|  |
| --- |
| Regshot |
| Mateo Šimonović, 0036465116 |

**SADRŽAJ**

[1. Uvod 2](#_Toc406538216)

[2. Instaliranje i pokretanje programa 3](#_Toc406538217)

[3. Rad s programom 4](#_Toc406538218)

[4. Regshot u primjeni analize zloćudnih programa 8](#_Toc406538219)

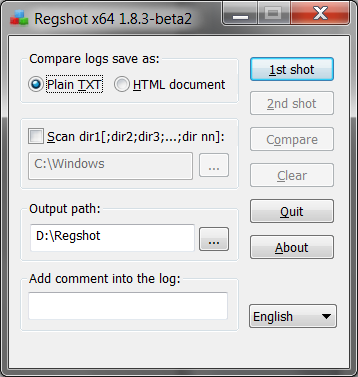
[5. Zaključak 12](#_Toc406538220)

[6. Literatura 13](#_Toc406538221)

# Uvod

Regshot je besplatan program otvorenog koda, pisan u jeziku C, kojeg su izvorno u siječnju 2001. godine na SourceForge web stranici predstavili M. Buecher, XhmikosR, i TiANWEi. To je jednostavan alat koji omogućuje snimanje kompletnog stanja registara sustava u dva vremenski odvojena trenutka te njihovo uspoređivanje. Od tog dana, program je doživio nebrojene modifikacije i ažuriranja radi poboljšanja svoje funkcionalnosti.

Regshot je program koji je vrlo jednostavno preuzeti, instalirati te na kraju i koristiti. Jednostavnost njegovog korištenja vidljiva je već iz izgleda njegovog grafičkog korisničkog sučelja prikazanog na slici 1.1.



Slika 1.1 - Osnovni prozor programa Regshot

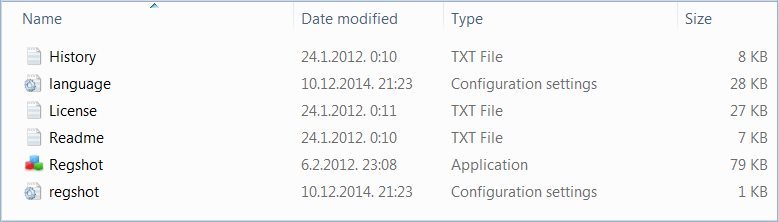
Regshotova glavna primjena je u mogućnosti snimanja svih registara računala u dva različita trenutka u vremenu. To je operacija koja naprednijim korisnicima računala omogućava pregled stanja registara nakon neke kritične ili nepoznate operacije. Primjerice, da bi se provjerilo da li instalacija nekog novog programa mijenja zapise u registrima koje ne bi smjela mijenjati, pogodno je pomoću Regshota snimiti stanje registara prije i nakon instalacije programa te dati mu naredbu da usporedi te zapise. Nakon usporedbe se u ispisu vide zapisi koji su dodani, obrisani te mijenjani iz čega se može vidjeti na što je instalacija utjecala.

U ovom projektu je predstavljen alat Regshot, od njegove instalacije do upotrebe s konačnim primjerima na kojima je detaljnije objašnjen njegov rad.

# Instaliranje i pokretanje programa

Program Regshot je vrlo jednostavno preuzeti s Interneta, instalirati te pokrenuti po prvi put. Postoji mnogo stranica s kojih se može preuzeti Regshot, ali najlakše je to napraviti direktno s SourceForge stranice Regshot projekta: <http://sourceforge.net/projects/regshot>.

Nakon preuzimanja zadnje inačice programa (trenutno 1.8.3), dovoljno je raspakirati dobivenu arhivu u željeni direktorij. Izgled direktorija programa Regshot nakon raspakiravanja prikazan je na slici 2.1. Regshot je jednostavan alat koji za svoje izvođenje ne zahtjeva klasičnu instalaciju, već se pokreće iz bilo kojeg željenog direktorija pokretanjem izvršne datoteke Regshot.exe.



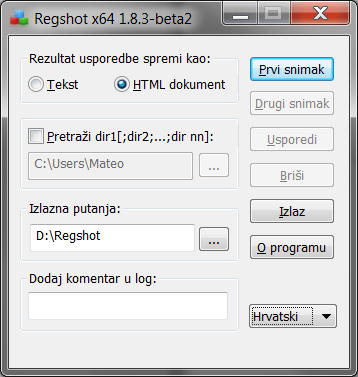
Slika 2.1 - Izgled direktorija programa nakon raspakiravanja

Sa slike je vidljivo da se nakon raspakiranja programa u željenom direktoriju osim datoteke za pokretanje alata nalaze još neke datoteke. Značenje pojedine datoteke objašnjeno je u nastavku.

