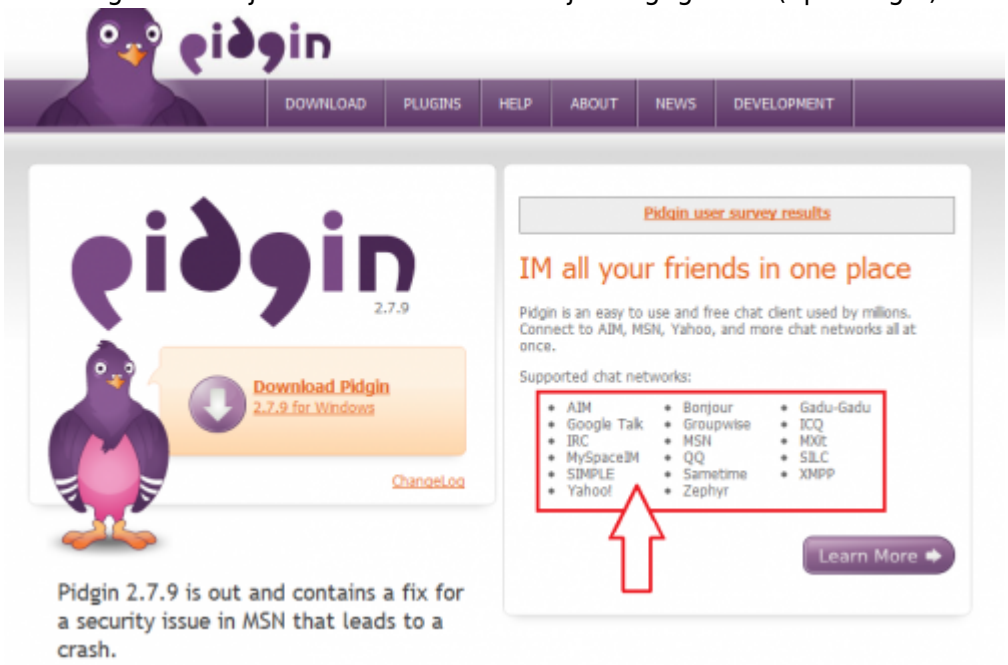
Instant Messaging

Instant Messaging ili IM je od devedesetih godina prošlog stoljeća sve popularniji način komuniciranja putem Interneta. Začetnik ovog trenda, ICQ, još je i danas među popularnijim IM servisima. Među ostale popularne messaging alate spadaju Windows Live Messenger (ranije poznat kao .NET ili MSN Messenger), AOL IM, Google Talk, iChat, Jabber, Qnext, QQ, Meetro, Skype, Trillian, Yahoo! Messenger, Excite/Pal, Gadu-Gadu, Rediff Bol IM, itd. IM je način komunikacije slanjem poruka u stvarnom vremenu u sučelju određenog alata. Standardno, obje strane komunikacije (ili više strana ako je riječ o konferencijskoj sjednici) moraju koristiti isti alat, no postoje i alati koji omogućavaju korisniku da pohrani sve kontakte iz ostalih messengera te s njima komunicira iz sučelja drugog alata (npr. Pidgin).



