Procura della Repubblica
presso il Tribunale di Milano

PROCEDURE INVESTIGATIVE

SUI PRIMI ACCERTAMENTI DI POLIZIA GIUDIZIARIA IN MATERIA DI REATI INFORMATICI

ESTRATTO DAL DOCUMENTO

"DIRETTIVE PER LA POLIZIA GIUDIZIARIA SUI PRIMI ACCERTAMENTI INVESTIGATIVI IN MATERIA DI REATI INFORMATICI E MODALITA' DI TRASMISSIONE DELLE RELATIVE COMUNICAZIONI DI NOTIZIA DI REATOALLA PROCURA DI MILANO"

Versione 1.0 del 5 maggio 2011

Le seguenti procedure investigative sono state formalizzate dal pool reati informatici della Procura di Milano (costituitosi nel 2004 all'interno del VII Dipartimento) in collaborazione con il Compartimento Polizia Postale e delle Comunicazioni per la Lombardia, con il supporto della Squadra Reati Informatici della Sezione Polizia Giudiziaria (che dal 2007 coadiuva il pool reati informatici).

Informazioni che la persona offesa dovrebbe fornire in sede di querela

- ***siti web**:* nome del sito; stampa del contenuto, se il sito non è pedo-pornografico (se contiene immagini di minori è sufficiente il nome della pagina web);

- ***messaggi presenti in newsgroup*[1]*:*** indicazione del nome del newsgroup e del modo di poterlo reperire; stampa del messaggio, se questo non è pedo-pornografico (se contiene immagini di minori è sufficiente spiegare come poterlo reperire);

- ***social network*[2]*:*** nome del *social network* adoperato; giorno e ora dell'attività segnalata; ID *(Identification Number*) dell'utente; ID del gruppo; URL[3] completo del profilo; indirizzi *e-mail* rilevati; stampa del profilo; sunto delle conversazioni avviate all'interno del *social network*;

- ***e-mail**:* copia dell'*e-mail* comprensiva dell'*header* (intestazione[4] del messaggio, nella sua forma estesa) del messaggio e degli allegati (anche se sono relativi a immagini pedo-pornografiche);

- ***chat-line*[5]*:*** giorno e ora della *chat*; nome della *chat* adoperata; *nick name*[6] proprio e dell'utente con cui si è conversato; dati della stanza in cui è avvenuta la conversazione (ad esempio il nome del server[7] e del canale in IRC[8]; la stanza in C6[9]; l'UIN - *Universal ICQ Number*- in ICQ[10]); testo della

[1] Un **newsgroup** è uno degli spazi virtuali creato su una rete di server interconnessi per discutere di un argomento (*topic*) ben determinato. In italiano a volte viene utilizzato il termine **gruppo di discussione** (tratto da wikipedia).
[2] Una **rete sociale** (in inglese ***social network***) consiste di un qualsiasi gruppo di persone connesse tra loro da diversi legami sociali, che vanno dalla conoscenza casuale, ai rapporti di lavoro, ai vincoli familiari. Tra i più diffusi social network vi è Facebook.
[3] Un **Uniform Resource Locator** o **URL** è una sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa in Internet, come un documento o un'immagine (es. *www.giustizia.it*).
[4] Nelle reti informatiche l'**header** (intestazione) di un "messaggio" (ossia di un pacchetto di dati che viaggia in rete) è quella parte che contiene informazioni di controllo necessarie al funzionamento della rete o dello specifico servizio. Si consideri che un messaggio, ad esempio una *e-mail*, prima di essere inviato in rete viene incapsulato in vari protocolli e ognuno di questi aggiunge un *header* con informazioni specifiche. Analizzare gli *header* dei messaggi permette di ricavare alcune informazioni di interesse, sia tecnico che investigativo.
[5] Il termine **chat** (in inglese, letteralmente, "chiacchierata"), viene usato per riferirsi a un'ampia gamma di servizi sia telefonici che via Internet; ovvero, complessivamente, quelli che i paesi di lingua inglese distinguono di solito con l'espressione *"online chat"*, "chat in linea". Questi servizi, anche piuttosto diversi fra loro, hanno tutti in comune due elementi fondamentali: il fatto che il dialogo avvenga in tempo reale, e il fatto che il servizio possa mettere facilmente in contatto perfetti sconosciuti, generalmente in forma essenzialmente anonima. Il "luogo" (lo spazio virtuale) in cui la chat si svolge è chiamato solitamente *chatroom* (letteralmente "stanza delle chiacchierate"), detto anche *channel* (in italiano *canale*), spesso abbreviato *chan*. (tratto da wikipedia).
[6] Nella cultura di Internet, un **nickname** o semplicemente **nick** è uno pseudonimo o "nome di battaglia", usato dagli utenti di Internet per identificarsi in un determinato contesto o in una determinata comunità virtuale. Spesso sono soprannomi, ma possono essere sigle, combinazioni di lettere e numeri. (tratto da wikipedia).
[7] In informatica il termine *server* (in inglese letteralmente *servitore*) indica genericamente un componente informatico che fornisce un qualunque tipo di servizi ad altre componenti (tipicamente chiamate *client*, cioè "cliente") attraverso una rete di computer. (tratto da wikipedia). Di regola con il termine server si indica un computer utilizzato per fornire servizi ad altri computer, a prescindere dalle sue caratteristiche hardware.
[8] **Internet Relay Chat (IRC)** è stata la prima forma di comunicazione istantanea (chat) su Internet. Consente sia la comunicazione diretta fra due utenti che il dialogo contemporaneo di interi gruppi di persone in *stanze* di discussione chiamate *canali*. (tratto da wikipedia).
[9] **C6 Messenger** è un programma di messaggistica istantanea prodotto dal Gruppo Telecom Italia.