* **History.txt** – sadrži opis svake inačice programa od verzije 1.01c do trenutno zadnje inačice uz nabrojene značajke programa koje su u svakoj inačici dodane, maknute te posebno naznačene značajke koje autori programa smatraju da bi korisnicima mogle biti korisne
* **language.ini** – sadrži prijevode svih tekstova u programu na 29 svjetskih jezika te program omogućuje izbor jednog od ponuđenih jezika. Ovu datoteku je moguće uređivati, iako nije preporučljivo.
* **License.txt** – sadrži opće uvjete korištenja pod kojima je program izdan
* **Readme.txt** – sadrži kratak opis i verziju programa, upute za njegovo korištenje te na kraju zahvale svim sudionicima na projektu i autorska prava
* **Regshot.exe –** izvršna datoteka za pokretanje samog alata
* **regshot.ini –** sadrži konfiguracijske postavke alata koje se spremaju u datoteku kako bi korisnika prilikom ponovnog pokretanja alata dočekale zadnje korištene postavke. Ovu datoteku moguće je uređivati u uređivaču teksta i učinak tih promjena vidljiv je prilikom sljedećeg pokretanja alata.

# Rad s programom

Rad s programom započinje pokretanjem izvršne datoteke *Regshot.exe* nakon čega se otvara prozor prikazan na slici 3.1. Na prozoru na slici je također jezik promijenjen na Hrvatski radi primjera na ovom projektu. U nastavku su detaljnije objašnjene sve komponente prikazanog prozora, a zatim i primjer njihovog korištenja.



Slika 3.1 - Osnovni prozor programa Regshot

Prva opcija koju Regshot nudi je odabir želimo li rezultat izvođenja programa (usporedbu registara dva različita vremenska trenutka) pohraniti u **tekstualnom** ili **HTML** formatu. Ukoliko je odabran *tekst* format, rezultat izvođenja generirat će običan tekstualni (.txt) dokument koji se može otvoriti u bilo kojem uređivaču teksta (Notepad, Sublime, Vim…), dok će odabirom *HTML dokument* opcije korisnik kao rezultat izvođenja dobiti web stranicu (.html) koja ima malo ljepši format od tekstualne datoteke i koja se može otvoriti u bilo kojem web pregledniku (Mozilla Firefox, Google Chrome…).

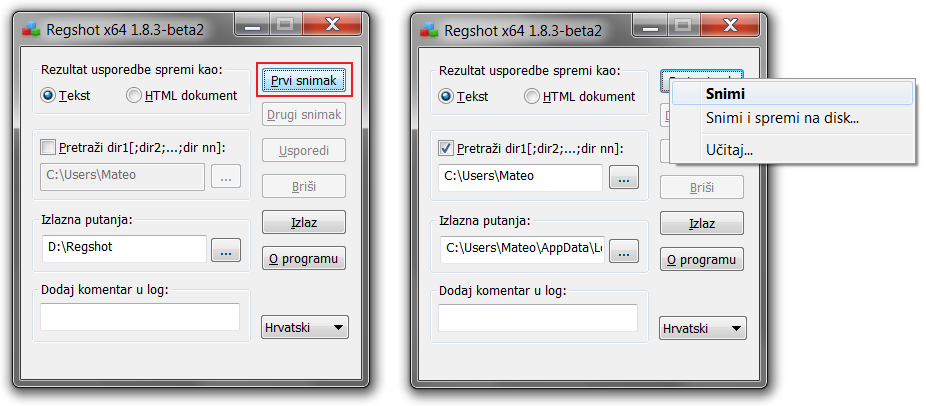
Sljedeća opcionalna kućica koju Regshot nudi je praćenje datotečnog sustava, točnije određenih direktorija u kojima korisnik očekuje promjene prilikom provođenja neke akcije a računalu. Regshot nudi odabir više direktorija, dovoljno ih je odvojiti znakom točka-zarez.

Sljedeće na redu je tekstualno polje za izbor izlazne putanje, odnosno direktorija gdje će se spremati sve datoteke nastale kao rezultat izvođenja programa. Ukoliko ova putanja nije navedena, Regshot uzima pretpostavljenu Windows putanju za privremene datoteke (npr. C:\Users\Mateo\AppData\Local\Temp).

Nakon toga, postoji okvir za opcionalni unos komentara u log. Komentar, za razliku od ostalih dijelova Regshot programa, ne utječe na izvođenje samog programa već se samo ispisuje napisani komentar u konačnu izlaznu datoteku kao pomoć korisniku radi lakšeg praćenja zbog čega je pokrenuo izvođenje programa, u kojim okolnostima i s kojim ciljem.