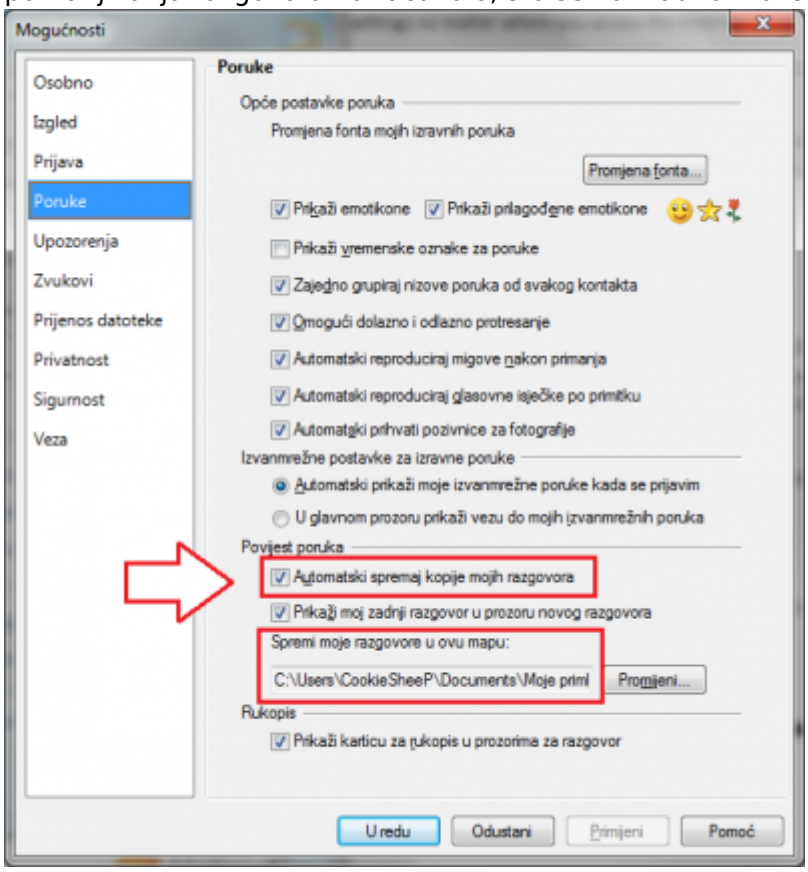
IM alati nude mogućnost pohranjivanja razgovora na lokalno računalo, a tako pohranjeni razgovori mogu pružiti mnogo informacija o korisniku. Doduše u slučaju kad korisnik odabere ne pohranjivati kopije razgovora, istražitelj se može tek nadati komadima razgovora razbacanih po cache memoriji. Većina alata radi na sličan način (nude pohranjivanje razgovora, kontakata i preuzetih datoteka), a u nastavku će se detaljnije opisati Windows Live Messenger koji je prema nekim statistikama najkorišteniji IM alat u svijetu. Osim tekstualnog dopisivanja, sve više IM alata nudi i mogućnost video poziva čime se sve više koriste i u poslovnom svijetu za komunikaciju s klijentima ili na poslovnim sastancima.

Windows Live Messenger

Windows Live Messenger konstantno izdaje nove inačice te se detalji u načinu rada mogu razlikovati od inačice do inačice. U ovom radu se koristi inačica iz 2009. (međuverzija 14.0.8117.416). Korisnik se u Windows Live prijavljuje s e-mail adresom i lozinkom (Microsoft .NET Passport). S tim se podacima korisnik može prijaviti u Windows Live za bilo kojim računalom s instaliranim alatom, kao i na Windows Live web servis (za kojeg nije potrebna instalacija) te Windows Live za mobilne uređaje.

