

ФЕЂА КУЛЕНОВИЋ



FEĐA KULENOVIĆ

DIGITALNA SIGURNOST/BEZBIJEDNOST

LIČNA I ORGANIZACIJSKA ZAŠTITA NA MREŽI

BANJA LUKA, 2018.

KONCEPT PRIVATNOSTI

- U NE-DIGITALNOM OKRUŽENJU JASAN. SVI SE TRUDIMO DA ZAŠTITIMO PRIVATNOST
- U DIGITALNOM OKRUŽENJU - nismo svjesni kada smo sami, a kada ne.

DIGITALNA SIGURNOST

Širok pojam

Digitalni sistem koji nije bezbijedan ne može se smatrati privatnim, dok samim tim što sistem ima obezbijeđenu privatnost, ne znači da je potpuno bezbijedan.

FAKTORI

- TEHNOLOŠKI
- NE-TEHNOLOŠKI - Navike korisnika
- Digitalna sjenka
- Možemo je kontrolisati

INTERNET PRIVATNOST

je oblik lične privatnosti koji se odnosi na čuvanje, reprodukciju, deljenje sa trećim licima i prikazivanje informacija koje pripadaju određenoj osobi, preko Interneta.

ENKRIPTCIJA

kriptografski koncept kodiranja poruka ili informacija čime se osigurava da će jedino osobe koje imaju način da je dekodiraju (dekriptuju) moći da je pročitaju.

LOREM IPSUM

ORIGINALNI TEKST

ERSPZHEBBZP73Z7YMBFFSA==

ENKRIPTOVANO

SUGURNNO SURFANJE

HTTP (HYPERTEXT TRANSFER PROTOCOL) je protokol kroz koji se odvija saobraćaj koji se odnosi na pretraživanje World Wide Web-a (WWW). Ovim protokolom je regulisana komunikacija između korisnika i servera na kom se sadržaj nalazi.

SSL (SECURITY SOCKET LAYER) je poseban sloj zaštite na HTTP Internet protokolu.

TLS (TRANSPORT LAYER SECURITY) je unapređena i novija verzija SSL-a.

MITM (MAN IN THE MIDDLE) napad je vrsta tehničkog napada u kom klijent i server nisu nužno kompromitovani, međutim veza između njih jeste, te napadač koristi nedostatke veze da bi imao pristup komunikaciji kako bi je kompromitovao.

BACKDOOR (SPOREDNI ULAZ) u IS je mehanizam zaobilaznja standardne forme autentifikacije i dobijanje neovlašćenog pristupa zaštićenom IS, pritom je specifično to što upadač ostaje nezapažen.

SADRŽAJ TREĆIH STRANA (THIRD PARTY CONTENT) je sadržaj koji korisnik nije direktno zahtevao, ali mu je prikazan zbog toga što je vlasnik zahtevanog sadržaja ustupio deo svog sajta trećim stranama (Google reklamama, Facebook komentarima itd).

VPN (VIRTUAL PRIVATE NETWORK) je Internet usluga koja omogućava povezivanje na privatnu mrežu kroz javnu mrežu kao što je Internet. VPN omogućava korisnicima da bezbedno šalju i primaju poverljive podatke kroz Internet.

PROXY je servis koji omogućava povezivanje na server na daljinu kroz koji se onda pristupa Internetu. Suštinska razlika između Proxy-ja i VPN-a jeste u tome što Proxy prolazi samo saobraćaj koji se odnosi na pregledač,