Glavna Regshotova funkcionalnost ostvaruje se najprije pritiskom na gumb *Prvi snimak*, što nudi tri opcije:

* Snimiti prvi snimak i sačuvati ga u memoriji kako bi ga se kasnije u radu mogao usporediti s drugim snimkom
* Snimiti prvi snimak, te ga osim u memoriju spremiti na disk radi moguće upotrebe u nekom kasnijem trenutku čak i nakon zatvaranja programa
* Učitavanje prethodno spremljenog snimka svih registara računala, datoteka se učitava s diska

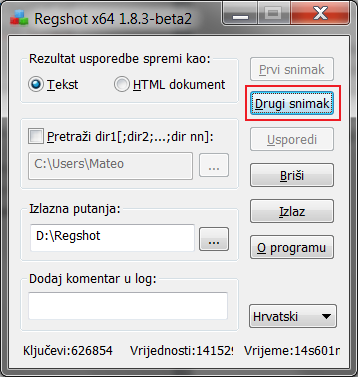


Slika 3.2 - Izvođenje prvog snimka

Nakon prvog snimka od korisnika se očekuje da napravi radnju za koju sumnja da prilikom svog izvršavanja na bilo koji način mijenja registre računala koje ne bi smjela. To može biti instalacija novog programa, pokretanje određenog programa, otvaranje određenih tipova datoteka, promjena postavki računala i niz drugih.

Na slici 3.3 je vidljivo stanje programa nakon prvog snimka. Program više ne dozvoljava odabir gumba prvog snimka već dozvoljava samo snimanje drugog snimka te brisanje trenutnog stanja. Osim toga, program ispisuje koliko je vremena bilo potrebno za prvo snimanje svih registara, te koliki je broj registarskih ključeva pritom spremljen. Iz ovih podataka se vidi da Regshot obavlja posao koji se ne može obaviti trenutno već se obavlja duži niz sekundi s obzirom da registarskih ključeva ima vrlo velik broj i da pored toga program mora posjetiti velik broj datoteka.

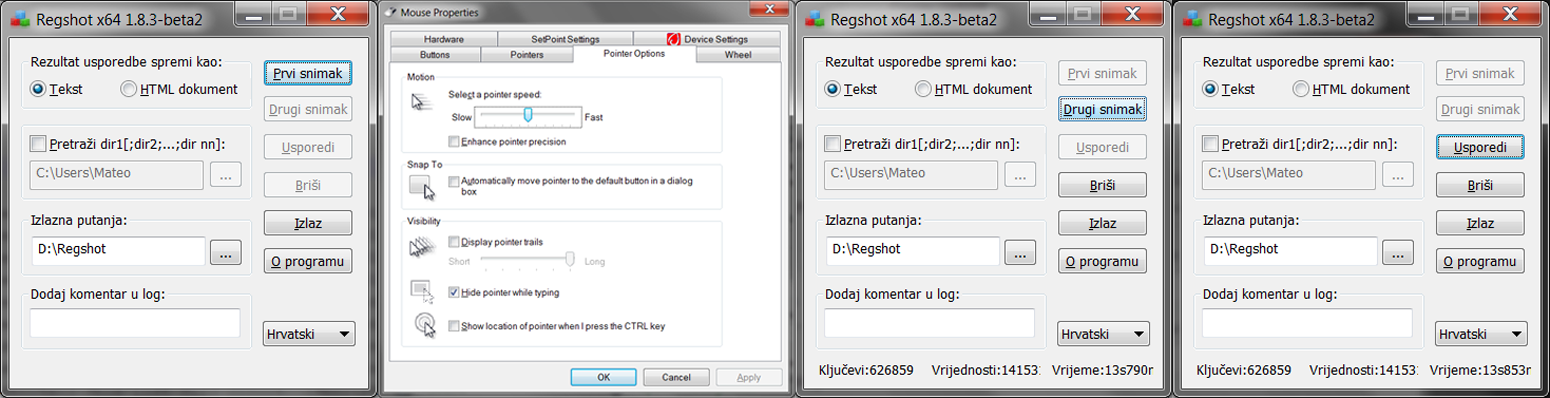
Sljedeći korak u analizi stanja registara je nakon obavljene kritične akcije na računalu, pritisnuti na Regshotu gumb *Drugi snimak* (slika 3.3.)što će pokrenuti istu akciju kao i kod odabira prvog snimka uz iste opcije: snimanje kompletnog novog stanja u radnu memoriju, snimanje stanja registara u memoriju uz dodatno spremanje na disk za kasnije učitavanje te zadnja opcija učitavanje prethodnog stanja registara iz datoteke spremljene na disku.



