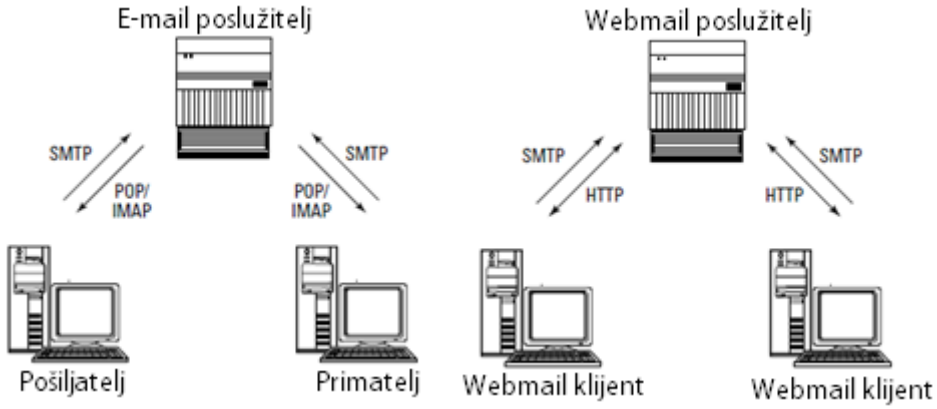
E-mail i webmail

Elektronička pošta (*e-mail*) je danas najpopularniji način komunikacije. Svaki dan se diljem svijeta šalju milijarde e-mail poruka, a koristi se podjednako za službenu i neslužbenu komunikaciju. Upravo zbog svoje učestalosti, e-mail se često može naći i u sudskim procesima kao ključni dokaz.

Kod korištenja e-mail klijenta za čitanje elektroničke pošte, poruke stižu do poslužitelja i tamo čekaju dok korisnik ne provjeri svoju poštu. U tom trenutku program za elektroničku poštu (npr. Mozilla Thunderbird) preuzima poruke i pohranjuje ih na lokalni disk, čime se one brišu s poslužitelja (ove se postavke mogu promijeniti iako to nije čest slučaj). Nakon što stignu na računalo, forenzičari ih, kao i sve ostale podatke na računalu, mogu pronaći i prema potrebi rekonstruirati. Pritom se za slanje koristi SMTP (eng. *Simple Mail Transfer Protocol*), a za preuzimanje POP (eng. *Post Office Protocol*) ili IMAP (eng. *Internet Message Access Protocol*) protokoli.

Webmail radi na taj način da poruke ostaju na poslužitelju, a korisnik im pristupa korištenjem web preglednika. To znači da korisnik može pristupiti pošti s bilo kojeg računala u bilo kojem trenutku (ako zna korisničko ime i lozinku). Pošta ostaje na poslužitelju čak i nakon što je korisnik izbrisao poruku, a koliko se dugo čuva nakon brisanja ovisi o e-mail servisu. Gmail tako, primjerice, u uvjetima korištenja spominje da se izbrisana pošta čuva na neodređeno vrijeme. To pogoduje istražiteljima, ali ne i ljudima koji ne žele da im pošta bude dostupna. Webmail za preuzimanje (ali i za slanje, uz SMTP) pošte koristi HTTP (eng. *Hyper-Text Transfer Protocol*) protokol što znači da se poruke šalju u obliku otvorenog teksta te ih je moguće presresti i pročitati.



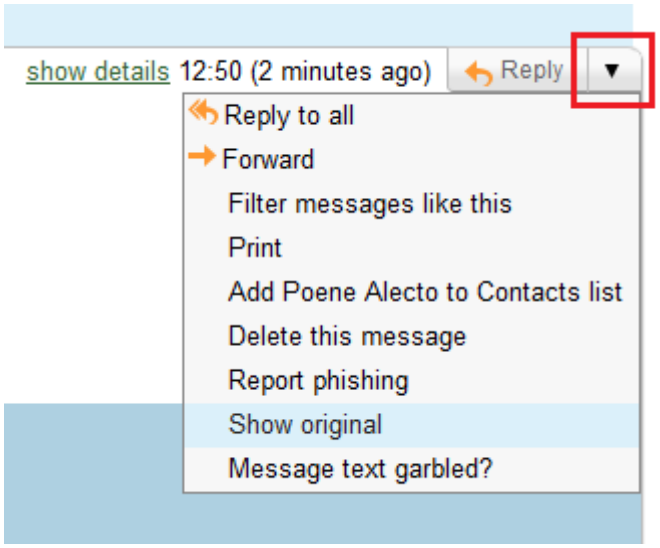
Svaki e-mail klijent pohranjuje podatke poput adresa kontakata ili sažetaka poruka ili same poruke u svom specifičnom formatu koje se mogu čitati samo u tom klijentu. No mnogi forenzički alati imaju mogućnosti analize popularnijih formata, od kojih su neki prikazani u tablici niže.

