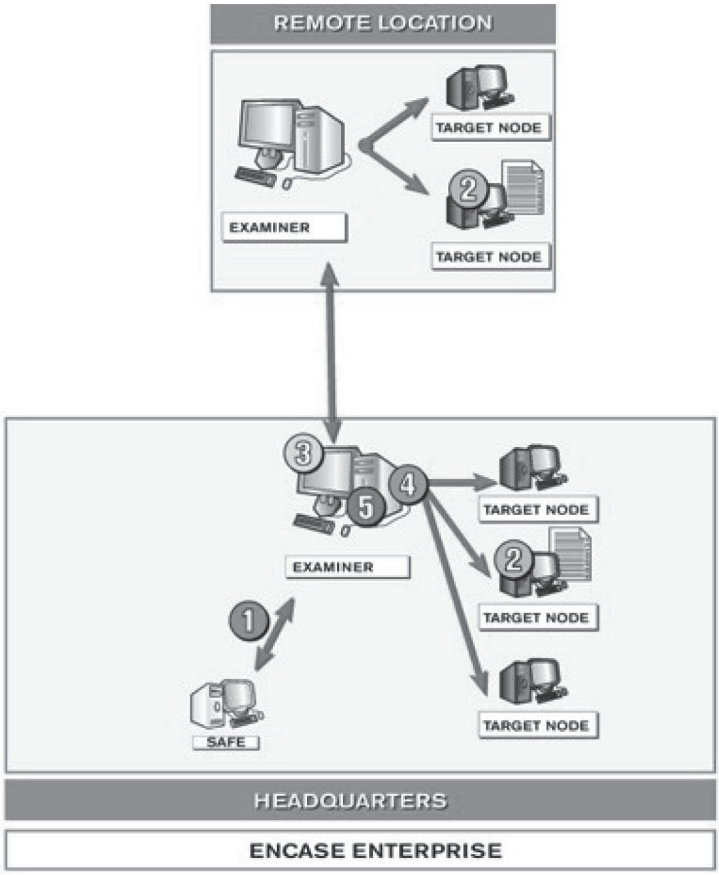
Верзије EnCase-а

Guidance software, желећи да се максимално прилагоди свакој категорији корисника, прилагодила је EnCase алат специфичним потребама сваке категорије посебно. Из овакве пословне политике настала је и палета

производа EnCase:

1. EnCase Forensic,
2. EnCase Enterprise,
3. EnCase Neutrino,
4. Field Intelligence Model,
5. eDiscovery Suite,
6. Automated Incident Response.

Како ради EnCase?



EnCase Enterprise се састоји од 5 компоненти: *Истражитељ, SAFE, Servlet, Веза* и *Одговор на инцидент*. Потребан вам је само један алат (EnCase) који се потпуно интегрише у постојећу ICT инфраструктуру омогућавајући практично тренутан приступ свим информацијама похрањеним на свим рачунарима спојеним у рачунарску мрежу. При томе, нити један рачунар на мрежи „не зна“ да се EnCase на њему извршава.

SAFE (Secure Authentication For EnCase) обавља аутентификацију корисника, управља корисничким правима, похрањује све логове из EnCase-а и осигурава сигуран пренос информација путем рачунарске мреже. *SAFE* комуницира са Истражитељем и одредишним рачунарима који су предмет истраге коришћењем 128-битне AES енкрипције.

Истражитељ је главни рачунар са којег форензичар истражитељ покреће дигитално истраживање, одговоре на инциденте, те ревизије одредишних рачунара. Основна компонента овога софтвера је *EnCase Forensics*, један од тренутно најбољих светских система за ефикасне форензичке истраге које дају резултат.

Servlet је неинвазивни, пасивни агент који се све време налази аутоматски инсталиран на клијентским и серверским рачунарима који су предмет истраге. Систем функционише на начин да се успоставља сигурна веза између *SAFE* и *Servlet* компоненти с јединим циљем – омогућавање *Истражитељу* да врши планиране форензичке истраге. *Servlet* се извршава на начин да рачунар домаћин уопште није свестан његовог постојања, он је за окружење у којем се извршава потпуно невидиљив. *Servlet* се може извршавати у следећим окружењима: сви Windows оперативни системи, Linux, Solaris, Max OS X и AIX.

Веза представља сигурну TCP/IP везу између *Истражитеља* и рачунара који је предмет истраге. Истражитељ, наравно, у истом тренутку може имати више отворених веза према рачунарима који су предмет форензичких истраживања.

Одговор на инцидент (snapshot) има могућност брзог и ефикасног претраживања информација које се налазе у радној меморији рачунара који је предмет истраге, чиме се омогућава тренутни увид у збивања на одредишном рачунару.

StandAlone режим рада EnCase-а

Циљ наредног текста је упознавање са алатом EnCase Forensic у стварним условима StandAlone режима рада.

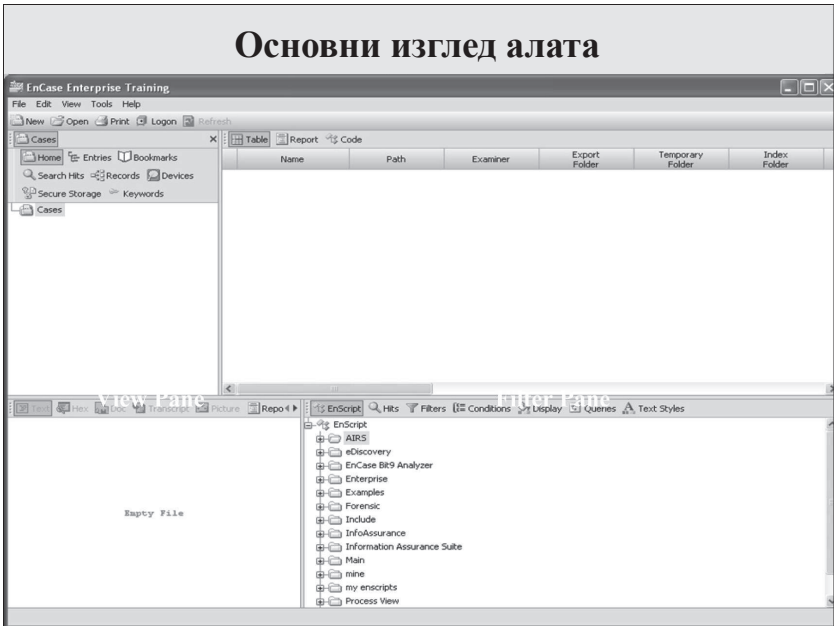
Сценарио приказан у овом раду извршава се у EnCase Forensic 11.6.2 верзији и објаснићe поступак како се:

- на основу налога спроводи претраживање форензички исправне слике предметног рачунара;
- слика рачунара прави коришћењем EnCase алата;
- спроводи анализа истим форензичким алатом;
- користе докази који су добијени.

Поступак је следећи:

1. Направити аквизицију дискова;
2. Оворити датотеку са доказима;
3. Дефинисати кључне речи за претрагу (keywords);
4. Спровести претрагу по кључним речима (search):
   - све што је занимљиво забележити (bookmark);
5. Спровести претрагу по имену датотека (conditions):
   - све што је занимљиво забележити (bookmark);
6. Спровести преглед слика (gallery view):
   - све што је занимљиво забележити (bookmark), и
7. На основу забележеног направити извештај (report).

Горе дефинисани кораци биће приказани преко одговарајућих екрана који их прате у наредном делу текста.