conversazione; *log* relativi alla conversazione in *chat*; *file* inviati durante la *chat*;

- ***querela per truffa tramite annuncio di vendita**:* nome del servizio di vendita usato; dati del venditore e del sistema di pagamento adoperato (fomiti direttamente dal gestore del servizio a semplice richiesta delle forze dell'ordine); *e-mail* comprensive di *header* relative ai contatti intrattenuti con il truffatore; indicazione degli elementi che fanno presuppone la truffa, e segnatamente gli artifizi e raggiri posti in essere dal sedicente venditore per conseguire l'ingiusto profitto, che sostanziano il reato distinguendolo dal semplice inadempimento di natura civilistica;

- ***querela per sostituzione di persona**:* nome del servizio attivato in frode e/o a nome del denunciante; indicazioni utili circa il profilo attivato illegittimamente; documentazione relativa all'attività illecita compiuta;

- ***querela per uso indebito di carta di credito/debito**:* indicazione del numero della carta di debito/credito; nome della società proprietaria e della banca emittente possibilmente con l'indicazione della filiale e del relativo numero di conto corrente; copia di estratto conto o lista dei movimenti con indicazione delle operazioni disconosciute effettuate con bancomat/carta di credito; copia degli estratti conti dei movimenti degli ultimi mesi, se possibile; copia fotostatica fronte-retro della carta di credito/debito, se ancora in possesso del denunciante e se ritenuto necessario;

- ***querela per ingiuria/diffamazione**:* copia del contenuto illecito (copia della pagina web, del messaggio o dell' e-mail comprensiva di *header*); eventuale istanza al fornitore del servizio di rimozione dei contenuti offensivi (che, qualora effettuata, rende impossibile la valutazione degli stessi)[11];

- ***querela per accesso abusivo a un sistema informatico**: file* di *log* relativi agli accessi disconosciuti; tipo e versione del sistema in uso; protocolli di comunicazione utilizzati; descrizione del tipo di operazioni illecite e dei danni accertati con eventuale loro qualificazione; nominativi delle persone informate sui fatti; *backup* dei file interessati dalle modifiche o contenenti informazioni relative all'attacco;

- ***querela per frode informatica avvenuta con il dirottamento di chiamate verso codici 899, satellitari e internazionali (00) – traffico dati Internet disconosciuto da intestatario/utilizzatore telefono cellulare**:* copia della bolletta telefonica ove saranno indicate le chiamate disconosciute; indicazioni su come è stato scaricato il *dialer* e su come si adopera e si è protetto il computer utilizzato; tipologia del contratto utilizzato per il traffico dati Internet da telefono cellulare;

- ***querela per frode informatica avvenuta con l'utilizzo fraudolento delle coordinate di home banking**:* lista dettagliata dei movimenti disconosciuti; indicazione se prima delle spendite fraudolente è stato ricevuto un messaggio di posta elettronica relativo al *phishing*; in caso positivo, *header* (intestazione) dell'e-*mail* di *phishing* e messaggio in formato elettronico; verifica di come sono custodite le credenziali di accesso (password,

[10] **ICQ** è il primo programma per computer di instant messaging (messaggi istantanei, chat) nel mondo, creato da Mirabilis, una compagnia start-up israeliana fondata a Tel Aviv. Il programma venne rilasciato per la prima volta nel novembre del 1996. Il nome è un gioco di parole sulla frase "I seek you" (io ti cerco) (tratto da wikipedia).

