CARNET

HxD

CERT.hr-PUBDOC-2019-3-376

CERT.hr

Sadržaj

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

1 Uvod

Gotovo svi korisnici računala su se susreli s nizom različitih vrsta datoteka – od tekstualnih dokumenata, prezentacija i proračunskih tablica pa do raznih vrsta slika, arhiva i izvršnih datoteka. Iako se takve različite vrste datoteka znatno razlikuju po funkciji, one su sve u konačnici pohranjene binarno, tj. u obliku niza nula i jedinica. Te nule i jedinice nazivaju se bitovi, te se oni obično grupiraju u bajtove – grupe od osam bitova.

Taj binarni zapis skriven je od krajnjeg korisnika, jer je interpretacija takvog zapisa obično prilično složena. Korisnika taj binarni zapis obično ne treba opterećivati – dovoljno je da korisnik zna raditi s datotekama kroz odgovarajuće programe više razine. Primjerice, dovoljno je da korisnik zna uređivati tekstualne dokumente programom kao što je *Microsoft Word* ili *LibreOffice Writer*. Obično nije potrebno znati kako se ti tekstualni dokumenti u konačnici pohranjuju u obliku nula i jedinica.

No, postoje situacije kad je poželjno izravno pregledati ili čak uređivati binarni zapis datoteke, primjerice:

- kada korisnika zanimaju podaci koje uobičajeni alati ne prikazuju,
- kada je datoteka oštećena i ne može se otvoriti uobičajenim alatima,
- kada je format datoteke nepoznat.

Za pregled i uređivanje binarnog zapisa datoteka često se koriste tzv. heksadekadski uređivači (engl. *hex editor*). Ti se alati nazivaju tako zato što prikazuju binarni zapis (niz nula i jedinica) pomoću heksadekadskih znamenaka, što može znatno olakšati njegovu interpretaciju. Za rad s heksadekadskim uređivačima potrebno je biti vješt u pretvaranju brojeva iz binarnog u heksadekadski sustav i obrnuto, te je potrebno znati kako interpretirati takve zapise. Pored toga, ponekad treba i znati pretvarati brojeve između heksadekadskog i dekadskog sustava, te interpretirati heksadekadske znakove prema sustavima kodiranja ASCII ili Unicode. Zbog toga, u usporedbi s uobičajenim korištenjem računala, pregledavanje i uređivanje datoteka pomoću heksadekadskih uređivača prilično je napredna vještina.

HxD je jedan od najpopularnijih uređivača heksadekadskih zapisa za Microsoft Windows operacijske sustave. HxD je besplatan, brz, jednostavan za korištenje i podržava rad sa svim datotekama, neovisno o njihovoj veličini. HxD-om je moguće i uspoređivati datoteke, računati njihovu kontrolnu sumu (engl. *checksum*) i sigurno brisati datoteke s računala. Uz sve navedeno, HxD pruža i niz naprednih mogućnosti poput pregledavanja i uređivanja sadržaja radne memorije, diskova ili snimki diskova, zbog čega može pomoći primjerice i pri rekonstrukciji obrisanih datoteka.

HxD je jednostavan za instalaciju te se oko njega razvila zajednica korisnika koja aktivno sudjeluje u odgovaranju na pitanja na službenim stranicama alata. Također, i sam proizvođač aktivan je u odgovaranju na korisničke upite i probleme.

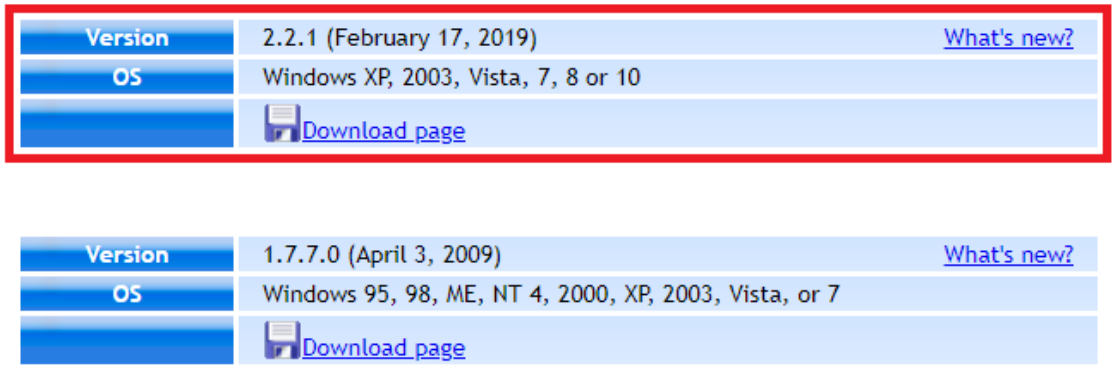
U ovom dokumentu bit će opisana instalacija i osnovno korištenje alata HxD.

2 Instalacija alata HxD

Alat HxD razvio je Maël Hörz i može se besplatno preuzeti s njegove službene stranice.

HxD se trenutno može koristiti isključivo na Microsoft Windows operacijskim sustavima. U nastavku će instalacija biti demonstrirana na operacijskom sustavu Windows 10, no postupak je sličan i na ostalim Windows operacijskim sustavima.

Kao što je prikazano na slici 2.1., za preuzimanje su dostupne dvije inačice, jedna za starije i jedna za novije Windows operacijske sustave. U slučaju instalacije na Windows 10, potrebno je odabrati noviju inačicu (u trenutku pisanja ovog dokumenta to je HxD 2.2.1) i kliknuti na ***Download page***.



Slika 2.1. Inačice HxD alata dostupne za preuzimanje

Otvorit će se stranica s prikazanim izborom jezika na kojima je moguće instalirati i koristiti alat. Potrebno je odabrati željeni jezik i zatim kliknuti na ***Download per HTTPS***. Oko HxD-a je okupljena velika zajednica korisnika koja je pomogla u prevođenju alata na više stranih jezika, ali trenutno ne postoji inačica alata na hrvatskom jeziku. Umjesto hrvatskog, može se odabrati npr. engleski jezik kao što je prikazano na slici 2.2.

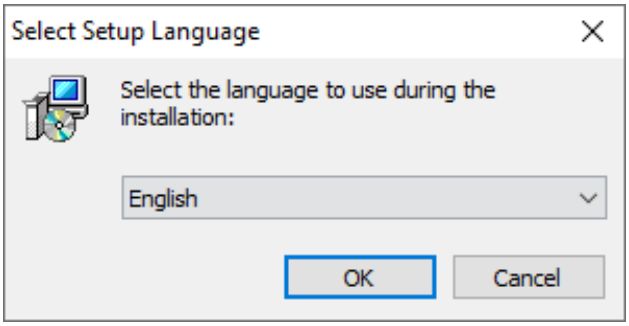
Product	Edition	Version	Translator	Release date		File signatures
HxD20, Chinese (simplified)	installable (can create portable)	2.2.1	何志翔	February 17, 2019	Download per HTTPS 3 MiB	SHA-1 and SHA-512
HxD20, Chinese (traditional)	installable (can create portable)	2.2.1	VincentLu@TW	February 17, 2019	Download per HTTPS 3 MiB	SHA-1 and SHA-512
HxD20, German	installable (can create portable)	2.2.1	Maël Hörz	February 17, 2019	Download per HTTPS 3 MiB	SHA-1 and SHA-512
HxD20, English	installable (can create portable)	2.2.1	Maël Hörz	February 17, 2019	Download per HTTPS 3 MiB	SHA-1 and SHA-512
HxD20, Spanish	installable (can create portable)	2.2.1	Emmanuel Carrara	February 17, 2019	Download per HTTPS 3 MiB	SHA-1 and SHA-512
HxD20, French	installable (can create portable)	2.2.1	Le Ch@land	February 17, 2019	Download per HTTPS 3 MiB	SHA-1 and SHA-512
HxD20, Italian	installable (can create portable)	2.2.1	Costantino Grana	February 17, 2019	Download per HTTPS 3 MiB	SHA-1 and SHA-512