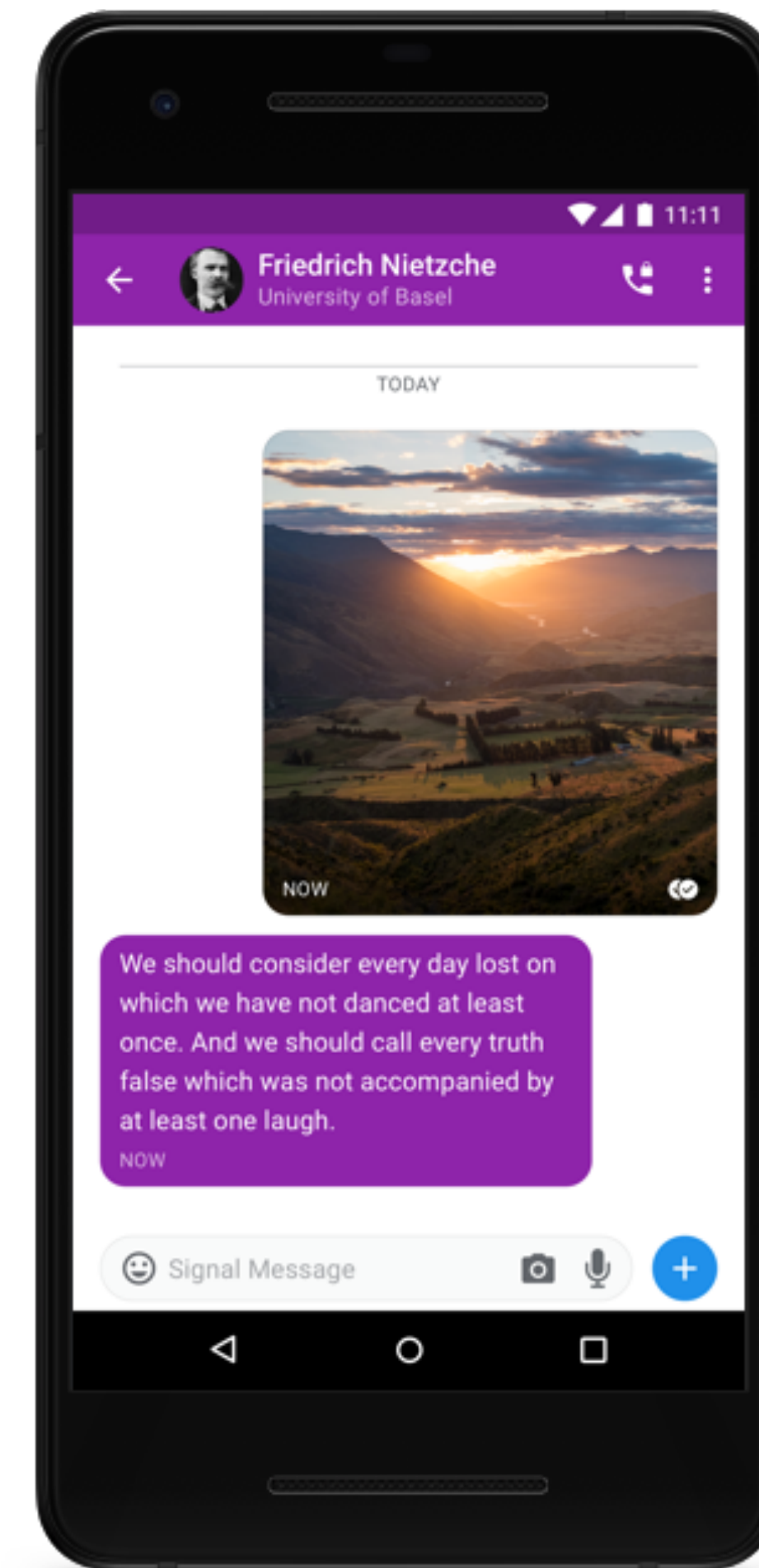
dok VPN pokriva ceo saobraćaj koji proizilazi iz tog računara (uključujući Skype, e-mail klijente itd)

(Napomena: Ne preporučuje se korišćenje TOR mreža za skidanje velikih datoteka zbog toga što se mreža opterećuje i to utiče na njenu brzinu. Takođe, u slučaju da korišćeni program nije pouzdan, TOR ne može garantovati anonimnost)