[11] Il gestore conserva comunque i dati relative all'inserimento del contenuto diffamatorio per un periodo di tempo variabile.

token[12]) e del fatto che la persona offesa abbia recentemente subito attività anomale (quali un furto).

- ***querela per intrusione centralini telefonici VOIP*[13]*:*** fattura telefonica con dettagli del traffico disconosciuto anche parzialmente oscurato, informazioni sulla configurazione del centralino telefonico e sull'accesso abusivo subito, *file* di *log* relativi alle violazioni, nominativi delle persone informate sui fatti.

[12] Un **token per la sicurezza** (chiamato anche **token hardware**, **token per l'autenticazione**, **token crittografico**, o semplicemente **token**) è un dispositivo fisico necessario per effettuare un'autenticazione (tipicamente una autenticazione a due fattori). Un *token* si presenta spesso sotto forma di dispositivo elettronico portatile di piccole dimensioni, alimentato a batteria con autonomia nell'ordine di qualche anno, dotato di uno schermo e talvolta di una tastiera numerica. Alcuni *token* possono essere collegati ad un computer tramite una porta USB per facilitare lo scambio di dati. Un *token* può anche essere di tipo software, ove le informazioni necessarie risiedono direttamente nel computer dell'utente, e non in un oggetto esterno (tratto da wikipedia).

[13] Con telecomunicazioni in **Voice over IP** (*Voce tramite protocollo Internet*), acronimo **VoIP**, si intende una tecnologia che rende possibile effettuare una conversazione telefonica sfruttando una connessione Internet o un'altra rete dedicata che utilizza il protocollo IP senza connessione per il trasporto dati (tratto da Wikipedia).

Leggere e stampare l'*header* di una *e-mail*

Il messaggio di posta elettronica o *e-mail* è costituito da:

- una busta (*envelope*)[14];
- un corpo del messaggio (*body*) [15];
- una sezione di intestazioni (*header*).

Le intestazioni (*header*) sono informazioni di servizio che servono a controllare l'invio del messaggio, o a tener traccia delle manipolazioni che subisce.
Ciascuna intestazione è costituita da una riga di testo, con un nome seguito dal carattere ':' e dal corrispondente valore. Alcune di queste vengono ***definite e possono essere modificate*** direttamente dall'utente. Tra le principali si possono citare:

- **Subject: (Oggetto:)** dovrebbe contenere una breve descrizione dell'oggetto del messaggio; **From: (Da:)** contiene l'indirizzo di posta elettronica del mittente;
- **To: (A:)** contiene gli indirizzi di posta elettronica dei destinatari principali;
- **Cc:** contiene gli indirizzi di posta elettronica dei destinatari in copia conoscenza (Carbon Copy);
- **Bcc: (Ccn:)** contiene gli indirizzi di posta elettronica dei destinatari in copia conoscenza nascosta (*Blind Carbon Copy*), ovvero destinatari che riceveranno il messaggio ma il cui indirizzo non apparirà tra i destinatari. Questa è in realtà una pseudo-intestazione, in quanto è visibile solo al mittente del messaggio, e per definizione non viene riportata nei messaggi inviati ai destinatari;
- **Reply-to: (Rispondi a:)** contiene l'indirizzo di posta elettronica al quale devono essere inviate le eventuali risposte al messaggio, se diverso da quello del mittente;
- **Date: (Data:)** contiene la data e l'ora in cui il messaggio è stato scritto.

Le intestazioni di servizio vengono aggiunte dai programmi che manipolano il messaggio.
La più importante è **Received:**, che viene aggiunta da ciascun *server* SMTP che manipola il messaggio, indicando da quale indirizzo ***IP il messaggio è stato ricevuto, a che ora, e altre informazioni utili a tracciarne il percorso***.

Il **Message-ID:** (Identificativo del messaggio) è un codice costruito dal *client* su cui il messaggio è stato composto, che dovrebbe permettere di identificare univocamente un messaggio (fonte Wikipedia).