Slika 2.2. Odabir željenog jezika

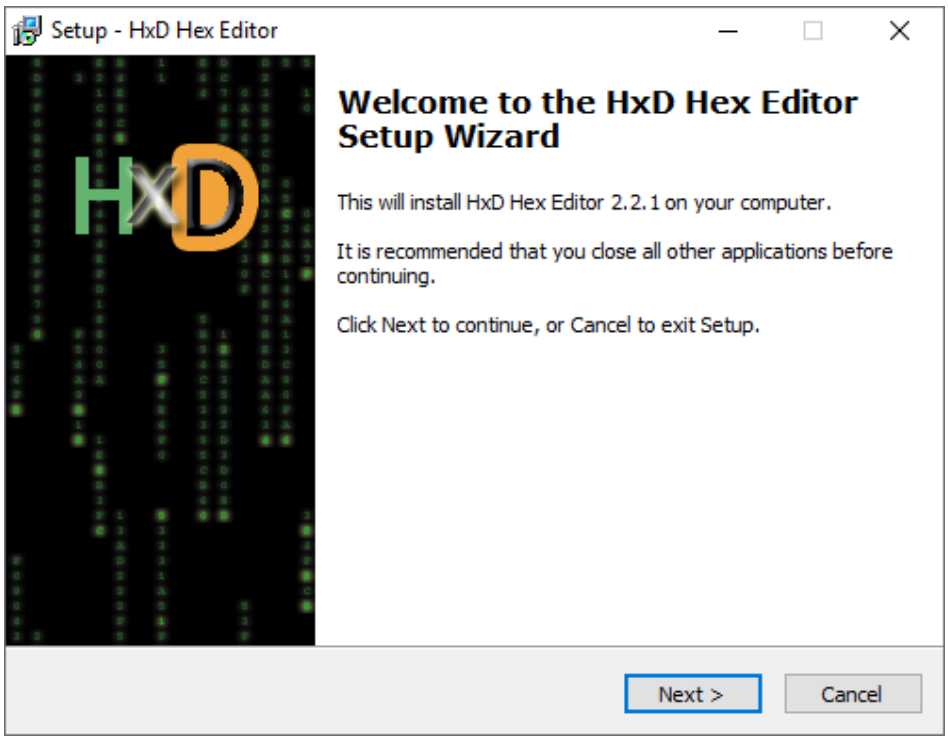
Za napredne korisnike, u zadnjem se stupcu nalazi i *File Signature* – kriptografski sažetak (engl. *hash*) kojim je moguće provjeriti je li ispravno preuzeta instalacijska datoteka.

Nakon preuzimanja, potrebno je raspakirati preuzetu zip arhivu („HxDSetup.zip“) i pokrenuti izvršnu datoteku koja se u njoj nalazi („HxDSetup.exe“).

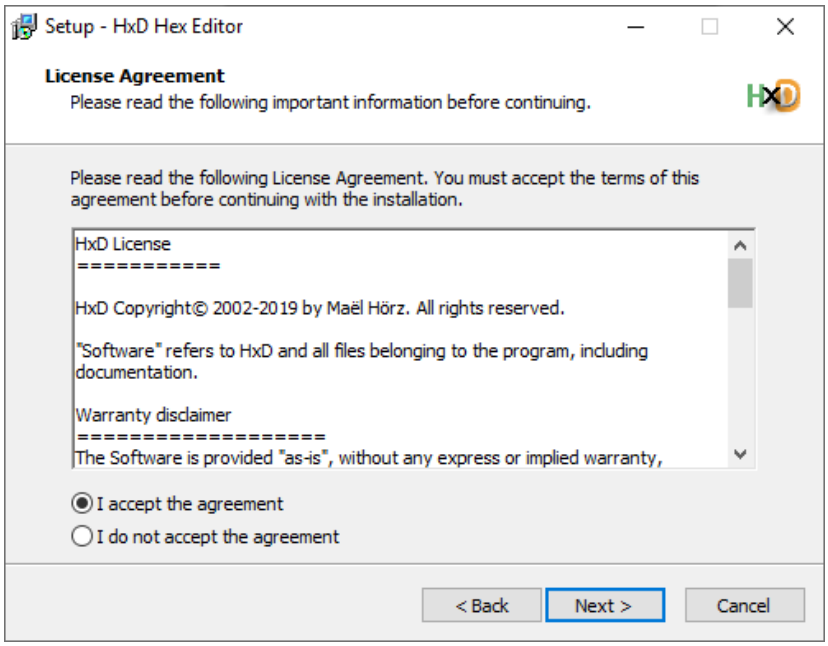
Na slikama 2.3. – 2.10. prikazani su početni koraci instalacije koji uključuju biranje jezika instalacije i prihvaćanje uvjeta korištenja.