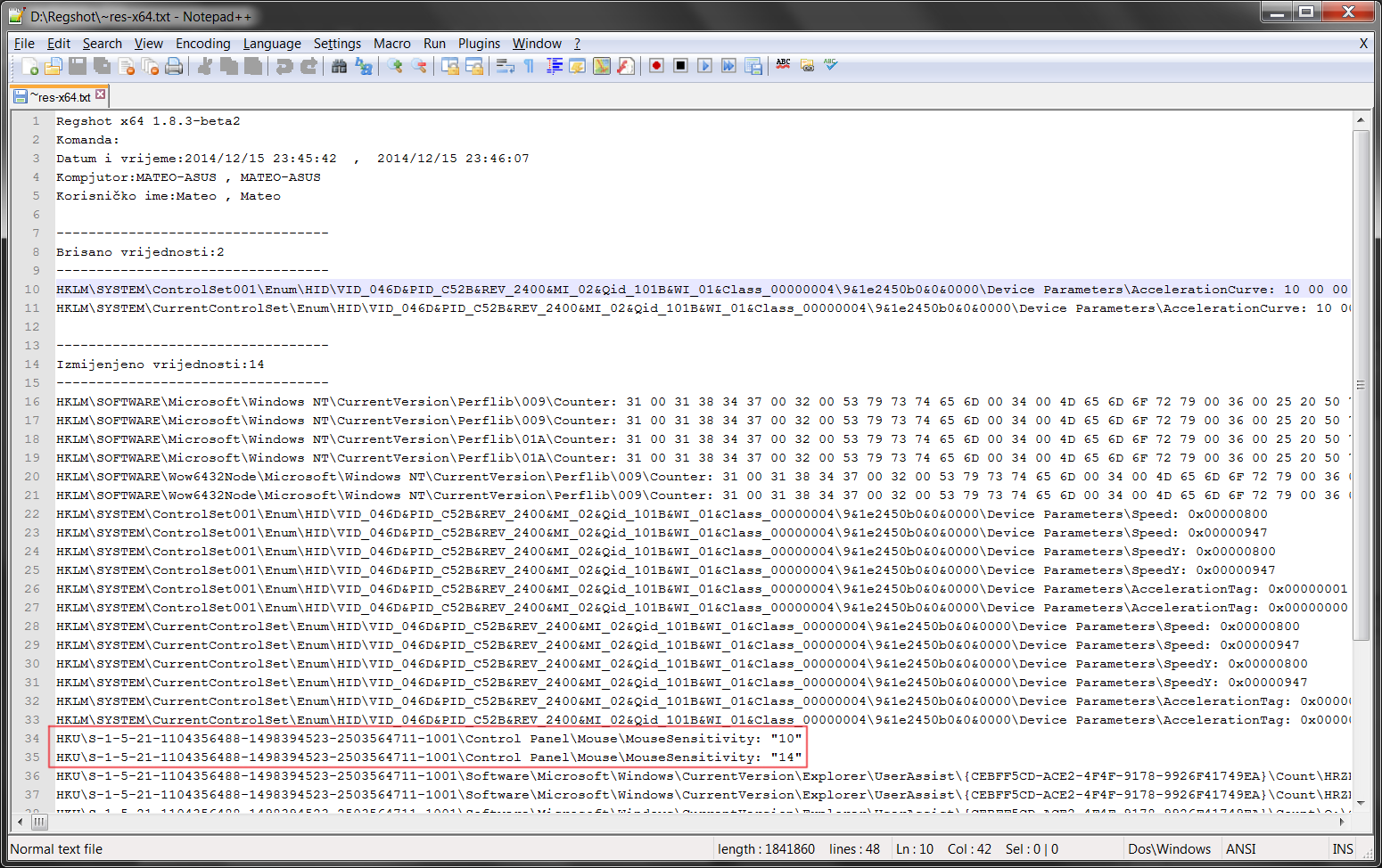
Slika 3.3 - Izvođenje drugog snimka

Nakon akcije učitavanja drugog snimka u memoriju, koje također traje nekoliko sekundi, korisnik ima opciju pokrenuti usporedbu prvog i drugog snimka i spremanje izlaznih rezultata u tekstualnu ili HTML datoteku klikom na gumb *Usporedi* nakon čijeg izvođenja se izlazna datoteka sprema u odabrani izlazni direktorij i automatski otvara.