E-mail klijent	**Povezane ekstenzije**	**Tip datoteke**
AOL	.abi, .arl .aim, .bag	Organizacijska datoteka IM poruke
Eudora	.mbx	Baza poruka
Outlook	.pab .pst .wab	Osobni adresar Komprimirana osobna datoteka Adresar
Outlook Express	.dbx .dgr\\.e-mail, .eml	Komprimirana baza podataka Stranica s faxevima E-mail poruka

E-mail klijent	Povezane ekstenzije	Tip datoteke
Thunderbird	.msf	Datoteka sažetaka poruka (eng. *Mail Summary File*)

Metapodaci zaglavlja

Metapodaci su tzv. podaci o podacima i često se po količini korisnih informacija uspoređuju s otiskom prsta ili balističkim nalazom. Važni su za forenzičku istragu jer mogu puno otkriti o korisniku i vremenskom slijedu događaja. Ti podaci se postavljaju automatski (npr. adrese računala na putu e-mail poruke od pošiljatelja do primatelja), ali ovise o podacima operacijskog sustava (npr. vrijeme zadnje izmjene datoteke) koje korisnik sam može izmijeniti, tako da ne moraju nužno biti ispravni. Elektronička pošta je najčešće korišten elektronički dokaz na sudu, bilo da je riječ o komunikaciji između dvoje nezadovoljnih zaposlenika koji planiraju ukrasti novac od tvrtke ili o nevjernom suprugu koji dogovara tajne sastanke. Metapodaci e-pošte se nalaze u zaglavlju (eng. *header*) poruke. Ono se može vidjeti bez posebnih alata, no postupak je za svaki e-mail klijent drugačiji. Upute za pojedine klijente se mogu potražiti u dokumentaciji klijenata.



Tablica ispod sadrži opis standardnih polja u zaglavlju elektroničke pošte. E-mail klijenti ponekad dodaju svoja polja, specifična samo za njih. Takva se polja označavaju s `X-<NazivPolja>`. Takva polja nisu sadržana u popisu standardnih polja, ali su dopuštena.

POLJE	OPIS	OBAVEZNO
Cc	Dodatni primatelj poruke.	Ne
Bcc	Dodatni primatelji poruke nevidljivi svim ostalim primaocima. Primatelji se ne prikazuju prilikom ispisa stranice osim ako se ispisuje s računala pošiljatelja.	Ne
Comments	Tekstualni komentari, ne utječu na sadržaj poruke.	Ne
Date	Datum slanja poruke.	Da
Encrypted	Metoda enkriptiranja poruke.	Ne
From	Identitet pošiljatelja, moguće ga je lažirati.	Da
In-Reply-To	Identificira prethodnu e-mail poruku na koju se odgovara ovom porukom.	Ne
Keywords	Ključne riječi odvojene zarezima.	Ne

POLJE	OPIS	OBAVEZNO
Message-ID	Identifikator čitljiv računalu jedinstven za konkretnu e-mail poruku. Ne prikazuje se pri ispisu poruke iz e-mail klijenta.	Ne, ali se gotovo uvijek koristi.
Received	Pokazuje vrijeme kad je poruka primljena i cijeli put koji je prešla od pošiljatelja do primatelja (može uključivati i nekoliko poslužitelja). Ove informacije su bitne za autenticiranje e-mail poruke i određivanje dodatnih računala koja treba uključiti u istragu. E-mail poslužitelji na cijelom putu slanja automatski dodaju ove podatke.	Ne, ali se gotovo uvijek koristi.
References	Identificira prethodnu poruku na koju se ova poruka odnosi.	Ne
Reply-To	Adresa na koju se trebaju slati odgovori na poruku. Obično je ista kao i adresa pošiljatelja, ali ne uvijek.	Ne, ali mnogi e-mail klijenti dodaju ovo polje.
Resent-bcc	Isto kao i Bcc, ali se odnosi na proslijeđene poruke.	Ne
Resent-cc	Isto kao i Cc, ali se odnosi na proslijeđene poruke.	Ne
Resent-date	Datum slanja proslijeđene poruke.	Ne
Resent-From	Identitet pošiljatelja proslijeđene poruke.	Ne
Resent-Message-ID	Message-ID za proslijeđenu poruku.	Ne
Resent-Reply-to	Reply-to za proslijeđenu poruku.	Ne
Resent-Sender	Izvorni pošiljatelj proslijeđene poruke.	Ne
Return-Path	Adresa i put natrag do tvorca e-mail poruke.	Ne
Sender	Adresa osobe koja je poslala e-mail poruku.	Da
Subject	Tema e-mail poruke.	Ne
To	Glavni primatelj poruke.	Da
X	Prefiks za oznake specifične za pojedine klijente.	Ne