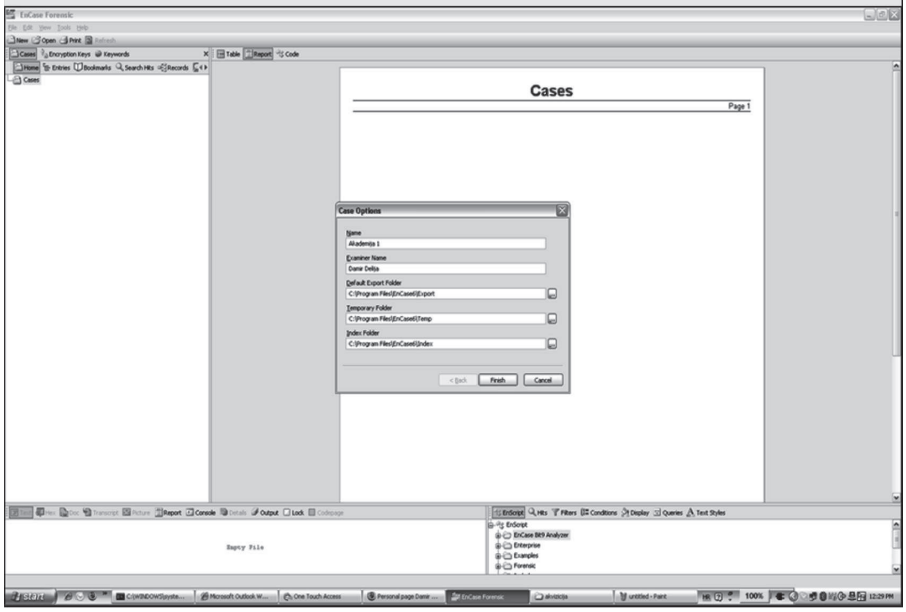


Направити аквизицију дискова

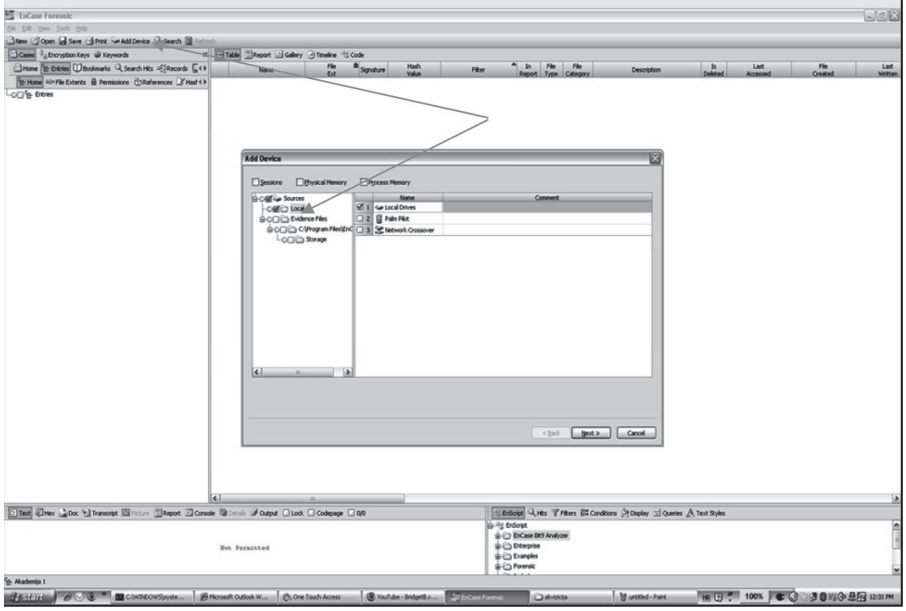
Задатак је направити слику диска кроз EnCase унутар новог случаја (Case):

- отвара се нови case;
- у Case се додају дискови и сл.;
- подешавају се параметри за аквизицију изабраних дискова, и
- изводи се аквизиција.