SIGURNA KOMUNIKACIJA

Signal

www.signal.org



SIGURNNA KOMUNIKACIJA

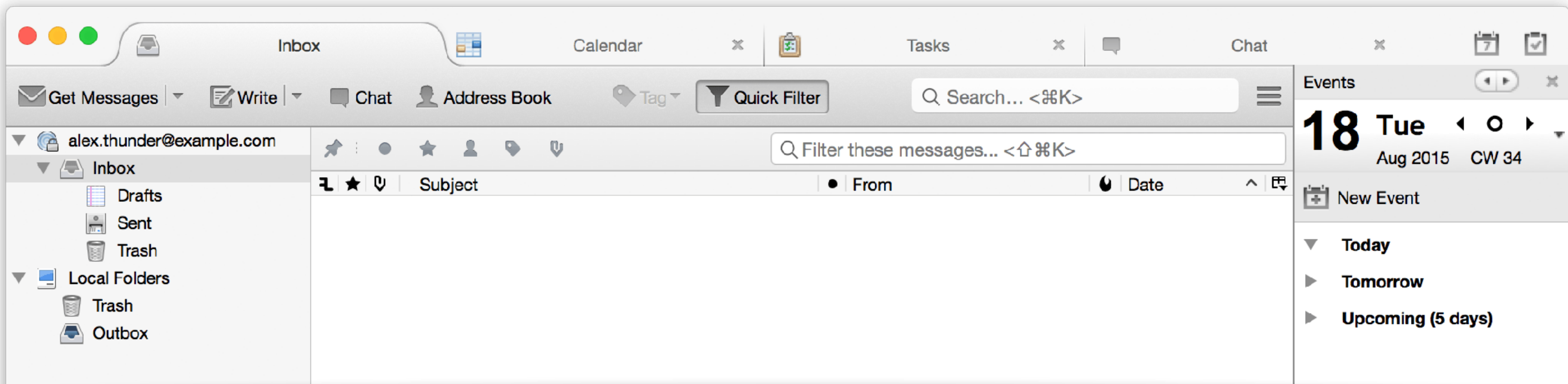
- <http://pidgin.im>

- **PODRŽAVA**

- AIM
- Bonjour
- Gadu-Gadu
- Google Talk
- Groupwise
- ICQ
- IRC
- SILC
- SIMPLE
- Sametime
- XMPP
- Zephyr

The image shows the word "pidgin" in a stylized, lowercase, purple font. The letters are thick and rounded, with a unique, slightly irregular design. The 'p' is particularly large and has a curved bottom. The 'i's have small dots above them. The 'g' has a large, rounded loop. The 'n' is also thick and rounded. The overall style is modern and friendly.

SIGURNA E-MAIL KOMUNIKACIJA



- Thunderbird sa PGP enkripcijom
- Za PGP enkripciju skinuti GPG4WIN sa <https://www.gpg4win.org>