Analiza zaglavlja

Analizom zaglavlja e-mail poruke se može puno toga otkriti o poruci. Ono što istražitelje uglavnom zanima jest da li je ikoji dio poruke falsificiran. Slijede primjeri nekih polja zaglavlja.

- **Protokoli**
  - (E)SMTP (eng. *(Extended) Simple Mail Transfer Protocol*) – ako se pri slanju koristi SMTP protokol, znači da je poruka poslana SMTP klijentom (npr. Outlook, Eudora, ...),
  - HTTP(S) (eng. *Hyper-Text Transfer Protocol (Secure)*) – ako prvo `Received` polje iznad polja `From` koristi HTTP ili HTTPS, to je očiti znak da pošiljatelj koristi webmail (npr. Hotmail, Gmail, Yahoo, ...). U primjerima niže se vidi kako Google koristi HTTP protokol dok Hotmail koristi SMTP za slanje pošte.

```
Delivered-To: csi.gmail@gmail.com
Received: by 10.229.80.73 with SMTP id s9cs99127qck;
Mon, 20 Dec 2010 02:31:27 -0800 (PST)
Received: by 10.90.118.2 with SMTP id q2mr5201143agc.11.1292841087267;
```

```
Mon, 20 Dec 2010 02:31:27 -0800 (PST)
Return-Path: < csi.hotmail@hotmail.com >
Received: from blu0-omc1-s9.blu0.hotmail.com (blu0-omc1-s9.blu0.hotmail.com
[65.55.116.20])
by mx.google.com with ESMTP id y10si2459486vch.161.2010.12.20.02.31.26;
Mon, 20 Dec 2010 02:31:27 -0800 (PST)
(…)
Received: from BLU139-W20 ([65.55.116.7]) by blu0-omc1-s9.blu0.hotmail.com
with Microsoft SMTPSVC(6.0.3790.4675);
Mon, 20 Dec 2010 02:30:51 -0800
From: Csi Hotmail < csi.hotmail@hotmail.com >
To: < csi.gmail@gmail.com >
```

```
X-SID-PRA: Csi Gmail < csi.gmail@gmail.com >
(…)
Received: from mail-qw0-f46.google.com ([209.85.216.46]) by bay0-mc2-
f4.Bay0.hotmail.com with Microsoft SMTPSVC(6.0.3790.4675); Mon, 20 Dec 2010
02:40:51 -0800
(…)
Received: by mail-qw0-f46.google.com with SMTP id 26so2637989qwa.19
for < csi.hotmail@hotmail.com >; Mon, 20 Dec 2010 02:40:51 -0800 (PST)
(…)
Received: by 10.229.90.196 with SMTP id j4mr3585879qcm.144.1292841651354;
Mon, 20 Dec 2010 02:40:51 -0800 (PST)
Received: by 10.229.80.73 with HTTP; Mon, 20 Dec 2010 02:40:51 -0800 (PST)
Date: Mon, 20 Dec 2010 11:40:51 +0100
(…)
From: Csi Gmail < csi.gmail@gmail.com >
To: csi.hotmail@hotmail.com
```