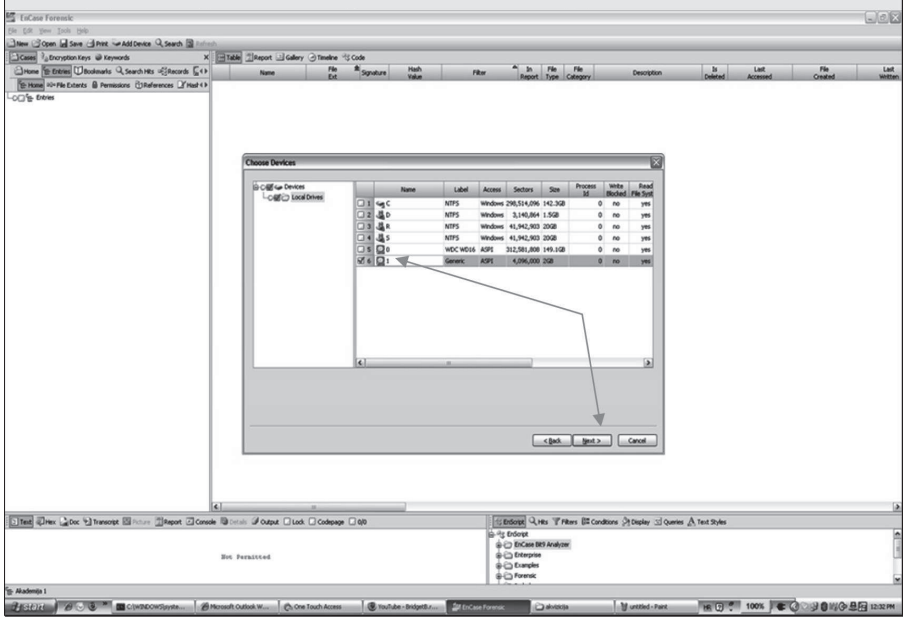
Отварање новог Case-а



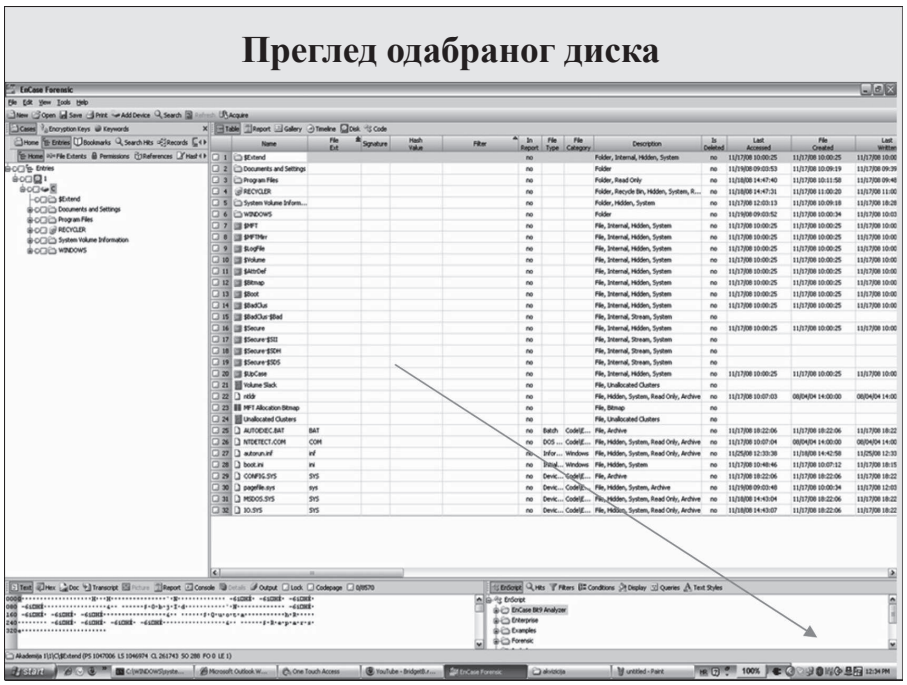
Одабирање локалних дискова



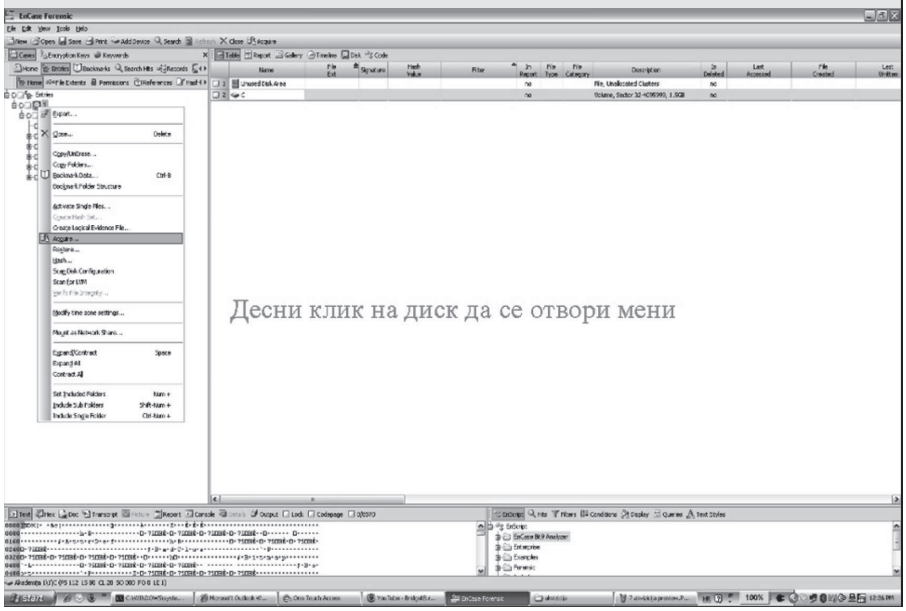
Одабирање физичког диска



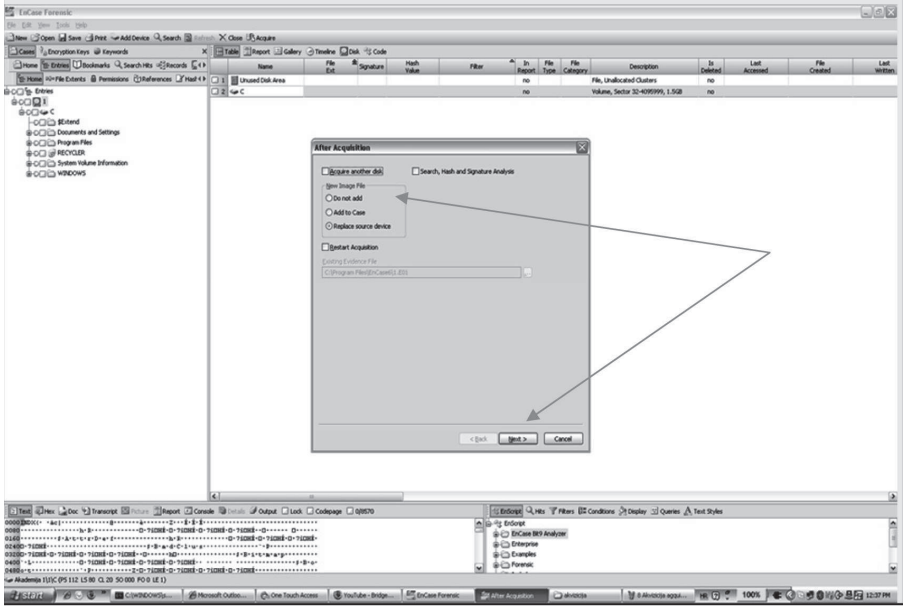
Преглед одабраног диска

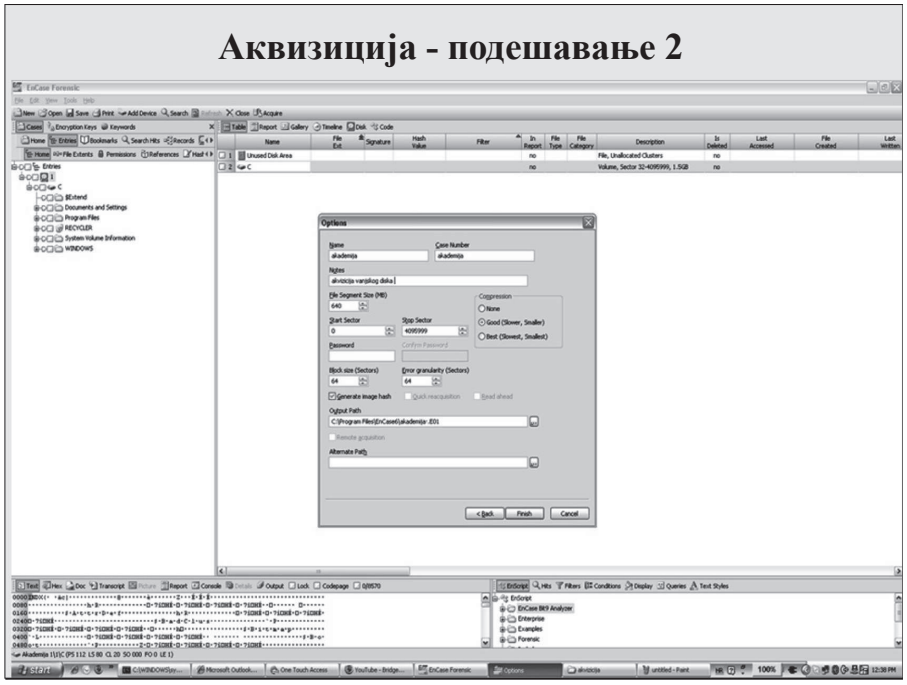


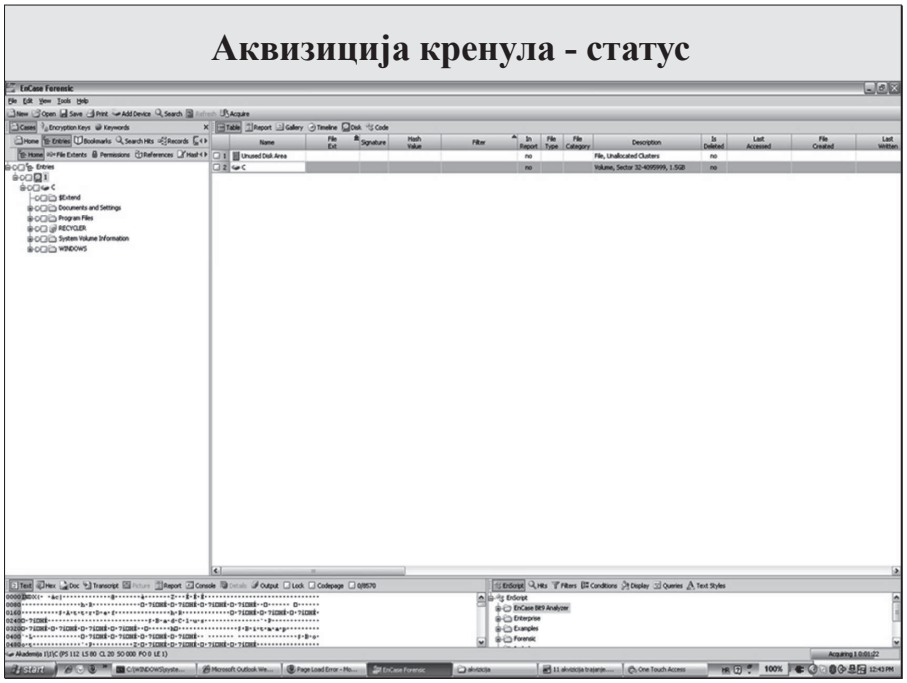
Аквизиција диска

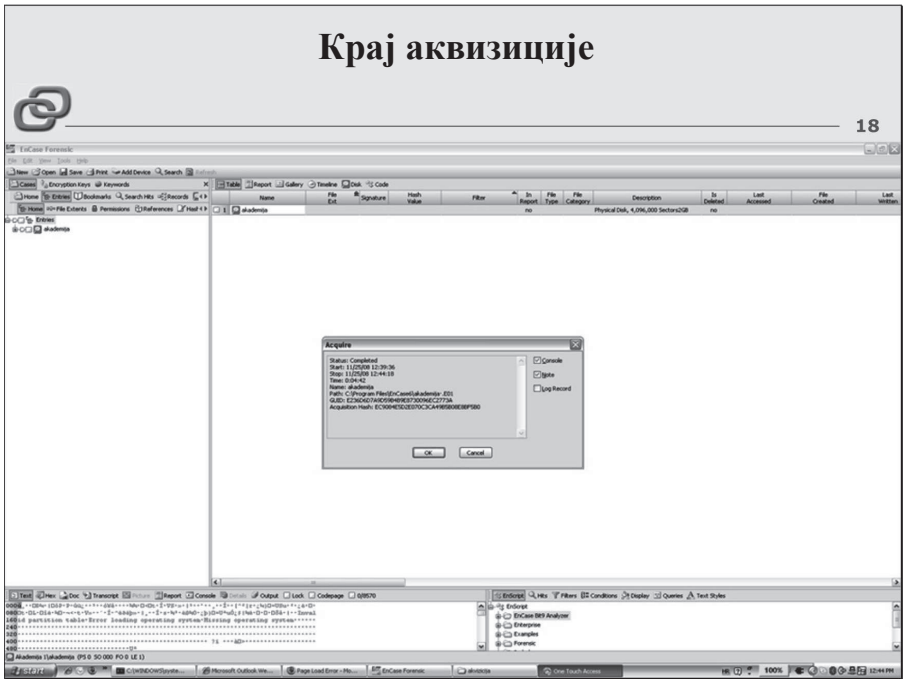


Аквизиција - подешавање 1

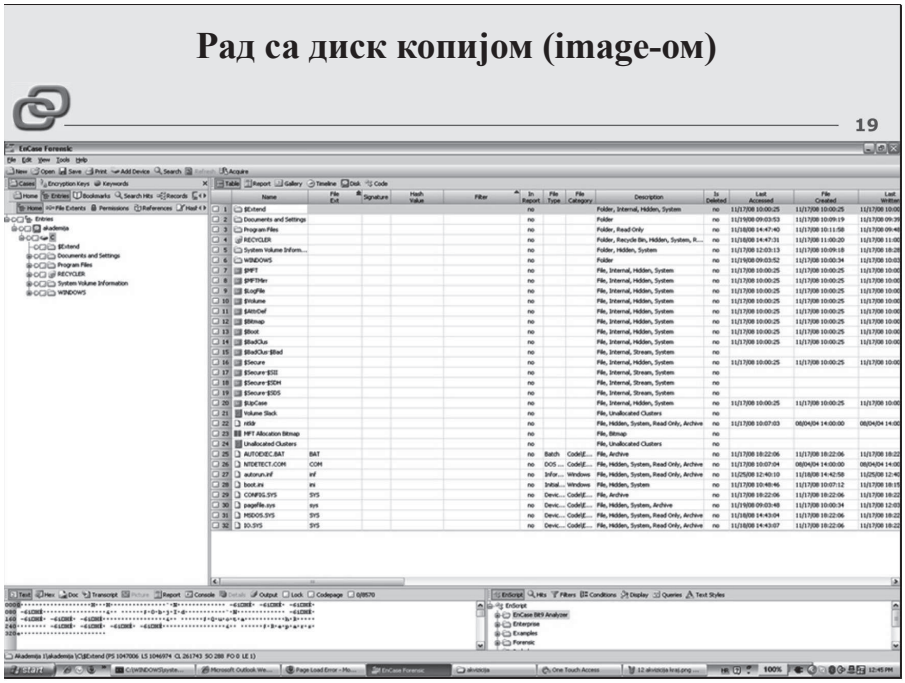