La visualizzazione delle intestazioni (*header*), varia a seconda dei *client*[16] e/o delle *webmail*[17] di posta utilizzate, di cui di seguito si forniscono alcune indicazioni.

[14] Per busta si intendono le informazioni a corredo del messaggio che vengono scambiate tra server attraverso il protocollo SMTP, principalmente gli indirizzi di posta elettronica del mittente e dei destinatari. Queste informazioni normalmente corrispondono a quelle che è possibile ritrovare nelle intestazioni, ma possono esserci delle differenze (fonte Wikipedia).
[15] Il corpo e gli allegati costituiscono il contenuto informativo che il mittente vuol comunicare ai destinatari. Esso era originalmente composto di testo semplice. In seguito è stata introdotta la possibilità di inserire dei file in un messaggio di posta elettronica (allegati), ad esempio per inviare immagini o documenti. Per fare questo il client di posta del mittente utilizza la codifica MIME (o la più desueta uuencode).
Gli allegati vengono utilizzati anche per comporre un messaggio di posta elettronica in formato HTML, generalmente per ottenere una più gradevole visualizzazione dello stesso.
[16] Un *client* di posta è un programma che consente di gestire la composizione, la trasmissione, la ricezione e l'organizzazione di *e-mail* (i messaggi di posta elettronica) da e verso un *server* di posta (fonte Wikipedia).
[17] Una *Webmail* è un'applicazione web che permette di gestire uno o più account di posta elettronica attraverso un navigatore web (fonte Wikipedia).

A) Client:

- Mozilla Thunderbird

- aprire Mozilla Thunderbird;
- evidenziare il messaggio dal quale si desidera visualizzare le intestazioni;
- scegliere **Sorgente del messaggio** (Ctrl+U) dal menu **Visualizza** (**Figura 7**);
- si aprirà una finestra nella quale è cosi possibile visualizzare *l'header* completo (**Figura 8**);
- si può copiare e incollare il testo nel Blocco Note, in un Word Processor e quindi stamparlo.

Figura 1

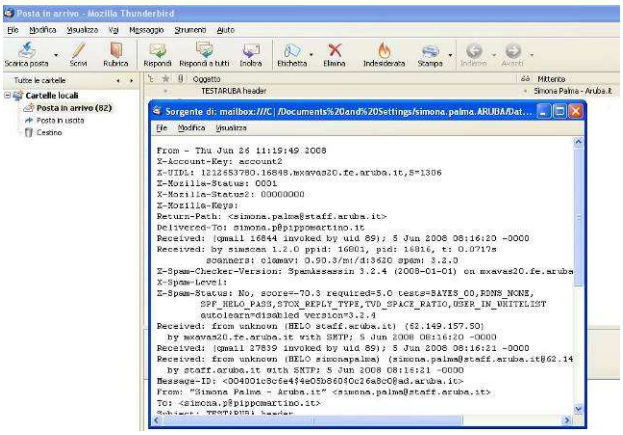


Figura 2

- Outlook Express

- aprire Outlook Express;
- evidenziare il messaggio del quale si desidera visualizzare le intestazioni;
- fare *click* con il tasto destro del *mouse*, apparirà un menù a tendina da cui scegliere l'ultima voce **Proprietà** (**Figura 9**);
- si aprirà una finestra e nella cartella Dettagli sarà possibile visualizzare *l'header* completo (**Figura 10**);
- si può copiare e incollare il testo nel Blocco Note, in un Word Processor e quindi stamparlo.