Radi ilustracije rada s programom, odabran je jedan jednostavan primjer i na slikama 3.4. i 3.5 je prikazan rezultat izvođenja programa. Za demonstraciju rada programa Regshot kao kritična akcija sustava uzeta je akcija promjene osjetljivosti miša u upravljačkoj ploči. Na slici 3.4 su prikazani svi bitni koraci s kojima se do rezultata došlo. S obzirom da su postavke miša i tipkovnice jedna od stvari koje se pamte u registrima računala, ispis vidljiv u tekstualnoj datoteci na slici 3.5 upravo pokazuje očekivano ponašanje gdje se vidi kako je Regshot prilikom svog rada zabilježio promjenu osjetljivosti miša.



Slika 3.4 - Praćenje promjene osjetljivosti miša programom Regshot



Slika 3.5 – Primjer tekstualne izlazne datoteke

# Regshot u primjeni analize zloćudnih programa

Regshot je vrlo jednostavan program i ima jednu jednostavnu i vrlo jasno definiranu zadaću: usporedbu svih registara računala u dva vremenski odvojena trenutka. Upravo zbog toga to je jedan od alata koji računalni i programski inženjeri koriste u procesu analize **zloćudnih programa**. Pod pojmom zloćudni softver podrazumijeva se svaki računalni program koji ima za cilj oštećenje programa i podataka koji se nalaze na sustavu, širenje na druga računala, krađa podataka, prikazivanje reklamnih poruka i ostalih radnji za koje korisnik ne zna i na koje korisnik nije pristao.

U svrhu demonstracije rada Regshota u okruženju analize zloćudnih programa nažalost nije bilo moguće zaraziti neko računalo stvarnim zloćudnim softverom i pogledati što se koristeći Regshot može uočiti. U tu svrhu, napisan je jednostavan program u programskom jeziku Java koji je demonstracija rada jednog **trojanskog konja**. Trojanski konj je maliciozni program koji se predstavlja kao neki posve drugi program koji radi nešto korisno ili zanimljivo (npr. računalna igra), dok zapravo osim predstavljene funkcionalnosti u pozadini radi neku štetnu radnju, a to može biti i zauzimanje velike količine memorije kako bi korisniku usporio rad na računalu.

Programski kod u Javi koji je moguće vidjeti u nastavku ima vrlo jednostavnu funkcionalnost: kao argumente komandne linije prima putanje do dviju datoteka te datoteku dobivenu kao prvi argument kopira na putanju predanu kao drugi argument. Ono što korisniku nije vidljivo, a iz koda je jasno vidljivo, je da metoda ***kopiraj*** koja obavlja kopiranje ne radi samo ono za što je zadužena. U toj metodi se nalazi poziv sljedeće naredbe:

Programski odsječak 4.1 – naredba za dodavanje novog zapisa iz naredbenog retka

runtime**.**exec**(**"reg add HKEY\_CURRENT\_USER\\Software\\test /v dangerousKey /d dangerousValue"**);**

Ono što ta naredba radi je da iz pokreće iz komandne linije naredbe za dodavanje novog zapisa u registre računala, točnije u registar HKEY\_CURRENT\_USER\Software\test dodaje ključ *dangerousKey*  čiju vrijednost odmah postavlja na *dangerousValue*. Ova naredba je u danom primjeru sasvim bezazlena, računalu se dodaje novi registar pod imenom *test* u kojem se dodaje kompletno novi ključ s novom pridruženom vrijednosti. Svakako, ozbiljni maliciozni programi ne dodaju nove ključeve niti rade bezazlene akcije. Ozbiljan maliciozan program bi u ovom kontekstu mogao bez problema mijenjati vrijednosti ključeva registara koji su bitni drugim programima i na taj način promijeniti kojim se programima određene datoteke otvaraju ostavljajući korisniku dojam da mu određeni korisnički programi više „ne rade“. S obzirom da su u registrima zapisane računalu veoma bitne informacije za normalan radi, izmjenom vrijednosti bitnijih registara, maliciozan softver može vrlo naštetiti radu računala, pa i do te mjere da se sustav više ne može pokrenuti. Analiza danog programskog odsječka dana je u nastavku.