- **Najčešće vremenske oznake**
  - PST (*Pacific Standard Time*, GMT-8:00) – vrijeme u državama SAD-a Washington, većem dijelu Oregona, Nevada, California (gdje Google ima sjedište),
  - UTC (*Coordinated Universal Time*, GMT) – vrijeme na Islandu, u Velikoj Britaniji i Portugalu.
- **Vrijeme**
  Prilikom analize zaglavlja, istražitelj treba obratiti pažnju na vremena kad je poruka prolazila kroz poslužitelje. Ukoliko je korisnik pokušao lažirati vrijeme slanja poruke, vremena na poslužiteljima se neće podudarati. Na primjeru ispod se vidi nelažirani prolaz poruke do pošiljatelja (zna se da je nelažirani zbog sličnih vremena). Poslužitelj (u polju `Received`) koji je u zaglavlju najbliži polju `From` je prvi primio poruku od pošiljatelja, a poslužitelj najbliži polju `Delivered-To` je bio posljednji na tom putu, dakle redoslijed se promatra od dna prema vrhu zaglavlja.

```
Delivered-To: csi.gmail@gmail.com
```

```
Received: by 10.229.80.73 with SMTP id s9cs98569qck;
Mon, 20 Dec 2010 02:19:41 -0800 (PST) ⇒ 02:19:40 po PST vremenu (11:19:41 u ZG)
Received: by 10.216.173.7 with SMTP id u7mr7299694wel.50.1292840380705;
Mon, 20 Dec 2010 02:19:40 -0800 (PST) ⇒ 02:19:40 po PST vremenu (11:19:40 u ZG)
Return-Path: < ime.prezime@fer.hr >
Received: from munja.zvne.fer.hr (munja.zvne.fer.hr [161.53.66.248])
by mx.google.com with ESMTP id m49si5391189weq.54.2010.12.20.02.19.40;
Mon, 20 Dec 2010 02:19:40 -0800 (PST) ⇒ 02:19:40 po PST vremenu (11:19:40 u ZG)
Received-SPF: pass (google.com: best guess record for domain of
ime.prezime@fer.hr designates 161.53.66.248 as permitted sender) client-
ip=161.53.66.248;
Authentication-Results: mx.google.com; spf=pass (google.com: best guess
record for domain of
ime.prezime@fer.hr designates 161.53.66.248 as permitted sender)
smtp.mail=ime.prezime@fer.hr
Received: from sluga.fer.hr ([161.53.66.244]) by munja.zvne.fer.hr with
Microsoft SMTPSVC(6.0.3790.4675);
Mon, 20 Dec 2010 11:19:39 +0100 ⇒ 11:19:39 po hrvatskom vremenu (GMT+1)
(…)
From: “Ime Prezime” < ime.prezime@fer.hr >
```

- **Identifikacijski broj poruke** (`Message-ID`, `id`)
  E-mail klijent s kojeg korisnik šalje poruku, kao i svaki SMTP poslužitelj koji prenosi poruku od pošiljatelja do primatelja, poruci dodjeljuje identifikacijski broj. Korištenjem tog broja istražitelji mogu u bazi podataka poslužitelja pronaći poruku. U donjem primjeru se može primjetiti i logika iza davanja id brojeva (koja nije jednaka kod svih e-mail klijenata), kao na primjer vrijeme i datum slanja poruke.

```
Received: from blu0-omc1-s9.blu0.hotmail.com (blu0-omc1-s9.blu0.hotmail.com
[65.55.116.20])
by mx.google.com with ESMTP id y10si2459486vch.161.2010.12.20.02.31.26;
Mon, 20 Dec 2010 02:31:27 -0800 (PST)
```

- **Autentikacija**

Kad e-mail klijent primi poruku, provjerava se SPF (eng. *Sender Policy Framework*) za tog pošiljatelja na DNS poslužitelju. Poslužitelj će odgovoriti da li je ta poruka uistinu poslana iz njegovog područja, čime se pošiljatelj autenticira ili smatra spammerom. Dolje vidimo dva primjera, jedan u kojem je pošiljatelj prošao autentikaciju (`spf=pass`) te jedan u kojem nije (`spf=none`).

```
Delivered-To: csi.gmail@gmail.com
Return-Path: < ncsi.gmail@gmail.com >
Received-SPF: pass (google.com: domain of ncsi.gmail@gmail.com designates
10.224.2.196 as permitted sender) client-ip=10.224.2.196;
Authentication-Results: mr.google.com; spf=pass (google.com: domain of
ncsi.gmail@gmail.com designates 10.224.2.196 as permitted sender)
smtp.mail=ncsi.gmail@gmail.com; dkim=pass header.i=ncsi.gmail@gmail.com
(…)
From: Ncsi Gmail < ncsi.gmail@gmail.com >
To: Csi Gmail < csi.gmail@gmail.com >
```

```
(…)
X-SID-PRA: Ime Prezime < ime.prezime@fer.hr >
X-AUTH-Result: NONE ⇒ polje specifično za Hotmail
(…)
From: “Ime Prezime” < ime.prezime@fer.hr >
To: < csi.hotmail@hotmail.com >
```