Slika 2.3. Odabir jezika instalacije



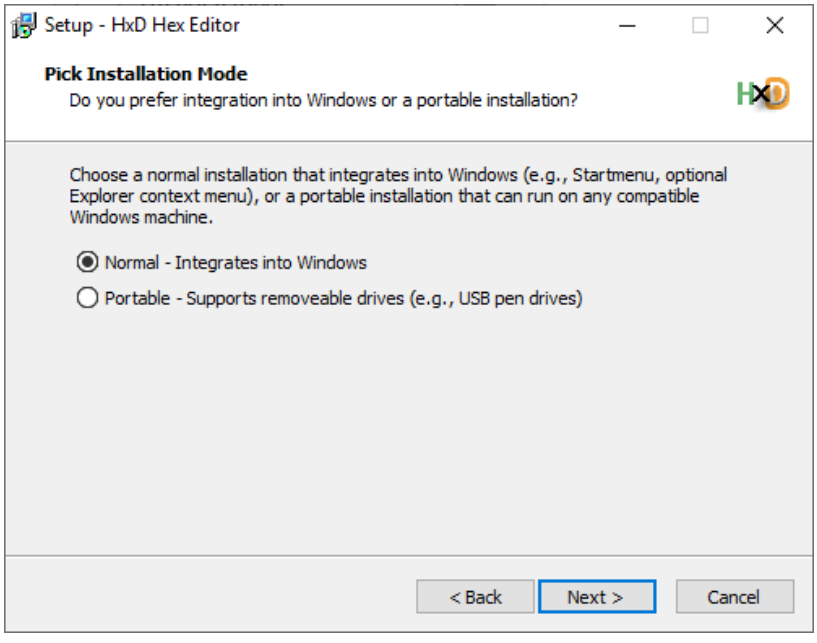
Slika 2.4. Pokretanje instalacije



Slika 2.5. Prihvaćanje uvjeta korištenja

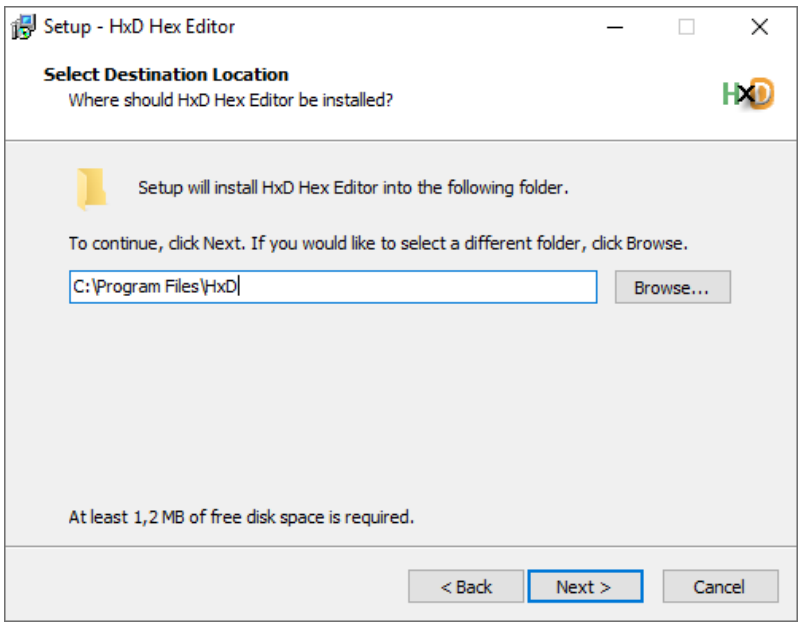
Zatim se pojavljuje prozor u kojemu se bira način instalacije. Razlikuju se uobičajena (engl. *normal*) i prijenosna (engl. *portable*) instalacija. U većini slučajeva, korisnici jednostavno žele instalirati HxD na svoje računalo, te je za to preporučljivo koristiti uobičajenu instalaciju. S druge strane, prijenosna instalacija korisna je kada korisnik želi koristiti HxD na više različitih računala bez da svaki put pokreće instalacijski proces. Tada se HxD može primjerice prijenosno instalirati na USB *stick*, pa se taj USB *stick* zatim može priključiti na bilo koje računalo, te se s njega u konačnici može pokrenuti prijenosno instalirani HxD.

Kao što je prikazano na slici 2.6., u ovom slučaju će se koristiti uobičajena instalacija.



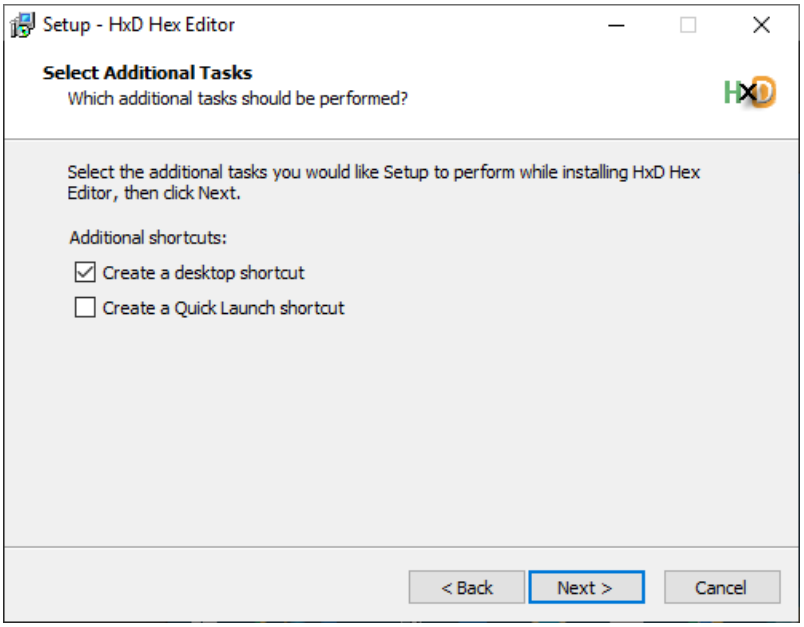
Slika 2.6. Odabir načina instalacije (obična instalacija ili prijenosna)

Prilikom odabira mape na datotečnom sustavu u koju će se instalirati HxD, preporučljivo je ostaviti zadanu mapu (*Program Files*) kao što je prikazano na slici 2.7. Naravno, može se proizvoljno odabrati i neka druga mapa.



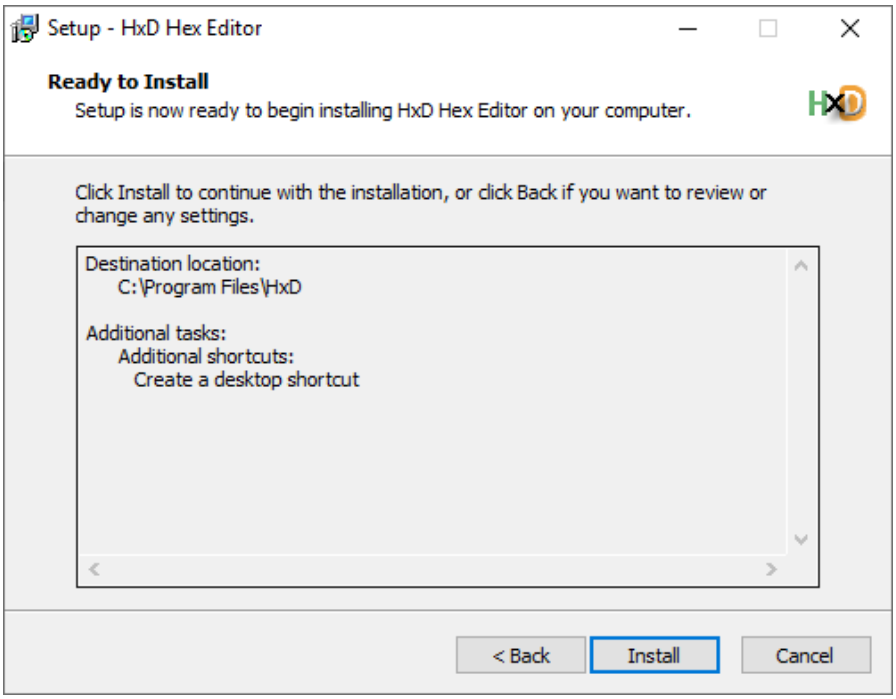
Slika 2.7. Odabir mape u koju će se instalirati HxD

Dodatne mogućnosti prilikom instalacije koje HxD nudi su stvaranje prečaca (engl. *shortcut*) na radnoj površini (engl. *desktop*) i stvaranje prečaca za brzo pokretanje (engl. *Quick Launch shortcut*).