Аквизиција - подешавање 2


Аквизиција кренула - статус

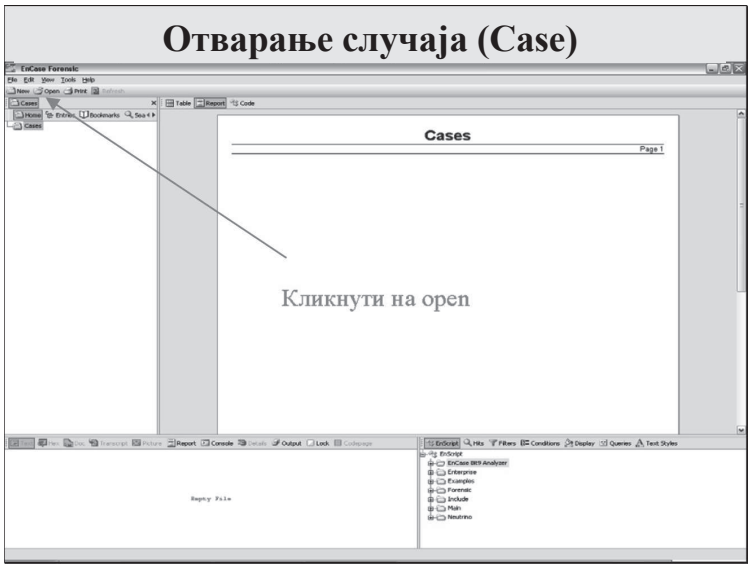


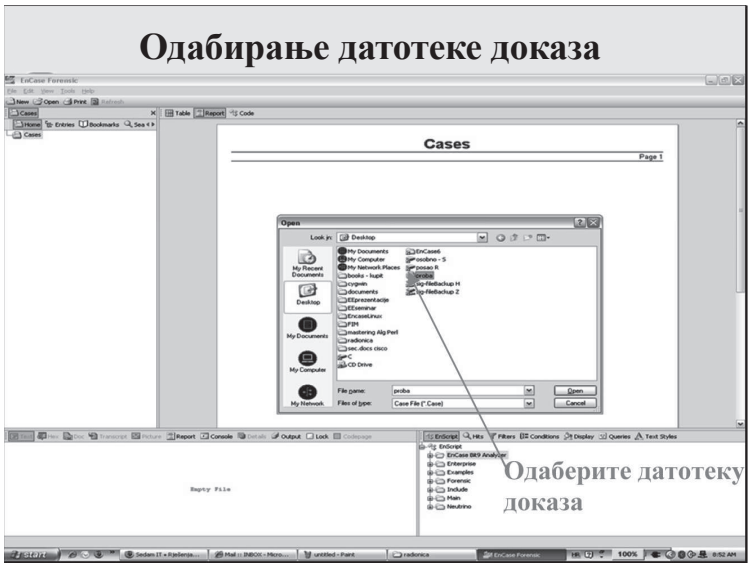
Завршавање аквизиције и спремање слике.

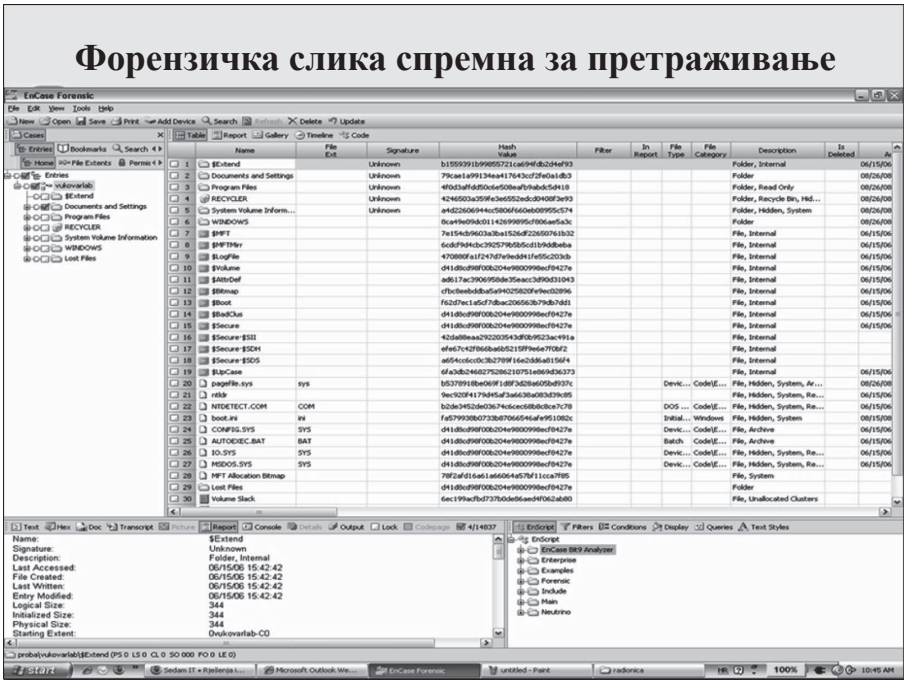


Након аквизиције се препоручује:
- да се запамти Case (File → Save);
- добра пракса је затворити Case (File → Exit) и поново га отворити;
  - због контроле да ли је све успело;
  - или због израде копије Case датотека на друге медије (ствар процедуре).