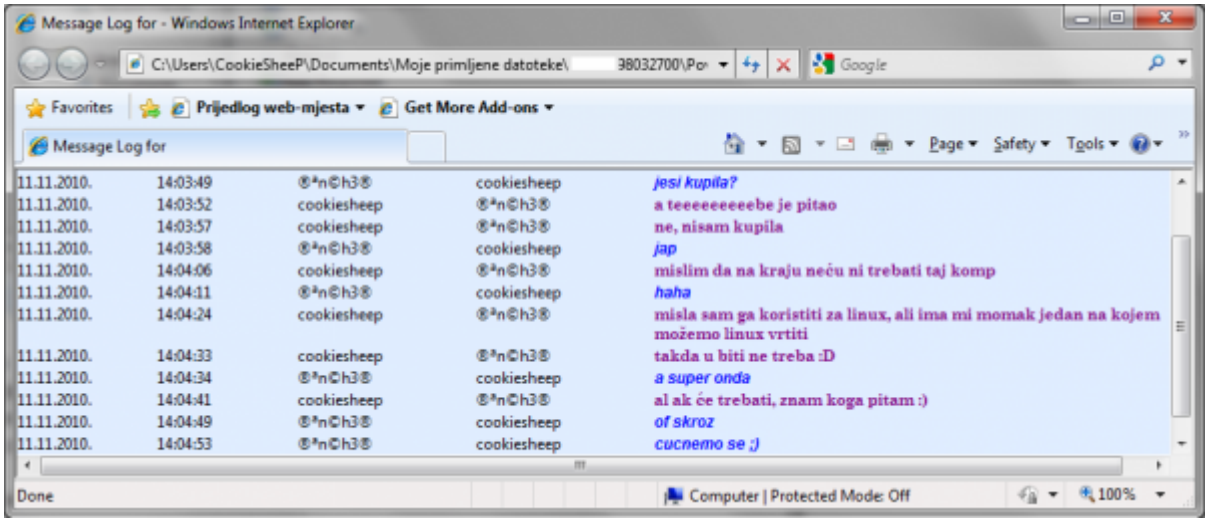
Pohranjivanje razgovora

Svaki put kad se korisnik prvi put prijavi na novom računalu, Windows Live će ponuditi opciju pohranjivanja razgovora na računalo, što se naknadno može izmijeniti.



Razgovori se pohranjuju u .XML formatu što je korisno znati kad se pretražuje računalo u potrazi za razgovorima, pogotovo ako je korisnik odredio da se pohranjuju na neku drugu lokaciju (umjesto na automatski podešenu) ili ako ih je prenio s drugog računala. U tom slučaju istražitelj može filtrirati datoteke po formatu i tako suziti područje pretrage da uštedi na vremenu. Doduše, ne valja se oslanjati na to kao apsolutno sigurnu metodu jer korisnik može namjerno pokušati prikriti format datoteke kako bi je sakrio “na otvorenom”.
Datoteke u .XML formatu se mogu otvoriti bilo kojim tekstualnim uređivačem, ali ih je preglednije otvoriti web preglednikom. U slučaju operacijskog sustava Windows Vista/7, kopije razgovora i datoteke preuzete u razgovoru se automatski pohranjuju na adresu:

```
C:\Users\<User's ID>\Documents\Moje primljene
datoteke\<PassportName>########\Povijest
```

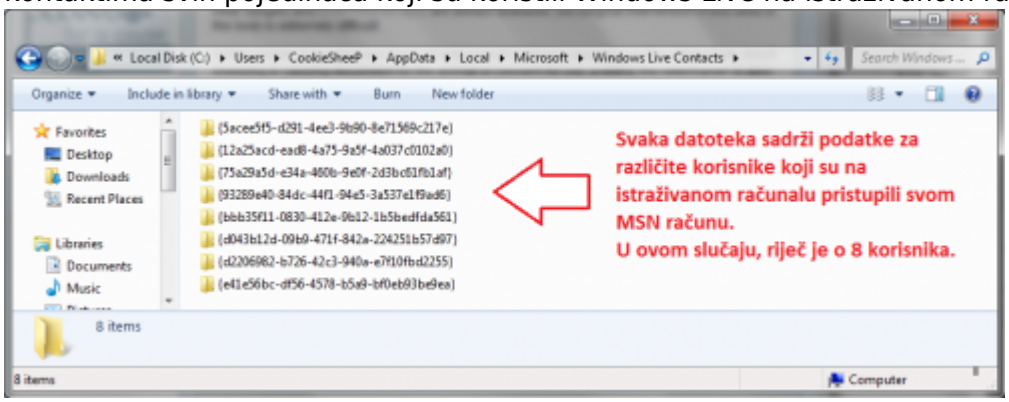


Podaci o kontaktima

Osim razgovora, Windows Live na računalo pohranjuje i podatke o kontaktima za svaki račun kojem je pristupljeno s istraživanog računala (datoteka contacts.edb). U slučaju operacijskog sustava Windows Vista/7, ti se podaci nalaze na adresi:

```
C:\Users\<User's ID>\AppData\Local\Microsoft\Windows Live Contacts\<RandomNoFolderName>
```

Alatom LiveContactsView tvrtke NirSoft se može otvoriti datoteka contacts.edb koja sadrži detalje o kontaktima svih pojedinaca koji su koristili Windows Live na istraživanom računalu.



Podaci koji se pritom otkrivaju su e-mail adresa kontakta, nadimak, ime, prezime, adresa, broj telefona, vrijeme zadnjeg kontakta, grad, itd. Naravno, kontakti moraju prvo unijeti te podatke u svoj profil (što nije čest slučaj jer ljudi često ne žele objavljivati previše detalja o sebi). Slika ispod prikazuje sučelje alata s otvorenim podacima jednog kontakta (podaci su skriveni da bi se zaštitio kontakt).