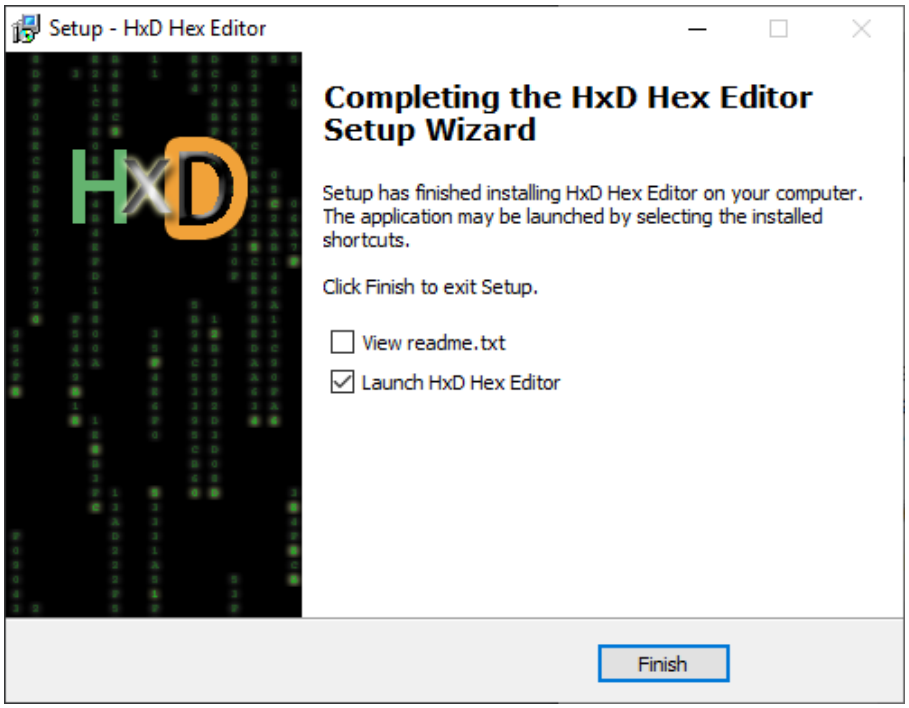


Slika 2.8. Dodatne mogućnosti prilikom instalacije

Zatim slijedi potvrda odabranih postavki, sama instalacija te obavijest o uspješnoj instalaciji, nakon čega je HxD spreman za korištenje.



Slika 2.9. Potvrda odabranih postavki i pokretanje instalacije

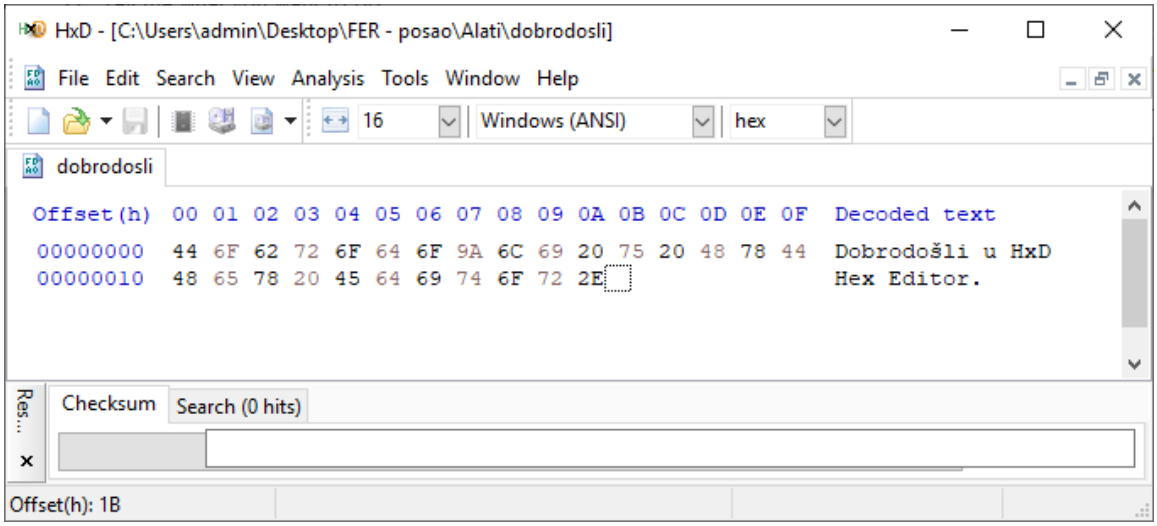


Slika 2.10. Obavijest o uspješnoj instalaciji

3 Korištenje alata HxD

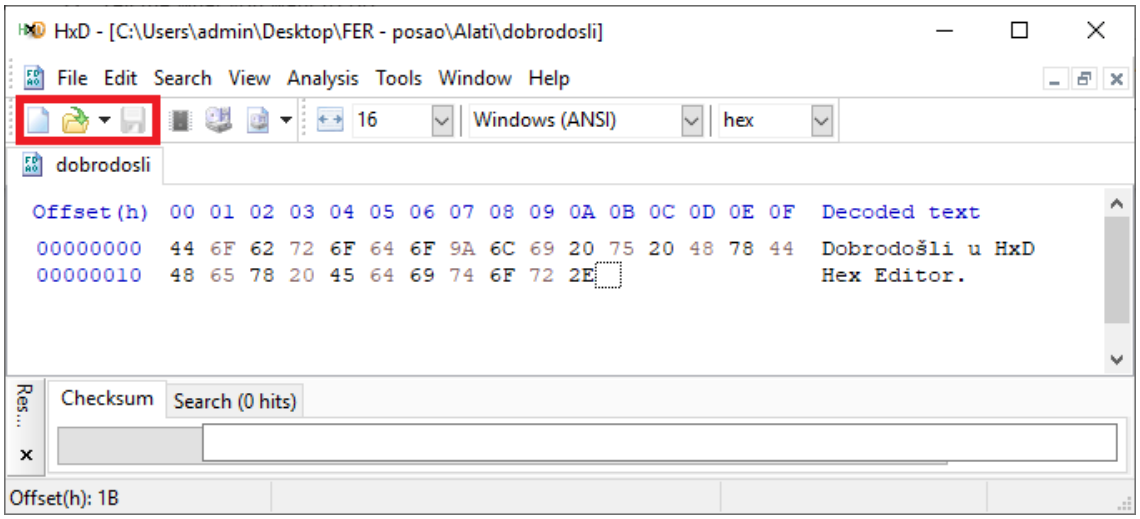
3.1 Sučelje HxD-a

Prije početka rada, korisno je upoznati se sa sučeljem HxD-a i mogućnostima koje on nudi. Na slici 3.1.1. vidljivi su različiti izbornici i postavke te heksadekadski i tekstualni prikaz sadržaja datoteke.