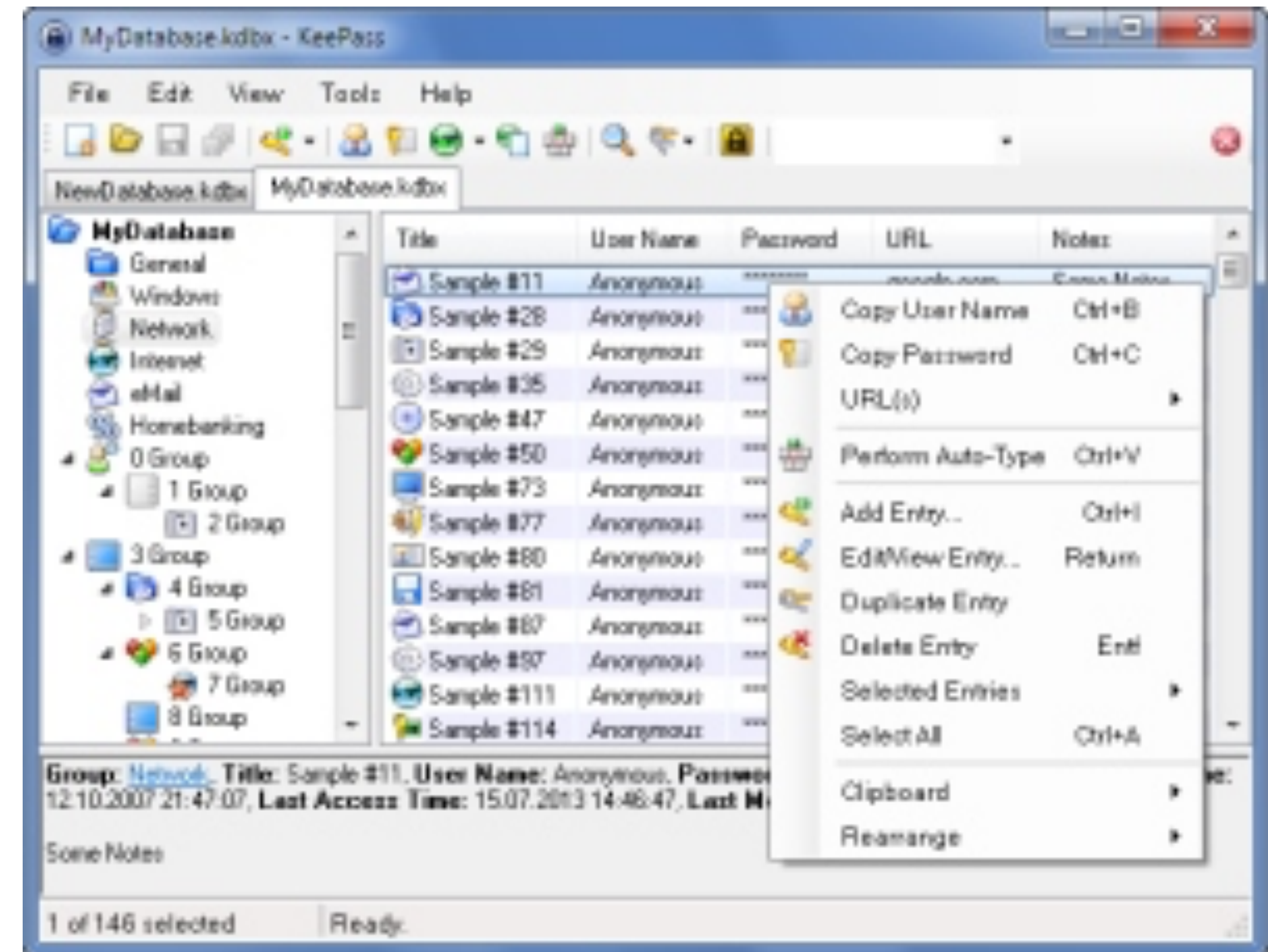
Enkripcija diskova

- VeraCrypt
- BitLocker
- Boxcryptor (za fajlove u oblaku)



UPRAVLJANJE PASSWORDIMA

- KeePass



SIGURNO PRETRAŽIVANJE

- DuckDuckGo www.duckduckgo.com
- Šalje Google-u zahtjeve za pretraživanje
- Na taj način anonimizira vaše upite
- Mana je što Google ne prilagođava algoritam vašim navikama pretraživanja pa rezultati mogu biti generalniji nego što smo navikli.



SIGURNO BRISANJE PODATAKA

- **ERASER**

https://download.cnet.com/Eraser/3000-2144_4-10231814.html

- **SHREDDER** za Mac

<https://www.apple.com/downloads/dashboard/business/shredder.html>

- **Darik's Boot and Nuke for CD and DVD** (za vanjske uređaje)

https://download.cnet.com/Darik-s-Boot-and-Nuke-for-CD-and-DVD/3000-2094_4-10151762.html

PODEŠAVANJE PRIVATNOSTI

- Google myaccount.google.com
- Facebook sigurnosne postavke