Alati korišteni pri analizi elektroničke pošte

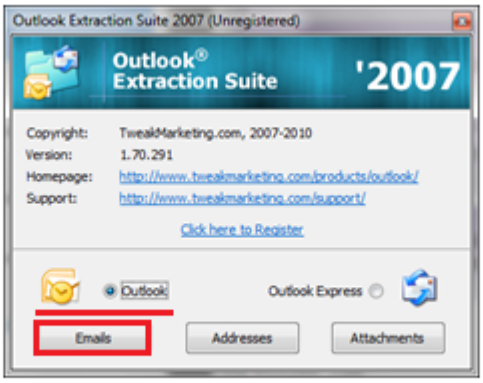
Tablica ispod sadrži neke korisne alata za analizu i praćenje elektroničke pošte. Nekoliko njih je korišteno u izradi ovog dokumenta te će biti detaljnije opisani u narednim poglavljima.

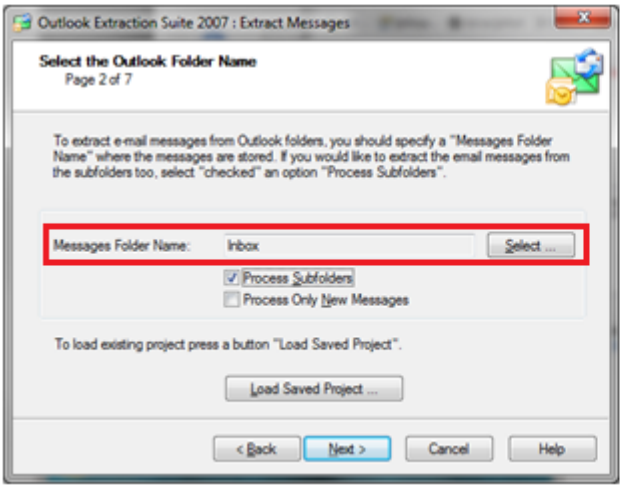
Program	Mogućnosti	Tehnički zahtjevi
Outlook Extraction Suite 2007	Izdvajanje e-mail adresa, e-mail poruka i privitaka (eng. attachment) iz .pst datoteke. Pohranjivanje rezultata u .eml formatu.	MS Windows 2000, 2003, Vista, XP, 7; MS Outlook 2000, 2003, 2007, 2010, Outlook Express.
LoPe	Mogućnost izdvajanja e-mail poruka i privitaka iz nekoliko .pst datoteka odjednom. Pohranjivanje rezultata u .msg, .eml ili .xml formatu.	
Recover My Email	Mogućnost rekonstruiranja izbrisanih e-mail poruka, kontakata i privitaka iz .pst/.dbx datoteke. Pohranjivanje rezultata u .pst ili .eml formatu.	MS Outlook 2000, 2002, 2003, 2007, 2010 (32-bitna inačica), sve inačice Outlook Express (.dbx)