Programski odsječak 4.2 – Primjer malicioznog programa

package hr**.**fer**.**zemris**.**sigurnost**;**

**import** java**.**io**.**File**;**

**import** java**.**io**.**FileOutputStream**;**

**import** java**.**io**.**IOException**;**

**import** java**.**nio**.**file**.**Files**;**

public class KopirajDatoteku **{**

public static void main**(**String**[]** args**)** **{**

**if** **(**args**.**length **!=** 2**)** **{**

System**.**err**.**println**(**"Molimo predajte 2 argumenta prilikom pokretanja programa: izvorišnu i odredišnu datoteku"**);**

System**.**exit**(-**1**);**

**}**

File src **=** **new** File**(**args**[**0**]);**

File dest **=** **new** File**(**args**[**1**]);**

**if** **(!**src**.**exists**())** **{**

System**.**err**.**println**(**"Izvorišna datoteka ne postoji. Molimo predajte postojeću datoteku!"**);**

System**.**exit**(-**1**);**

**}**

System**.**out**.**println**();**

System**.**out**.**println**(**"Izvorišna datoteka: " **+** src**.**getName**());**

System**.**out**.**println**(**"Odredišna datoteka: " **+** dest**.**getName**());**

System**.**out**.**println**(**"\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_"**);**

System**.**out**.**println**();**

**try** **{**

kopiraj**(**src**,** dest**);**

**}** **catch** **(**IOException e**)** **{**

System**.**err**.**print**(**"Datoteke nisu uspješno kopirane. Opis pogreške: " **+** e**.**getMessage**());**

**}**

System**.**out**.**println**(**"Vaša datoteka " **+** src**.**getName**()** **+** " je uspješno kopirana u datoteku " **+** dest**.**getName**());**

**}**

private static void kopiraj**(**File src**,** File dest**)** **throws** IOException **{**

System**.**out**.**println**(**"kopiranje u tijeku.."**);**

Files**.**copy**(**src**.**toPath**(),** **new** FileOutputStream**(**dest**));**

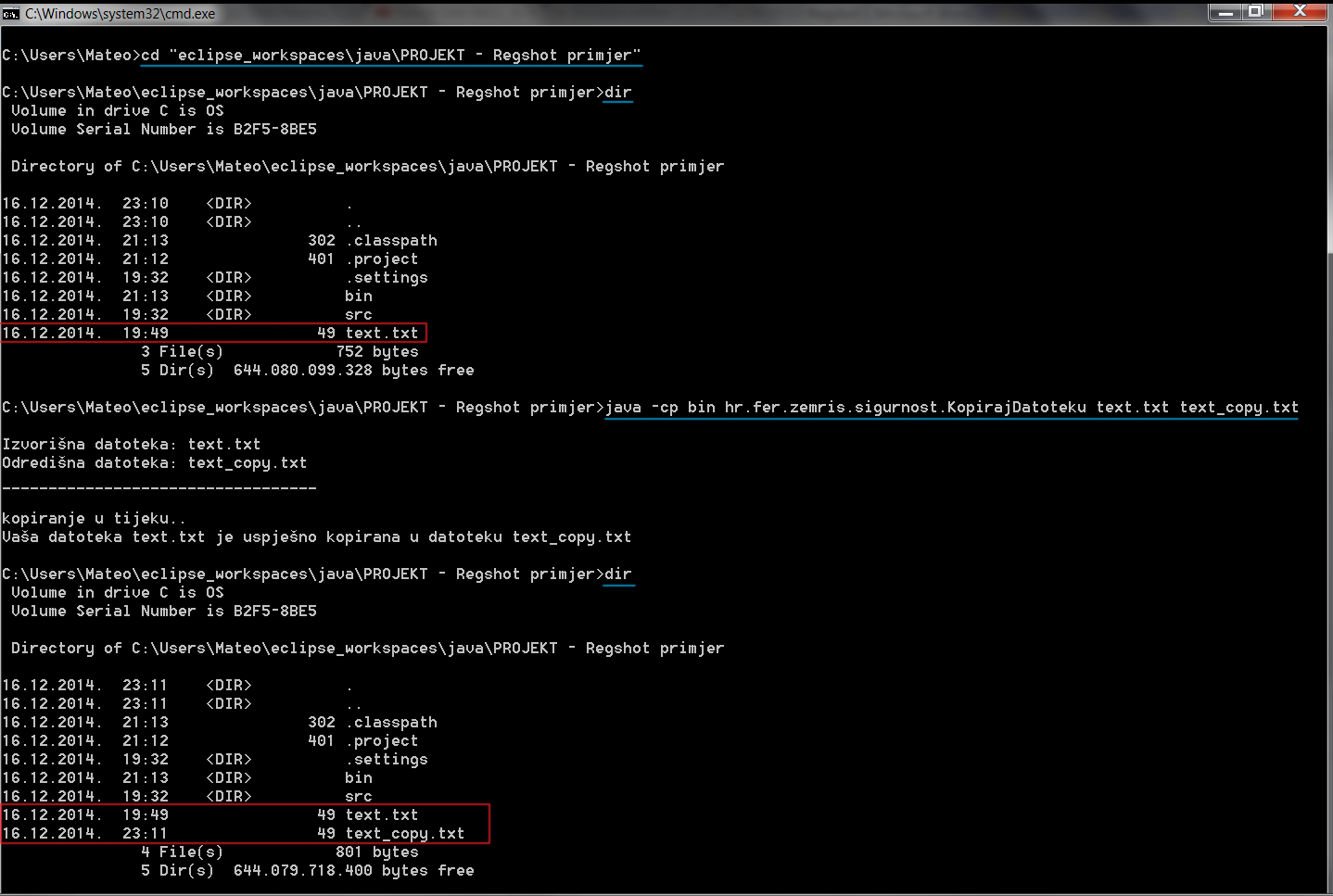
Runtime runtime **=** Runtime**.**getRuntime**();**