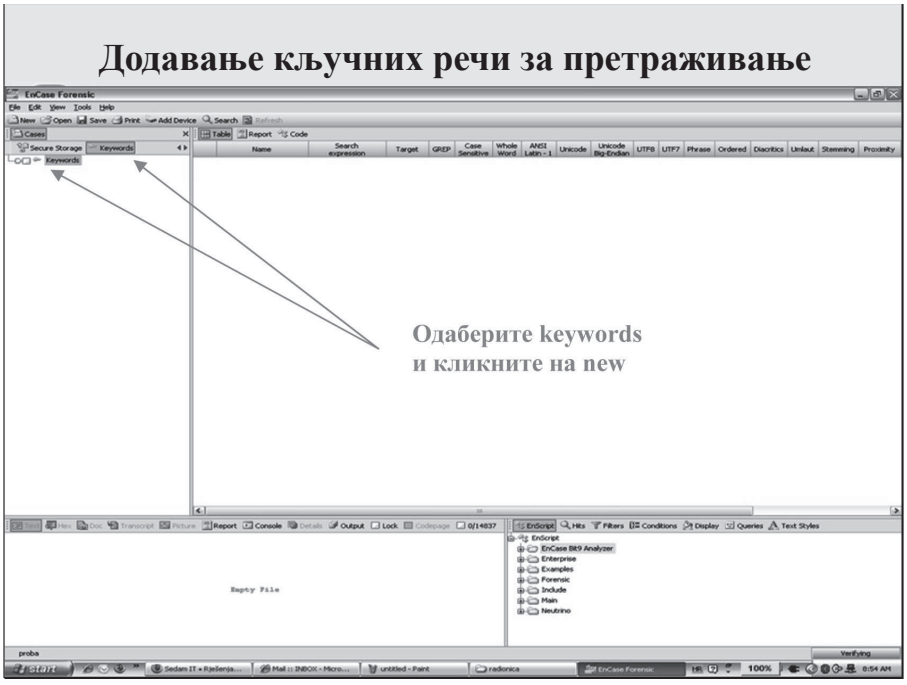
Оворити датотеку са доказима



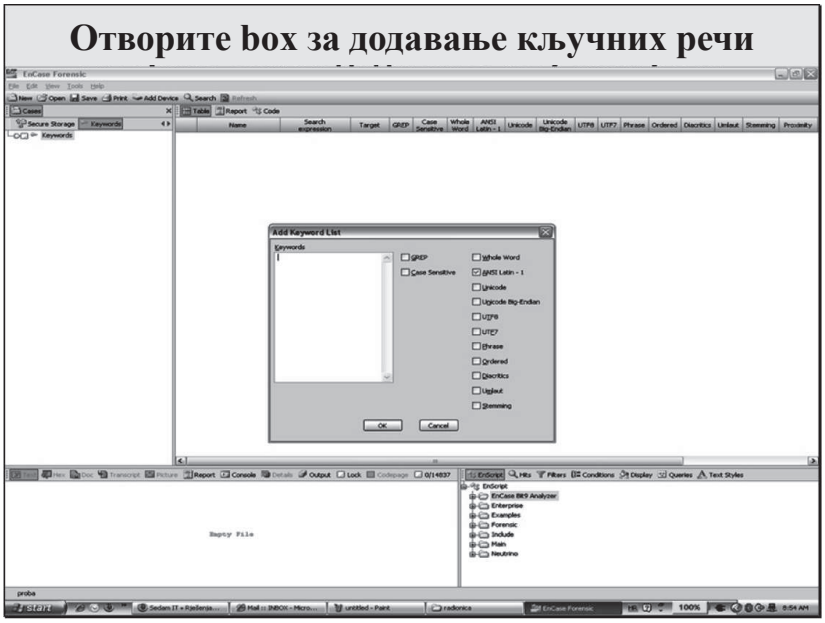


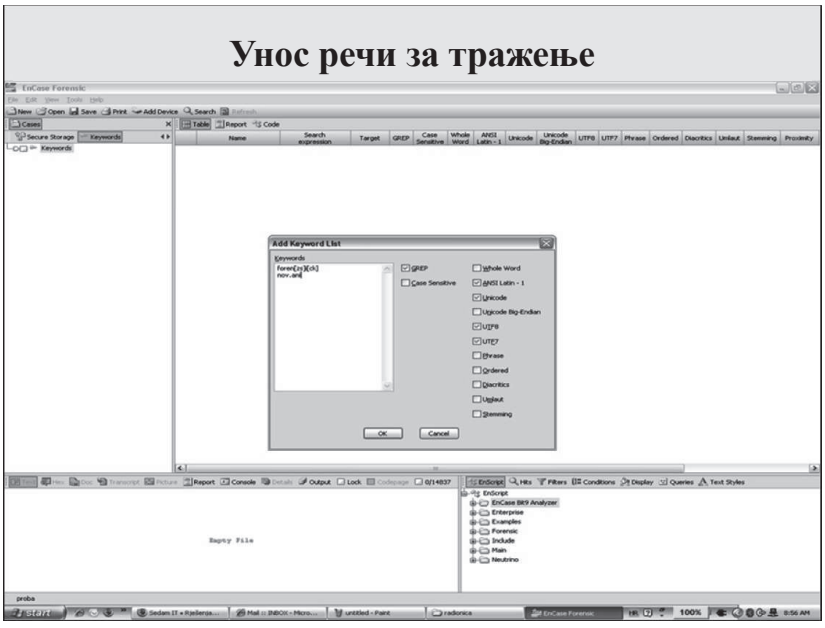


Дефинисати кључне речи за претрагу (keywords)

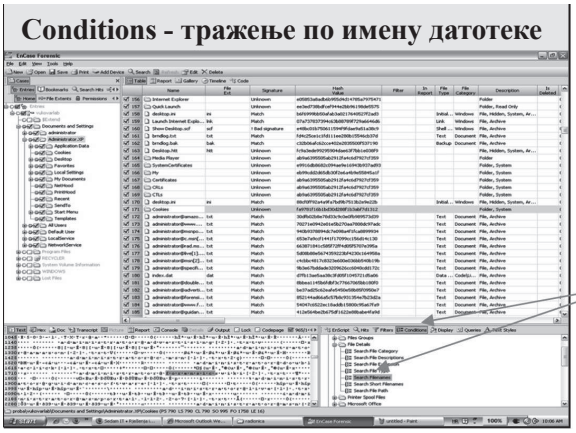


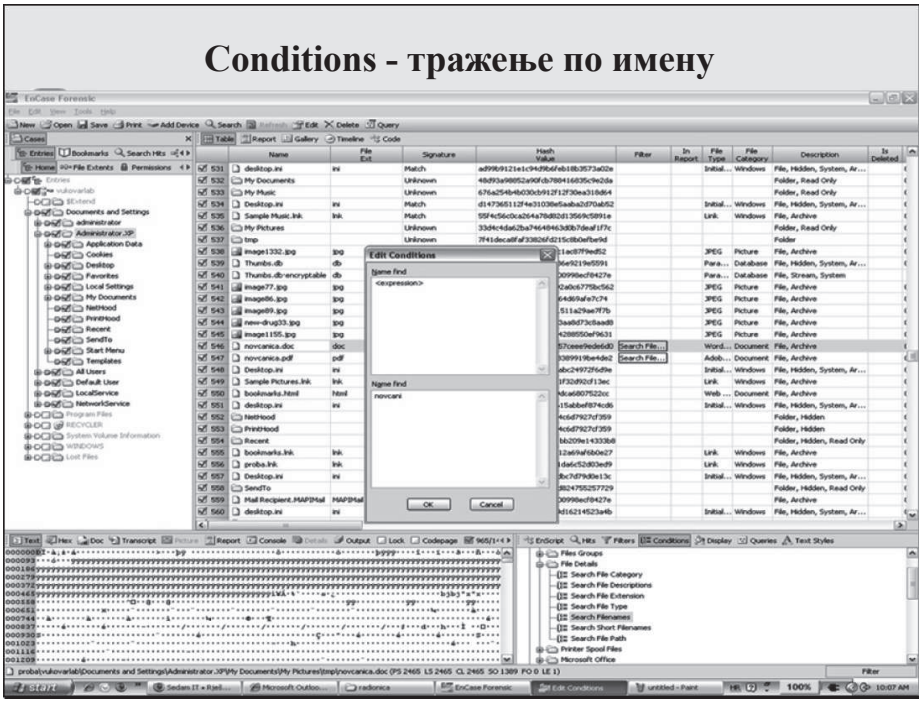
Спровести претрагу по кључним речима (search)



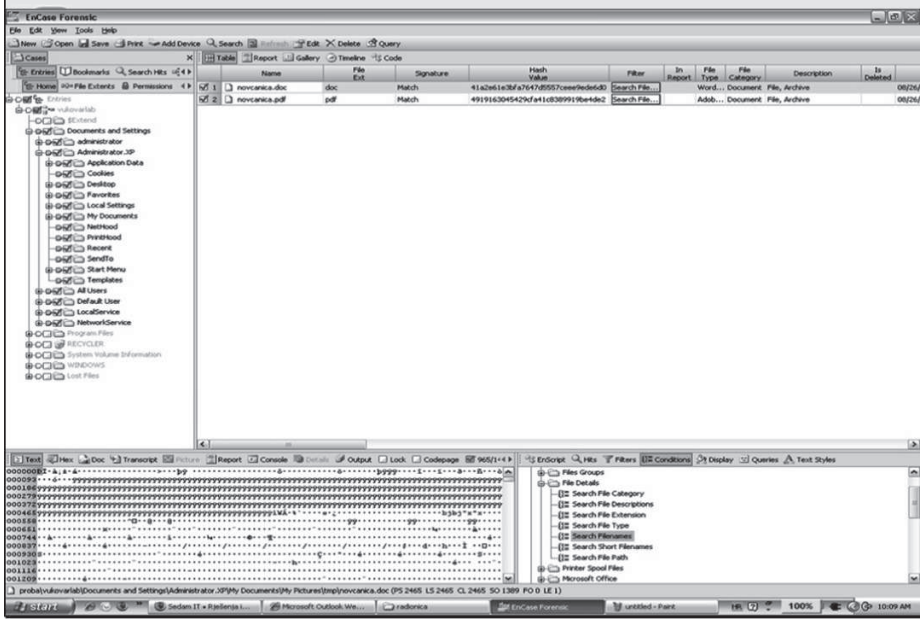


Спровести претрагу по имену датотека (conditions)