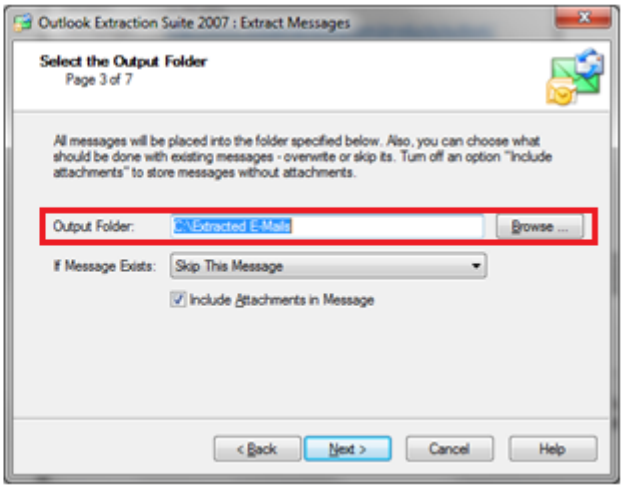
Program	Mogućnosti	Tehnički zahtjevi
MailDetective	Praćenje e-mail komunikacije u lokalnoj mreži: - stranke u komunikaciji, - učestalost komunikacije, - komunikacija po vremenskim intervalima.	- MS Windows 2000, 2003, XP, 2008, Vista, 7; - Jedan od poslužitelja: MS Exchange Server 5.5, 2000, 2003, 2007, 2010, Mdaemon, Kerio Mail Server, Kerop Visnetic Mail Server, Qmail, SendMail, Communigate; - 512 MB RAM memorije
eMailTrackerPro	Geografsko lociranje pošiljatelja e-mail poruke.	
SpyPig	Pošiljatelj e-mail poruke prima obavijest kada primatelj otvori poruku.	I pošiljatelj i primatelj moraju koristiti HTML e-mail (Outlook, Eudora, Yahoo e-mail, Gmail, Hotmail, AOL, ...). Ne funkcionira s običnim tekstualnim (eng. *plain-text*) i bogatim tekstualnim (eng. *rich-text*) e-mail klijentima.
AccessData FTK	Uz široki spektar mogućnosti u forenzičkom istraživanju – mogućnost pregledavanja, pretraživanja, ispisa i izdvajanja e-mail poruka, obnavljanja izbrisane pošte, automatski izdvaja komprimirane podatke (PKZIK, WinZip, WinRAR, GZIP, TAR).	Podržani formati: NTFS, komprimirani NTFS, FAT 12/16/32 i Linux ext2 & ext3
EnCase	Uz široki spektar mogućnosti prilikom forenzičkog istraživanja – mogućnost pronalaska, parsiranja, analize, prikazivanja i dokumentiranja različitih tipova e-mail formata. U nekim slučajevima je moguće obnavljanje izbrisane pošte i, ovisno o e-mail formatu, stanje računala.	Radi s e-mail klijentima: Hotmail, Outlook (inačice 1997 – 2003), Lotus Notes, Yahoo, AOL (6 – 9), Netscape, mbox i Outlook Express

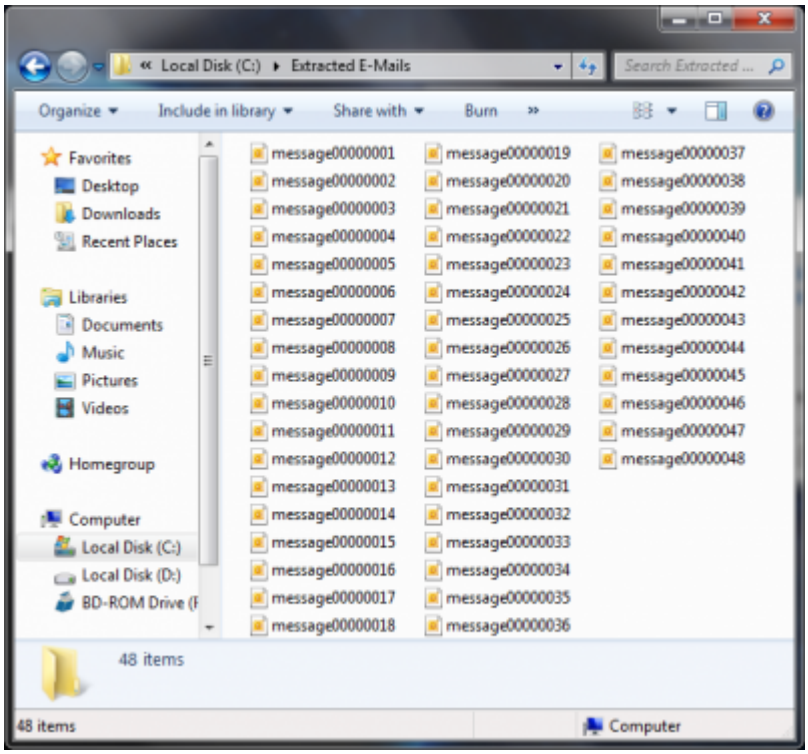
Outlook Extraction Suite

Ovaj alat se koristi za izdvajanje (eng. *extract*) e-mail poruka i privitaka tim porukama iz .pst ili .dbx datoteke. Podržava programe MS Outlook i Outlook Express. Slike ispod prikazuju prve korake prilikom pokretanja alata – izbor e-mail klijenta, što se želi pronaći (poruke, kontakti ili privitci) te gdje se žele pohraniti izdvojeni podaci. Oni se pohranjuju u .eml formatu, što znači da se mogu otvoriti programima MS Outlook, Outlook Express i web preglednicima.