runtime**.**exec**(**"reg add HKEY\_CURRENT\_USER\\Software\\test /v dangerousKey /d dangerousValue"**);**

**}**

**}**

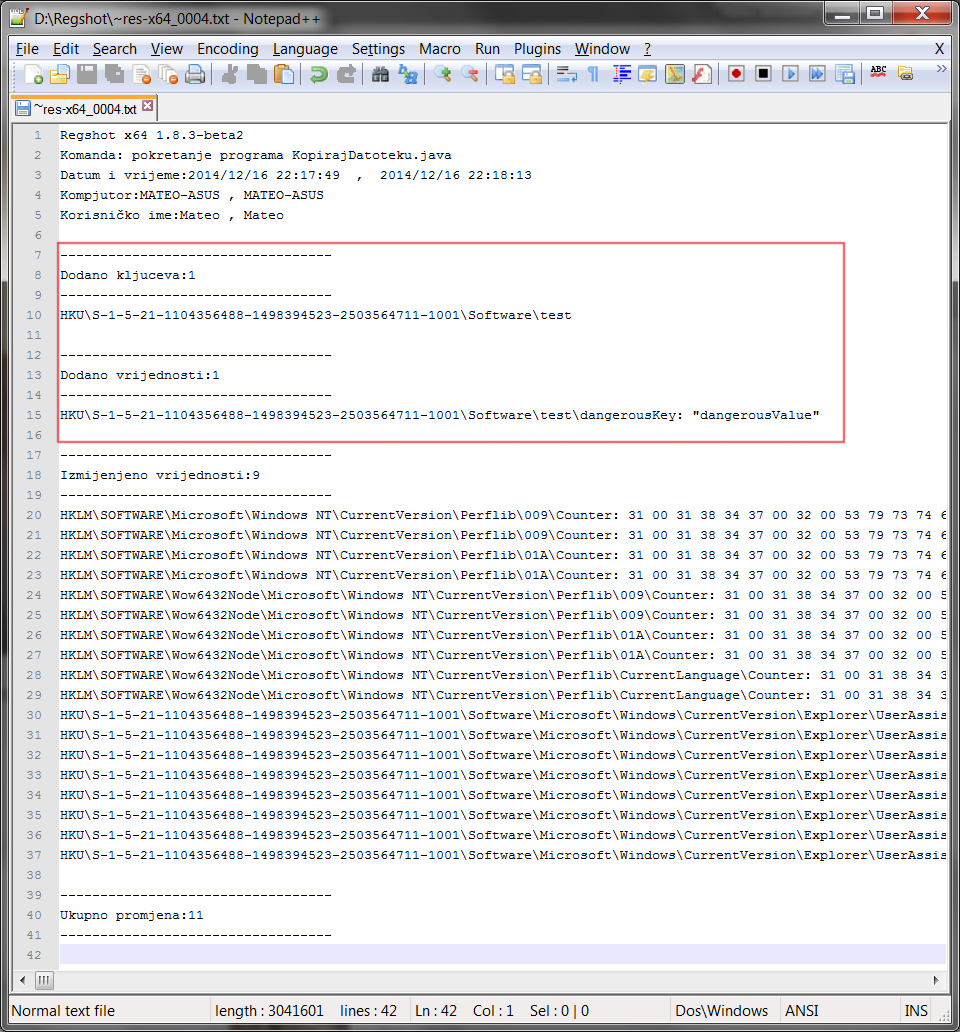
Analiza danog programskog odsječka uporabom programa Regshot odrađena je na sljedeći način. Programom regshot je najprije u mirnom stanju sustava snimljen prvi snimak registara računala kao što je prethodno pokazano. Nakon toga je iz naredbenog retka pokrenut program KopirajDatoteku.java koji je uredno završio svoje izvođenje i korisniku dojavio da je kopiranje uspješno završeno, što je vidljivo na slici 4.1. Na slici su plavom bojom podcrtane naredbe koje je korisnik unio u naredbeni redak prilikom pokretanja testnog programa. Na slici je također crvenom bojom prikazano stanje direktorija prije izvođenja programa i nakon izvođenja programa kako bi se pokazalo da je datoteka *text.txt* uistinu kopirana u datoteku *text\_copy.txt* baš kao što je to korisnik tražio.