Conditions - тражење по имену датотеке
Кликните на conditions
и одаберите Search filename


Conditions - тражење по имену
Edit Conditions
Name find
<expression>
Name find
novcani
OK
Cancel

Резултати тражења по имену датотеке



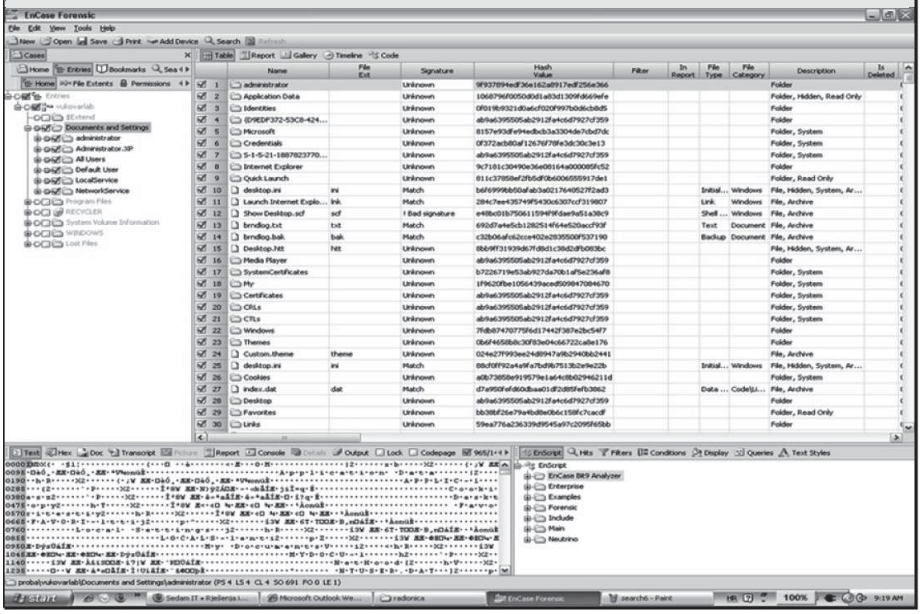
Спровести преглед слика (gallery view)

Gallery преглед - приказ слика

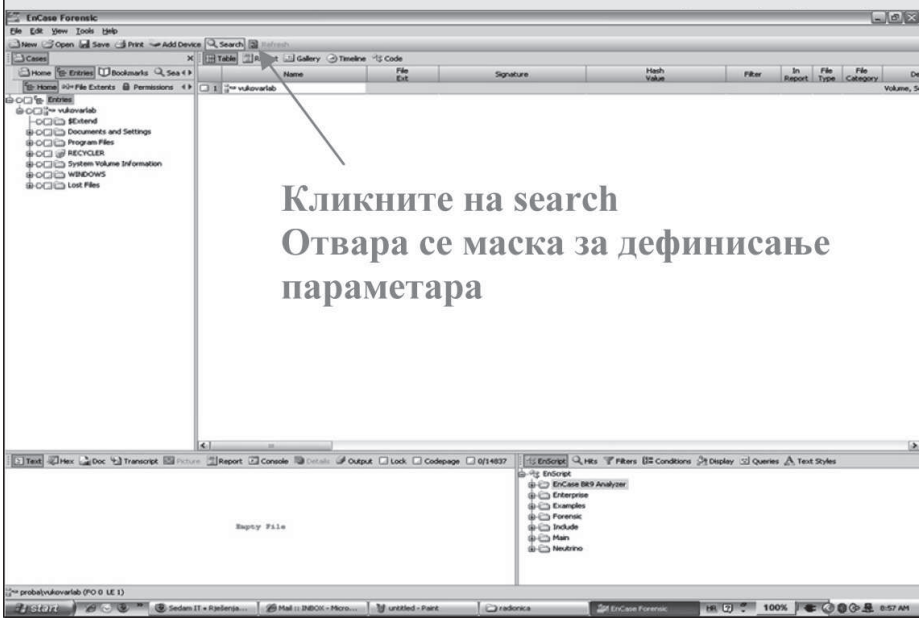
Кликните плаво штиклирано за одабир

Десним дугметом отворите мени одаберите bookmark

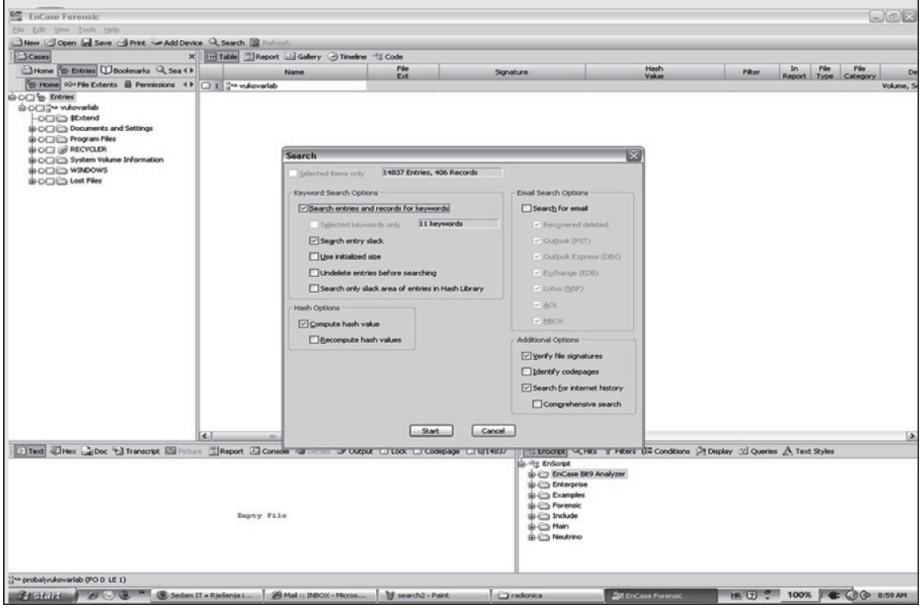
Приказ свих датотека са dixon box-ом и селектовањем



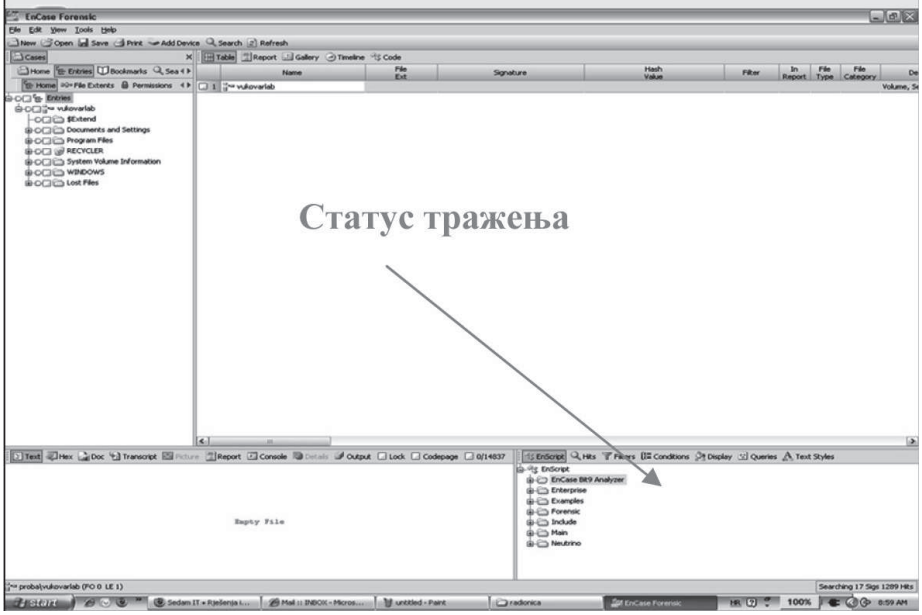
Тражење по свим датотекама на диску - траје дуго