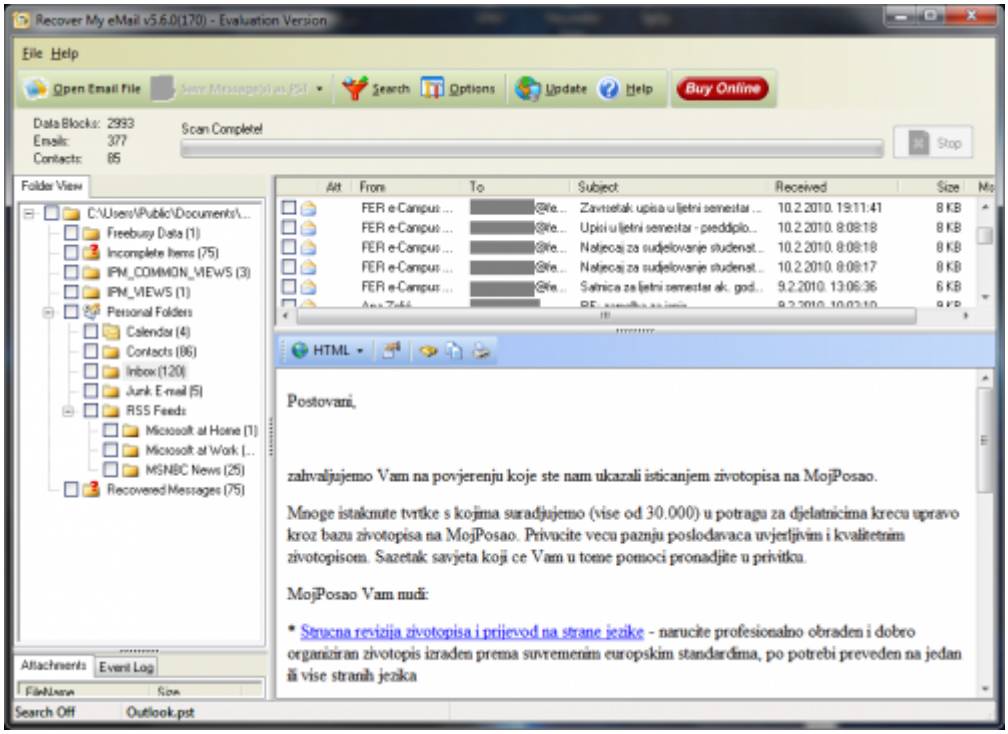




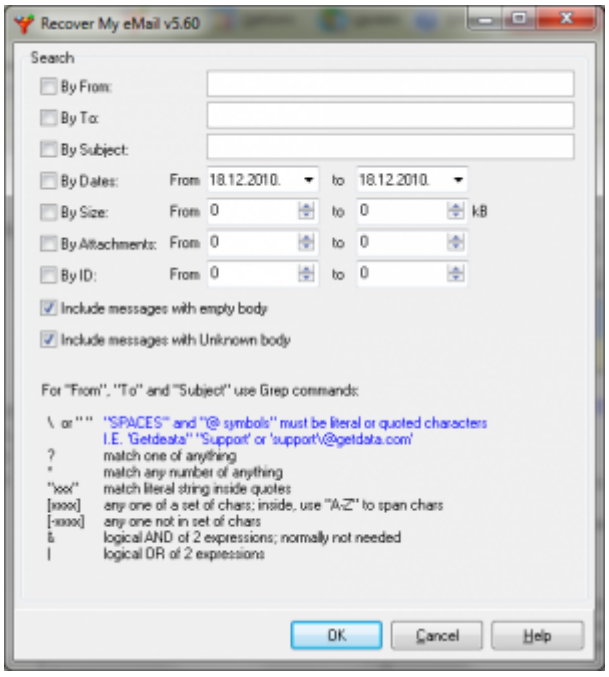


Recover My eMail

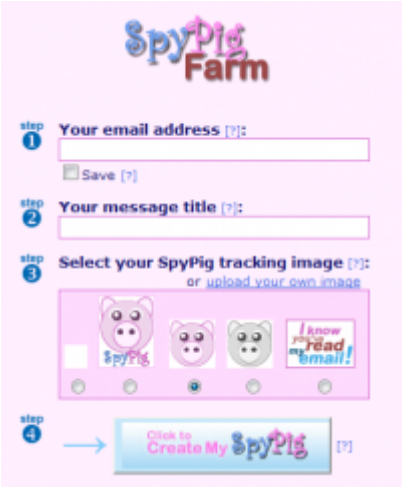
Kao i Outlook Extraction Suite, Recover My eMail rekonstruira poruke iz .pst ili .dbx datoteke te ih pohranjuje u .eml ili .pst formatu.