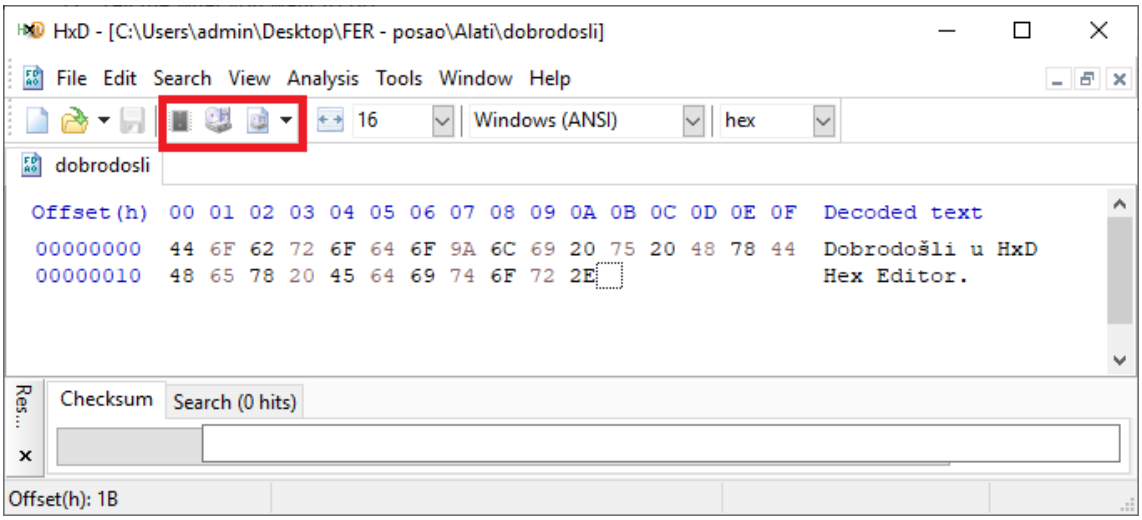
Slika 3.1.1. Sučelje HxD-a

Niz ikona istaknut na slici 3.1.2. odnosi se na uobičajene operacije s datotekama – stvaranje, otvaranje i pohrana datoteke.



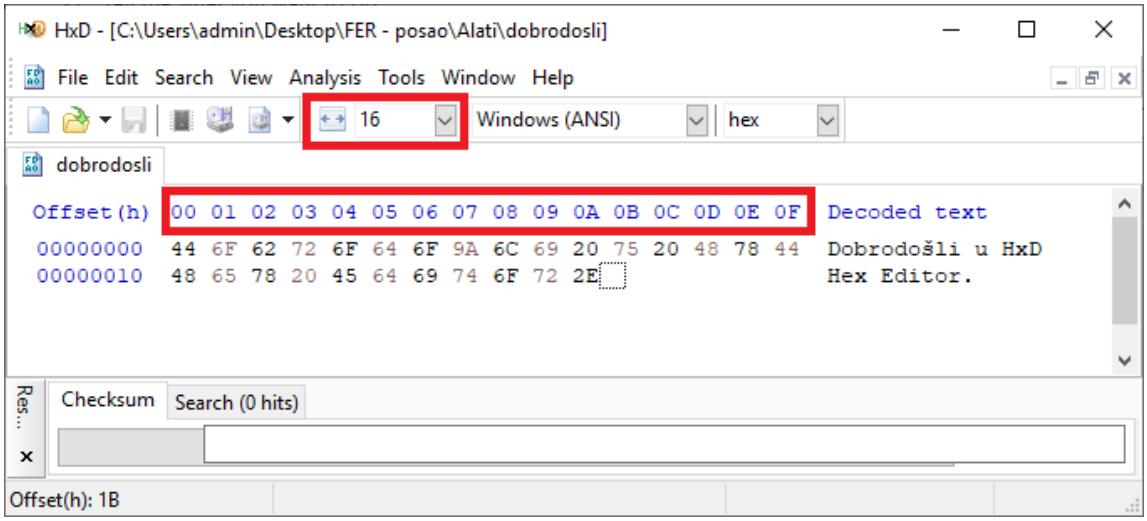
Slika 3.1.2. Ikone za uobičajene operacije s datotekama

Na slici 3.1.3. istaknute su ikone za napredne funkcionalnosti – pregled radne memorije koju koristi neki od pokrenutih procesa, pregled diska i pregled snimke diska (engl. *disk image*).



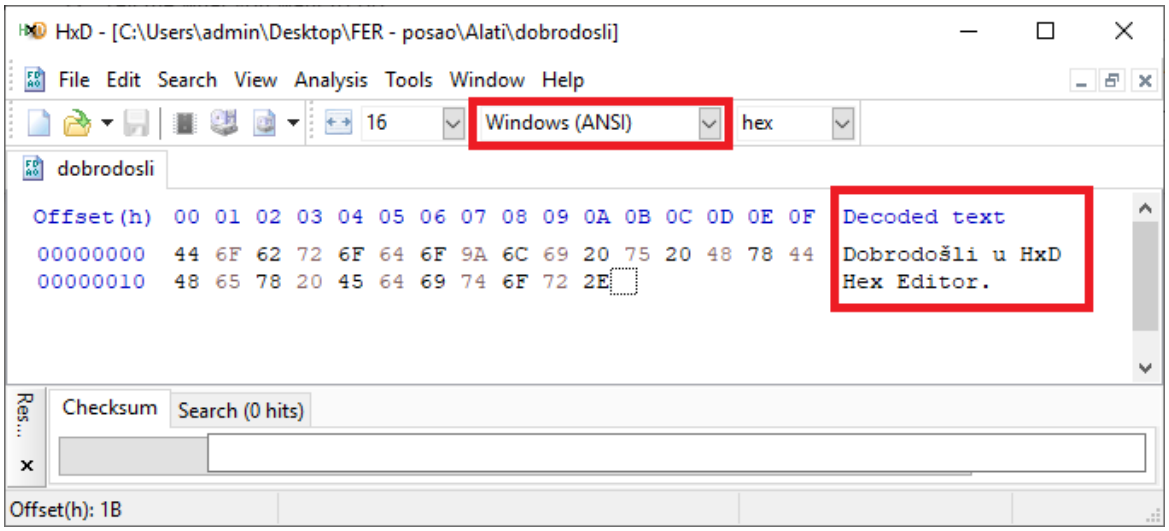
Slika 3.1.3. Ikone za napredne funkcionalnosti

Zatim slijedi dio sučelja u kojem je moguće ili odabrati fiksan broj bajtova koji će biti prikazan u jednom retku, ili postavku ***Adapt to window width*** koja će prikazati onoliki broj bajtova u jednom retku koliko stane u širinu prozora. Na slici 3.1.4. definiran je prikaz 16 bajtova po retku.