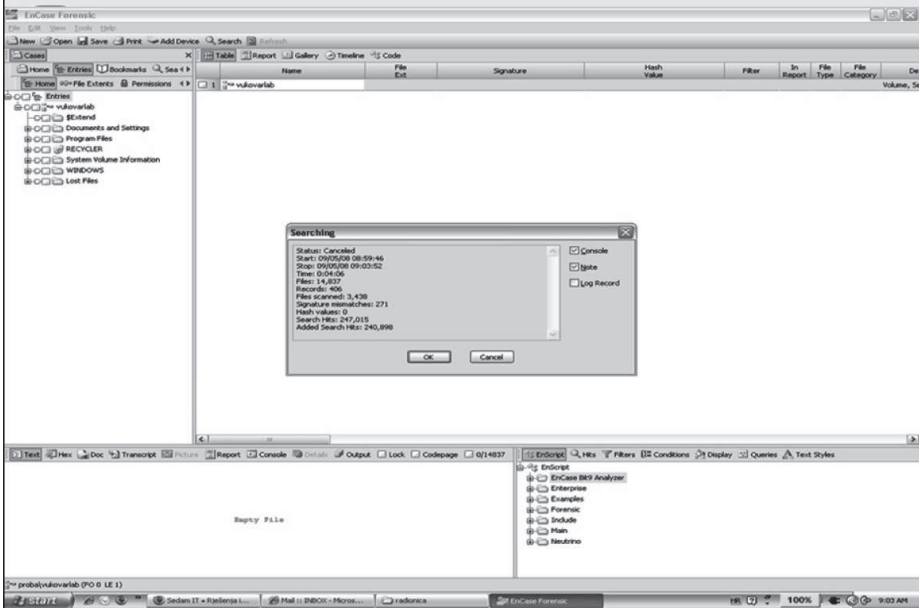
Избор параметара тражње



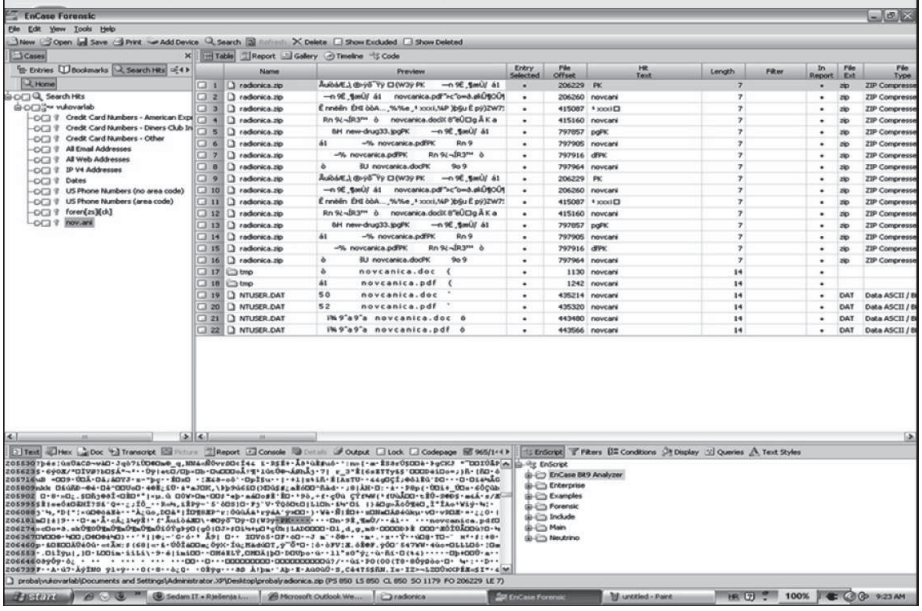
Тражење у току



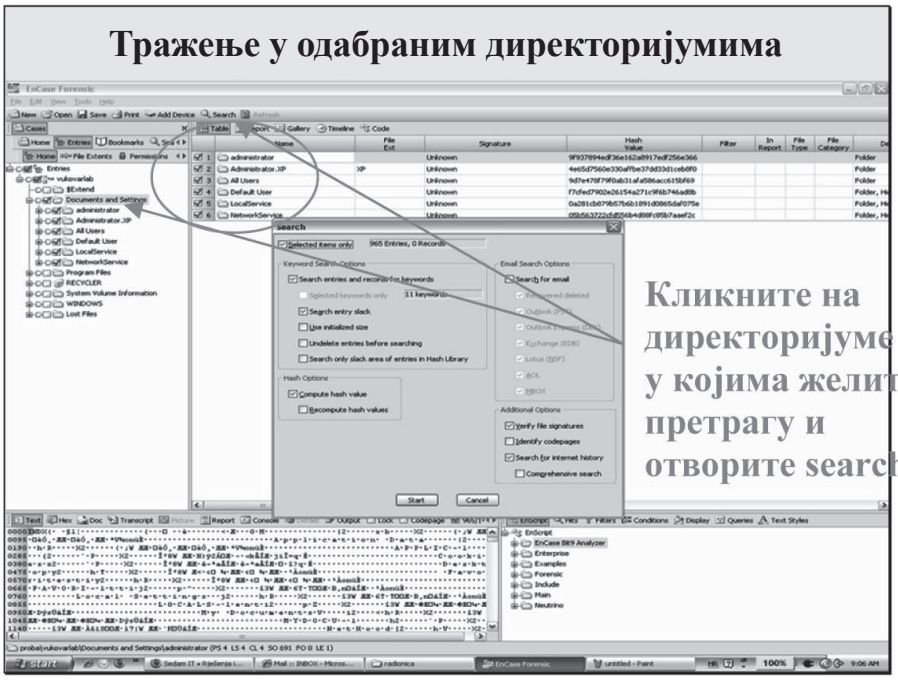
Резултати тражења - завршетак



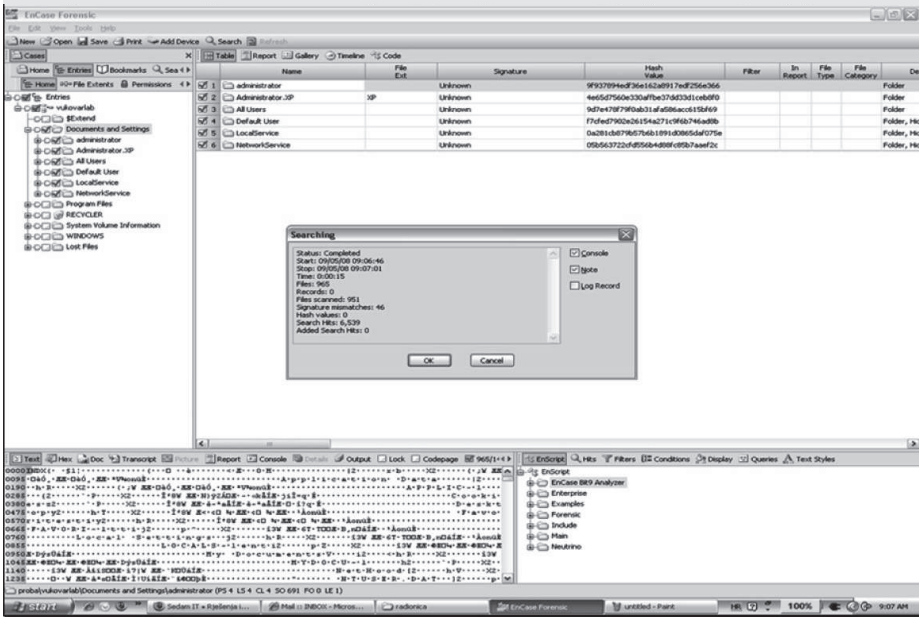
Резултати претраживања

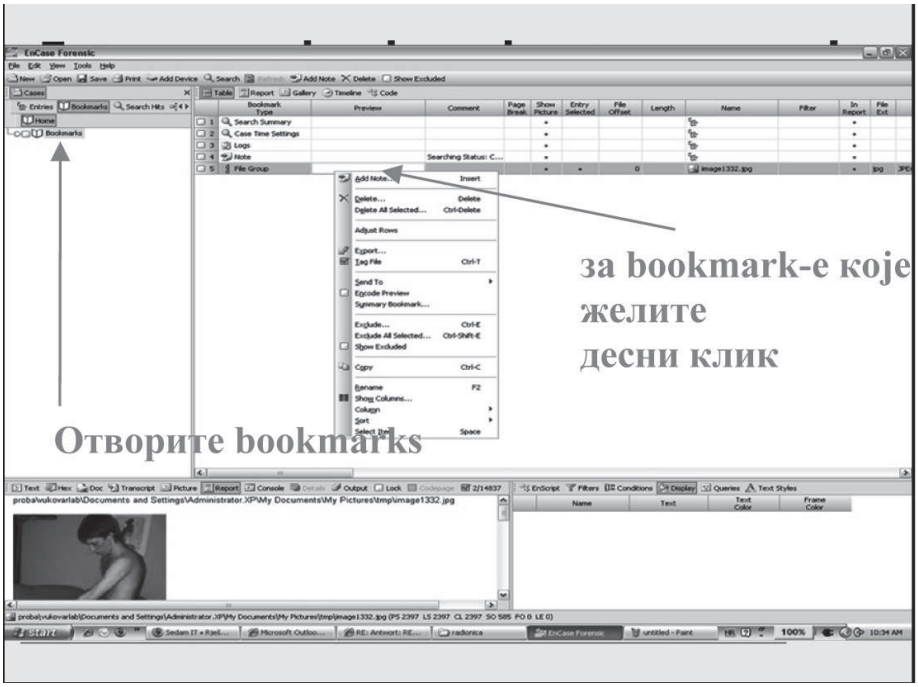


Тражење у одабраним директоријумима

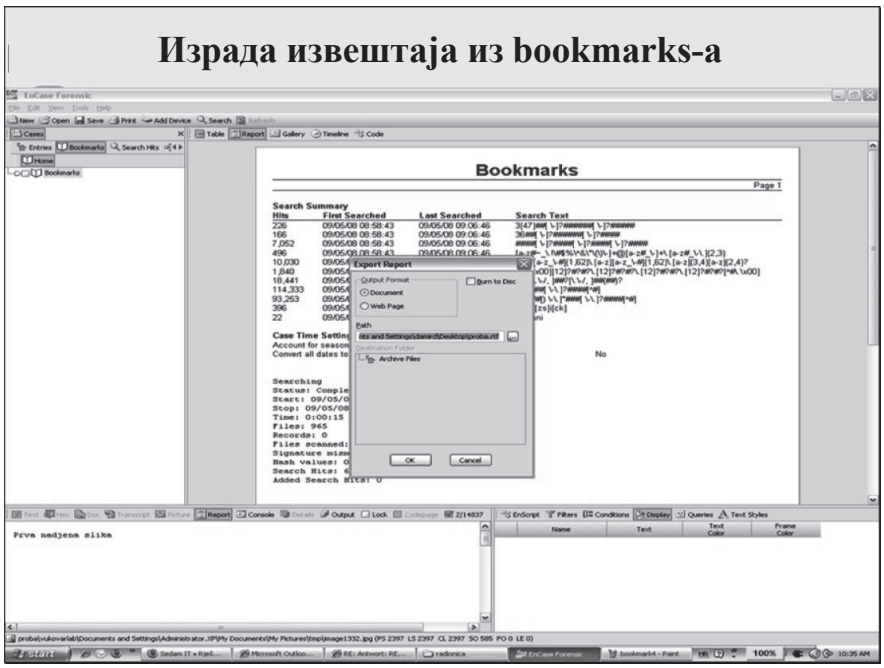


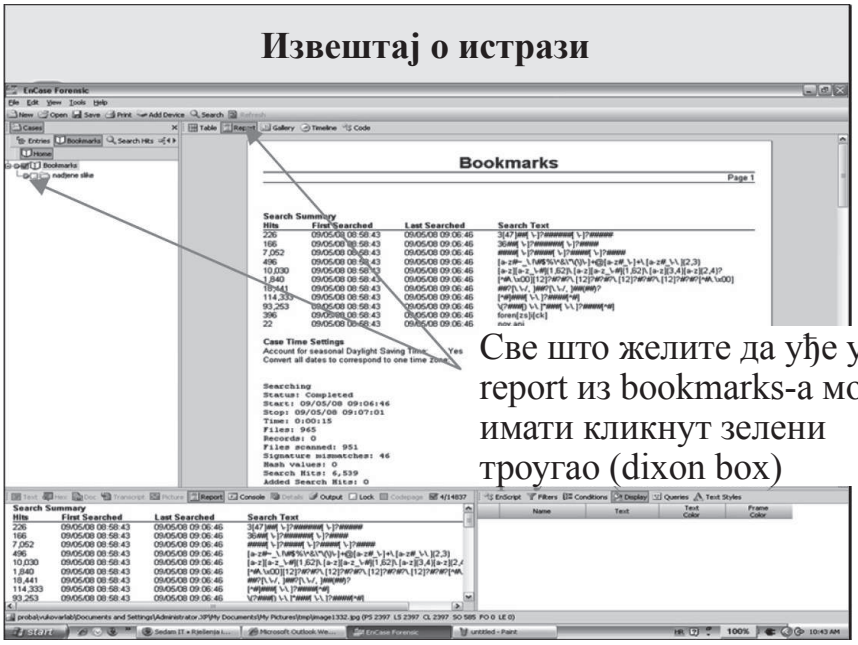
Резултати тражења у одабраним директоријумима





На основу забележеног направити извештај (report)





Закључак

У овом раду презентован је један од неопходних форензичких алата који, због својих изузетних, у раду побројаних, добрих особина, представља стандард у овој области.

У раду није експлицитно наглашена и његова евидентна мултифункционалност, која своју добру страну исказује, пре свега, у томе да је то алат који прави слику анализираног одредишта, али се исто тако користи и за каснију анализу и одговор.

Употреба форензичких алата, описаног EnCase или неког другог, постала је неопходна за детекцију инцидената и анализу рада сваког рачунарског система, били они предмет анализе полиције у владином сектору, или стручњака за безбедност у цивилном и корпоративном сектору. Како је већ наведено у раду, могућности самог оперативног система су у том смислу лимитиране.

Из разлога динамичног развоја EnCase алата (изласка нових верзија), у раду је, кроз приказ екрана побројаних опција, омогућено праћење (и поређење) ове са претходним али и новијим верзијама овог алата.

На крају, неопходно је напоменути да је овим радом обухваћено, пре свега у практичном приказу рада, до 25% и то основних могућности разматраног алата. Постоји и његова мрежна верзија:

- Enterprise,
- FIM (Field Investigation Module),

и она, као и поменути *enskript* језик за његова проширења, нису обухваћени овим радом, већ ће бити предмет посебног разматрања.

Литература:

1. Bishop, M., (2003), *Computer Security: Art and Science*, Addison-Wesley Professional.
2. Casey, E., (2004*)*, *Computer Crime Investigation Forensic Tools and Technology*, Elsevier Academic Press, London.