Slika 4.1 – Prikaz izvođenja programa KopirajDatoteku.java

Na sljedećoj slici prikazani su rezultati dobiveni iz programa Regshot. Regshot je korišten na standardan način: napravljena je prva snimka stanja registara prije pokretanja programa *KopirajDatoteku.java* te je nakon završetka izvođenja programa napravljena druga snimka stanja registara. Nakon toga je pokrenuta usporedba dvaju stanja i rezultati analize su spremljeni u tekstualnom formatu.

Rezultati analize prikazani su na slici 4.2. Vidljivo je da je program Regshot pokrenut dvaput u vremenskom intervalu manjem od minute, s obzirom da je bio cilj uhvatiti samo vrijeme izvođenja programa *KopirajDatoteku.java* i ništa drugo. Također, vidljivo je da je naredba ***reg add***stvorila novi ključ *test* s obzirom a prethodno nije postojao (u suprotnom ne bi bio napravljen), te njemu pridijelila vrijednost: dangerousKey=“dangerousValue“, točno što je dani program i napravio. Ostali prikazani registri su rezultat normalnog izvođenja operacijskog sustava Windows.



Slika 4.2 - Rezultat analize registara prije i nakon izvršavanja programa KopirajDatoteku.java

# Zaključak

Regshot je vrlo jednostavan alat koji pruža jednu funkcionalnost i adekvatno ju ispunjava. On omogućava praćenje promjena nad registrima računala prilikom izvršavanja određene kritične akcije na računalu. Ta akcija može biti vrlo jednostavna, kao što su promjene korisničkih opcija u Upravljačkoj ploči ili postavljanje varijabli okruženja, ali i vrlo komplicirana poput instalacije novog uređaja, novog sklopovlja i prikladnog pokretačkog programa ili raznih promjena na operacijskom sustavu.

Svakako postoje programi, kao što je Process Monitor, koji su daleko složeniji, brži i puno detaljnije prate promjene na registrima računala i mogu to raditi kontinuirano. Međutim, Regshot je program od kojeg neiskusni korisnik može krenuti kako bi naučio više o registrima, pogledao da li instalacija novog sumnjivog programa utječe na registre na koje ne bi smjela utjecati ili bilo koji sličan zahvat na računalu. Potpuno je besplatan i otvorenog je koda, što znači da svatko na njemu može napraviti promjene koje bi htio, te autori programa to i toplo podupiru. Svoju prednost krije u jednostavnosti za korištenje, ima vrlo detaljno opisanu *Readme* datoteku iz koje svatko može naučiti sve što je potrebno da bi započeo korištenje programa.

Jedna od namjena ovakvih alata je i u analizi zloćudnih programa. Zloćudne programe je često vrlo teško detektirati, njih je s korisničke razine korištenja sustava najčešće nemoguće vidjeti jer oni svoj posao rade u pozadini. Stoga je jedan od načina za detektiranje takvog tipa programa upravo praćenje promjena u registrima računala. Registri su vrlo važna komponenta operacijskog sustava jer su u njima zapisani svi operacijskom sustavu važni podaci i promjenom neke od bitnijih vrijednosti registara može se računalo dovest u stanje da se više ne može niti pokrenuti. U ovom projektu je za potrebe demonstracije rada s alatom prikazan jedan programski kod koji ne predstavlja točnu definiciju zloćudnog programa, ali to je svakako program koji osim deklarirane funkcionalnosti radi operacije koje korisniku nisu poznate niti vidljive. Uporabom programskog alata Regshot takvo je ponašanje vrlo brzo uočeno i korisnik može brzo shvatiti da to nije program koji želi dalje koristiti i kojem želi vjerovati.

# Literatura

1. Readme datoteka - <http://sourceforge.net/projects/regshot/>
2. REG.exe, dokumentacija naredbe „reg“ <http://ss64.com/nt/reg.html>
3. How to Use Regshot To Monitor Your Registry, How-To Geek, <http://www.howtogeek.com/198679/how-to-use-regshot-to-monitor-your-registry/>
4. Windows Registry, Everything You Need To Know, Gammadyne Corp., <http://www.gammadyne.com/registry.htm>
5. Zloćudni softver, Wikipedia, <http://hr.wikipedia.org/wiki/Zloćudni_softver>