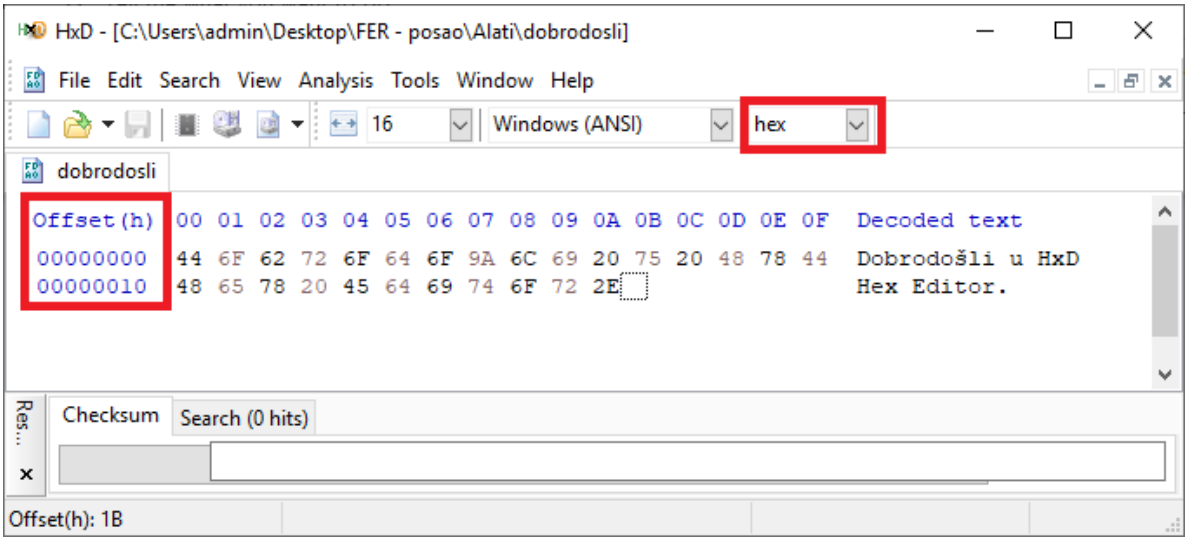
Slika 3.1.4. Definiranje broja prikazanih bajtova po retku

Slijedi odabir načina na koji će HxD tekstualno prikazivati binarni zapis datoteke. Na slici 3.1.5. prikazan je odabir formata „Windows (ANSI)“.

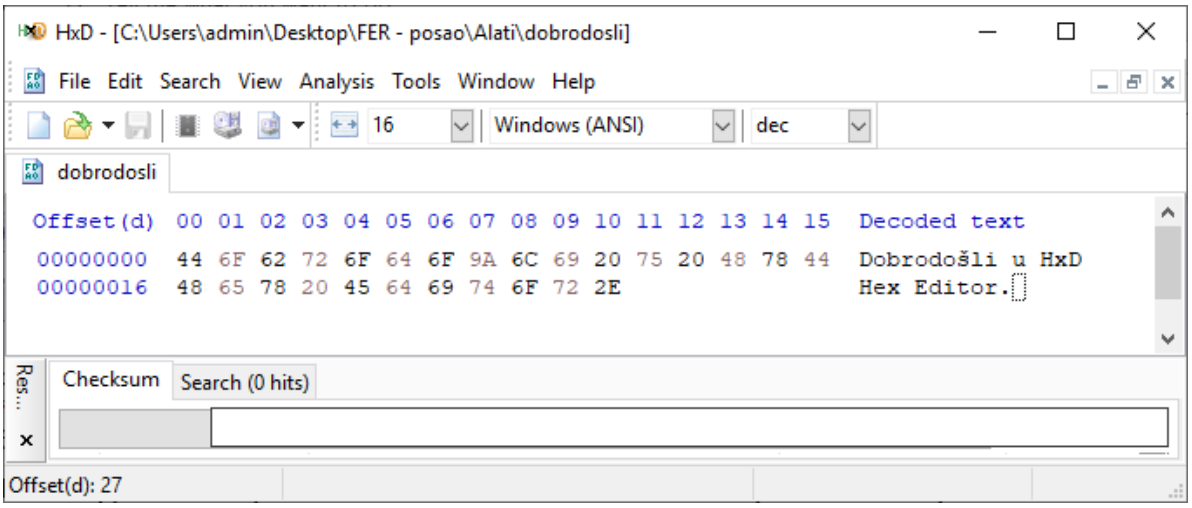


Slika 3.1.5. Tekstualni prikaz binarnog zapisa datoteke

Kako HxD nema ograničenje na veličinu datoteke koja se u njemu pregledava, nije rijetka pojava da prikaz datoteke ima i milijarde redaka bajtova. Zato je korisno znati snalaziti se s postavkama prikaza odmaka (engl. *offset*) koji prikazuje poziciju retka bajtova u datoteci. Na slikama 3.1.6. i 3.1.7. vidljiv je odabir prikaza odmaka u heksadekadskom (oznaka ***h***) odnosno dekadskom (oznaka ***d***) formatu.



Slika 3.1.6. Odabir heksadekadskog prikaza odmaka



Slika 3.1.7. Odabir dekadskog prikaza odmaka

3.2 Pregledavanje datoteka

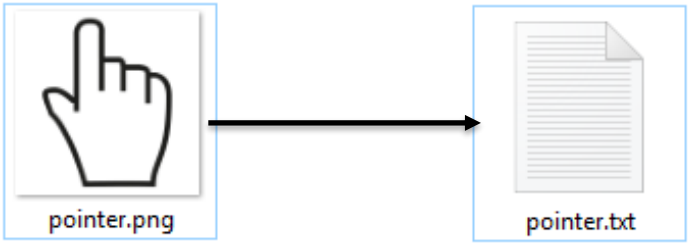
Datoteku je u HxD-u moguće otvoriti na dva načina:

1. Kroz izbornik ***File → Open***
2. Povlačenjem i ispuštanjem (engl. *drag and drop*) datoteke u prozor HxD-a

Jednom kada je datoteka otvorena u HxD-u, vidljiv je njen heksadekadski prikaz. Primjerice, jedna od prvih stvari koje pregled datoteke u HxD-u može otkriti je format te datoteke. Iako je uobičajeno vjerovati nastavku (engl. *extension*) nakon imena datoteke, postoji niz razloga zbog kojih je korisno moći objektivnije utvrditi format:

- lako je namjerno izmijeniti nastavak ,
- ako nam nije poznat pravi format datoteke, ne znamo kojim bismo je alatom pokušali otvoriti,
- datoteke se mogu oštetiti prilikom kopiranja, uređivanja ili preuzimanja i mogu „izgubiti“ nastavak.

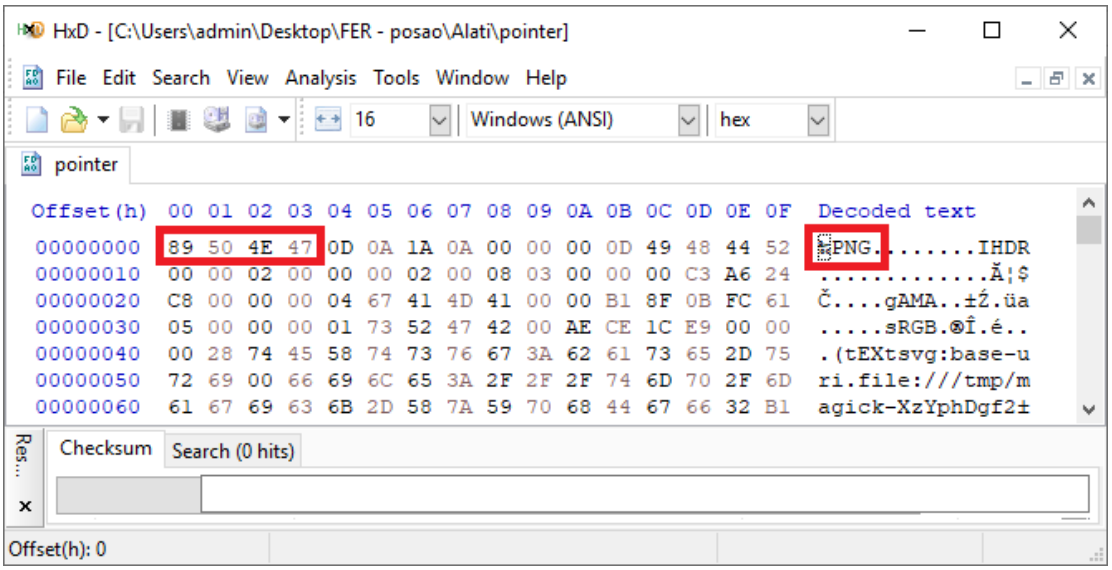
Primjerice, ništa (osim kratkog upozorenja da bi datoteka mogla postati neupotrebljiva) nas ne sprječava da slikovnoj datoteci izbrišemo nastavak *.png* i dodamo nastavak *.txt* kao što je prikazano na slici 3.2.1.