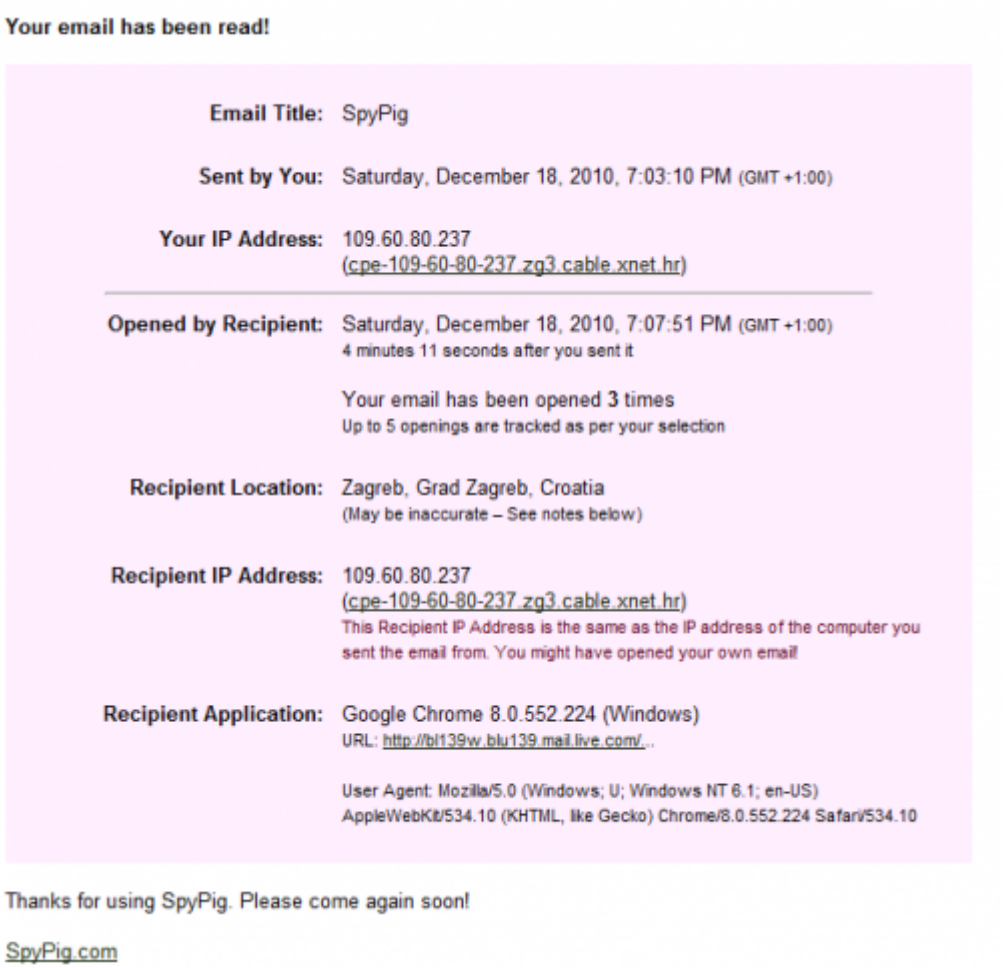
Izdvojena pošta se može filtrirati prema pošiljatelju, primatelju, datumu slanja, temi poruke, veličini poruke i broju privitaka.



SpyPig



SpyPig je alat koji, osim što zabavno izgleda, korisniku daje do znanja kad je poruka koju je poslao pročitana, u kojem gradu, na kojoj IP adresi, u koliko sati, koliko puta je pročitana, u kojem web pregledniku je otvorena i kojim operacijskim sustavom.



I pošiljatelj i primatelj koriste HTML e-mail klijente (Outlook, Eudora, Yahoo e-mail, Gmail, Hotmail, AOL, ...) jer ne funkcionira s običnim tekstualnim (eng. *plain-text*) i bogatim tekstualnim (eng. *rich-text*), a na web stranici je navedeno još poznatih razloga zbog kojih SpyPig možda neće funkcionirati.