3. McClure, S., Scambray, J., Kurtz, G., (2006), *Хакерске тајне: заштита мрежних система,* (превод), Микро књига, Београд.
4. Ђорђевић Б., Плескоњић, Д., Мачек Н., (2006), *Оперативни системи: концепти*, Виша електротехничка школа, Београд.
5. Howard, M., Lipner, S., (2006), *The security development lifestyle*, Microsoft Press.
6. Jones, K., Shema, M., Johnson B., (2003), *Антихакерски алати*, (превод), Компјутер библиотека, Чачак.
7. Pastore, M., Dulaney, E., (2007), *Security* +, (prevod na hrvatski), Miš d.o.o., Загреб.
8. Плескоњић, Д., Ђорђевић, Б., Мачек, Н., Царић, М., (2006), *Сигурност рачунарских мрежа,* Микро књига, Београд.
9. Tanenbaum, A., (2005), *Рачунарске мреже*, (превод), Микро књига, Београд.
10. Tanenbaum, A., Woodhull, A., (1997), *Operating System Design and Implementation*, CRC Press Inc.
11. Security-info (sada Zaštita), br. 7/2006, elektronsko izdanje na http:// *www.security-info.biz/hr/e_dokumenti/časopis/*
12. *http://www.encase.com*, 2009.
13. *http://www.insig2.hr/racunalna-forenzika/encase/*, 2009.

EnCase forensic service tools

Abstract: *Computer or digital forensics is defined as a process of acquisition, memorizing, analysis, and presentation of digital evidence in the nature of digital data which can confirm that crime was committed and also establish connection between the criminal act and its perpetrator. Digital forensics uses hardware and software service tools and scientific methods for detecting digital*

data, their identification, evaluation, extracting, recovering, and analysis.

Digital forensics is a new field of science with growing interest in this subject matter, resulting in the fact that now, in USA only, there are a dozen universities providing specific education in this field.

This paper presents one of the most popular forensic service tools, named EnCase (from Guidance Software), which is widely used and accepted in jurisprudence of USA and EU.

Key words: *digital forensics, forensic hardware and software service tools.*