Slika 3.2.1. Izmjena nastavka slikovne datoteke iz .png u .txt

Kada bismo sad pokušali otvoriti datoteku, operacijski sustav ne bi prepoznao da je riječ o slici i pokrenuo bi program zadužen za otvaranje tekstualnih datoteka (primjerice *Notepad*).

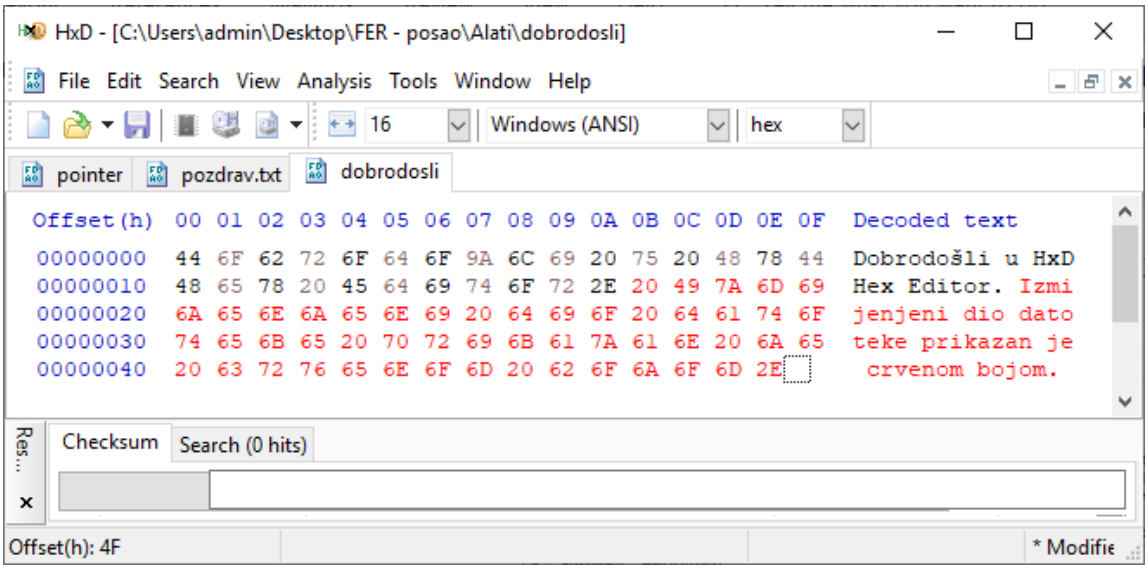
No, kada bismo otvorili datoteku u HxD-u, početni bajtovi, poznati pod nazivom magični broj (engl. *magic number*), otkrili bi da je riječ o slici u PNG formatu.



Slika 3.2.2. Pregled PNG datoteke u HxD-u

3.3 Izmjena datoteka

Datoteku je moguće mijenjati izravno u HxD-u, bilo u heksadekadskom bilo u tekstualnom prikazu. Nakon klika na željenu poziciju, dovoljno je upisati novi ili mijenjati postojeći heksadekadski odnosno tekstualni zapis. Dodani ili izmijenjeni dio datoteke bit će prikazan crvenom bojom do trenutka spremanja promjena, kao što je prikazano na slici 3.3.1.



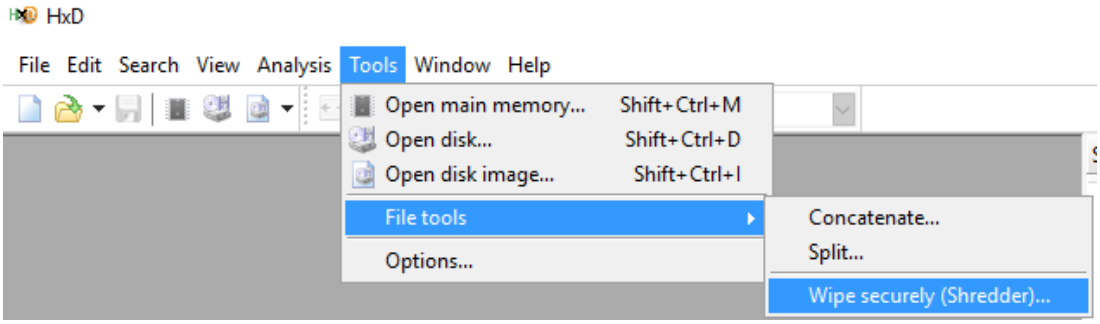
Slika 3.3.1. Uređivanje datoteke u HxD-u

3.4 Sigurno brisanje datoteka

Svaki put kad se datoteka na uobičajeni način obriše s računala, datoteka nije uistinu obrisana, već se samo memorijski prostor koji je ona zauzimala označava kao slobodan. No, dok se taj memorijski prostor uistinu ne prepiše nekim novim podacima, moguće je rekonstruirati sadržaj obrisane datoteke.

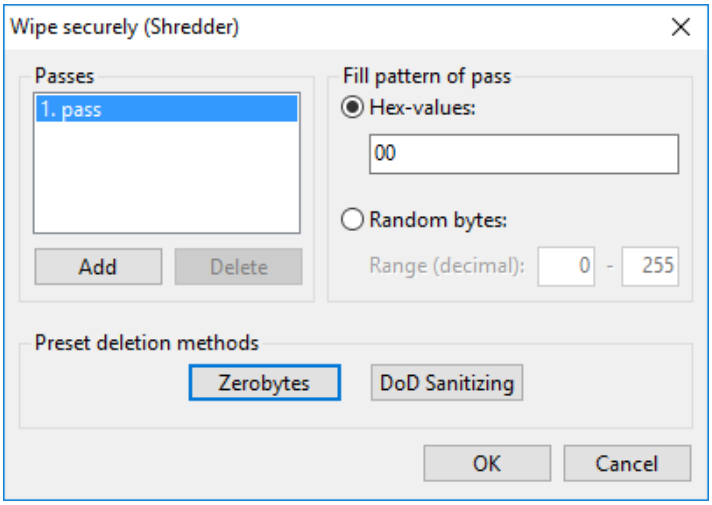
Ako je potrebno trajno obrisati neke povjerljive datoteke, tako da njihov sadržaj ne bude moguće lako rekonstruirati, korisna je HxD-ova funkcionalnost sigurnog brisanja. Sigurno brisanje u ovom kontekstu znači da će se memorijski prostor na kojem je datoteka bila pohranjena prepisati drugim vrijednostima, nakon čega sadržaj datoteke nije moguće vratiti.

Do HxD-ove funkcionalnosti za sigurno brisanje (pod nazivom *Shredder*) moguće je doći kao što je prikazano na slici 3.4.1.



Slika 3.4.1. Odabir funkcionalnosti za sigurno brisanje datoteka

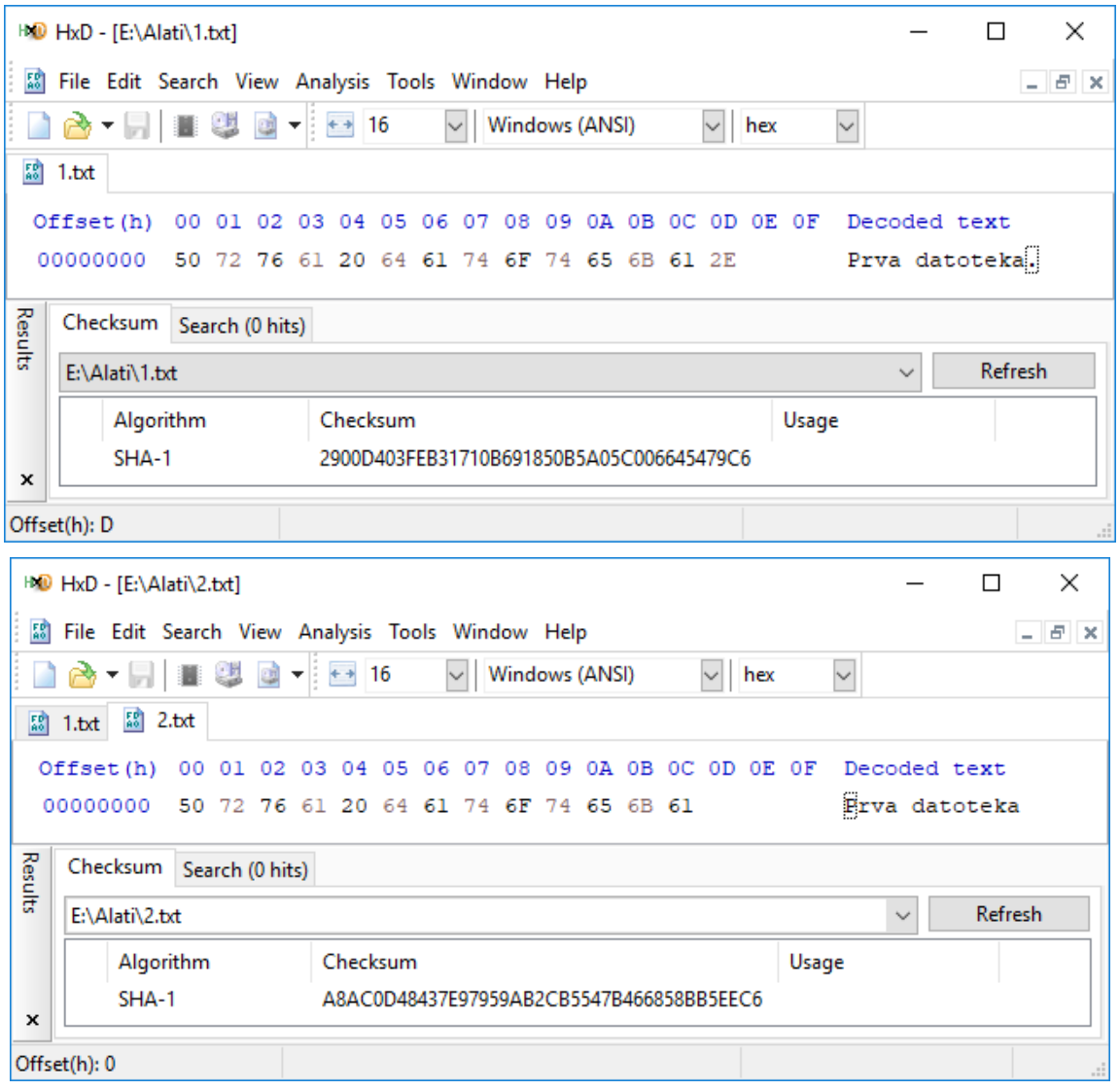
Na slici 3.4.2. prikazan je prozor s postavkama za sigurno brisanje. Moguće je definirati više prolaza (eng. *pass*) prepisivanja, a u svakom prolazu, memoriju je moguće prepisati nekom određenom (heksadekadski prikazanom) vrijednošću ili slučajnim vrijednostima. Dostupni su i predlošci postavka za sigurno brisanje, primjerice predložak „*DoD sanitizing*“ koji omogućava brisanje datoteka na način koji je propisalo Ministarstvo obrane SAD-a. Korištenje više prolaza prepisivanja dodatno otežava rekonstrukciju podataka.



Slika 3.4.2. Prozor s postavkama sigurnog brisanja

3.5 Kontrolni zbroj

Kontrolni zbroj (engl. *checksum*) općeniti je naziv za broj koji služi za provjeru je li se sadržaj dvije datoteke podudara. Proces dobivanja kontrolnog zbroja iz sadržaja datoteke napravljen je tako da već najmanja razlika između dvije datoteke, npr. razlika u samo jednom bitu, rezultira sasvim drugačijim kontrolnim zbrojem. Primjerice, kontrolnim zbrojem može se provjeriti je li datoteka ispravno preuzeta s web stranice ili je li neka pohranjena datoteka mijenjana. Na slici 3.5.1. prikazana je usporedba kontrolnog zbroja dvije datoteke koje se razlikuju samo u jednom znaku. Prva datoteka ima točku na kraju rečenice, a druga nema – vizualnom usporedbom datoteka bi tu razliku bilo teško primijetiti, dok je usporedbom kontrolnih zbrojeva jasno da se njihov sadržaj ne podudara.



Slika 3.5.1. Usporedba kontrolnih zbrojeva dvije slične datoteke

4 Zaključak

Iako se heksadekadski uređivači rijetko koriste za svakodnevne radnje na računalu, oni su neizostavni kada je potrebno dubinski istražiti sadržaj neke datoteke, ili čak diska i radne memorije. Primjerice, kada programeri rade na aplikaciji koja čita i zapisuje datoteke u nekom složenom formatu, heksadekadski uređivač im je često jedan od glavnih alata koje koriste. Stručnjaci informacijske sigurnosti, primjerice oni koji se bave digitalnom forenzikom ili analizom zlonamjernog softvera, također često posežu za heksadekadskim uređivačem kada je potrebno temeljito istražiti neki digitalni sadržaj.

HxD je besplatan, brz te ujedno moćan i jednostavan korištenje. Upravo zato, kada postoji potreba za heksadekadskim uređivačem na Microsoft Windows operacijskim sustavima, HxD je obično jedan od prvih izbora.