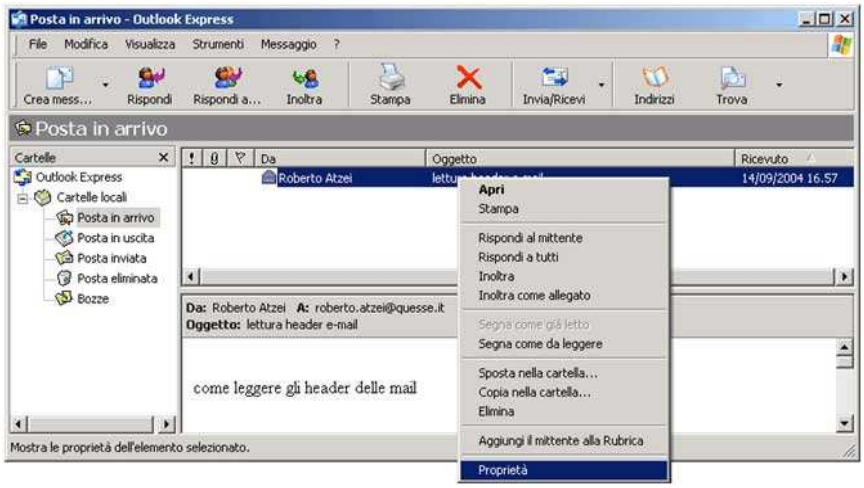
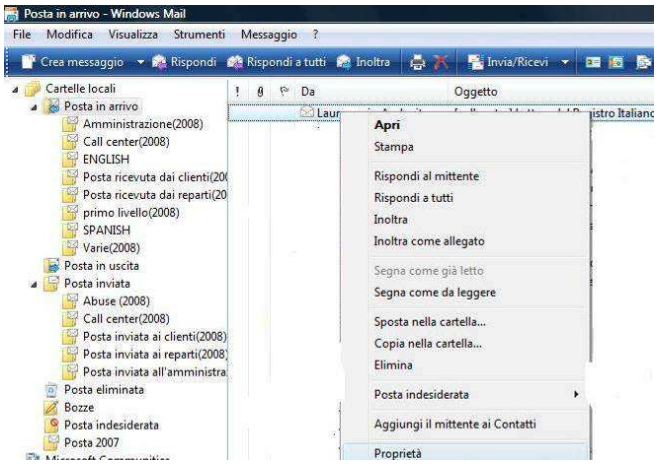


Figura 3

Figura 4

- **Windows Mail**

- aprire Windows Mail;
- evidenziare il messaggio del quale si desidera visualizzare le intestazioni;
- fare *click* con il tasto destro del *mouse*, apparirà un menù a tendina da cui scegliere l'ultima voce **Proprietà** (**Figura 11**);
- si aprirà una finestra e nella cartella Dettagli sarà possibile visualizzare *l'header* completo (**Figura 12**);
- si può copiare e incollare il testo nel Blocco Note, in un Word Processor e quindi stamparlo.



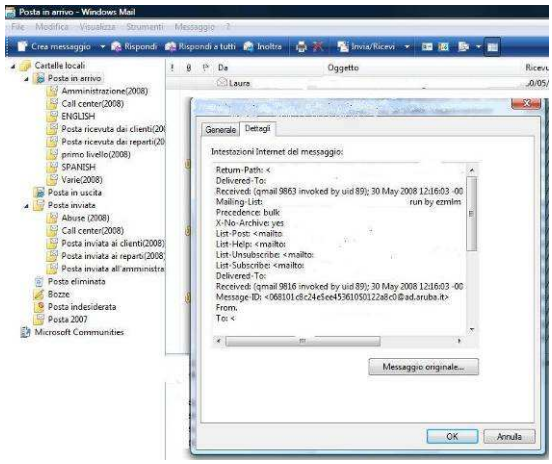
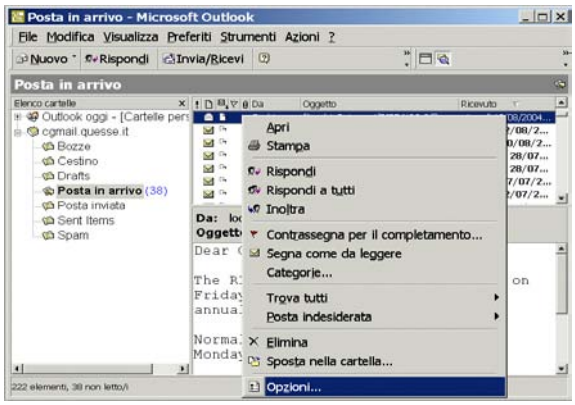


Figura 5 **Figura 6**

- **Outlook 2000**

- aprire Outlook;
- evidenziare il messaggio del quale si desidera visualizzare le intestazioni;
- fare *click* con il tasto destro del *mouse*, apparirà un menù a tendina da cui scegliere l'ultima voce **Opzioni** (**Figura 13**);
- si aprirà una finestra e nella casella Intestazioni Internet sarà possibile visualizzare *l'header* completo (**Figura 14**);
- si può copiare e incollare il testo nel Blocco Note, in un Word Processor e quindi stamparlo.



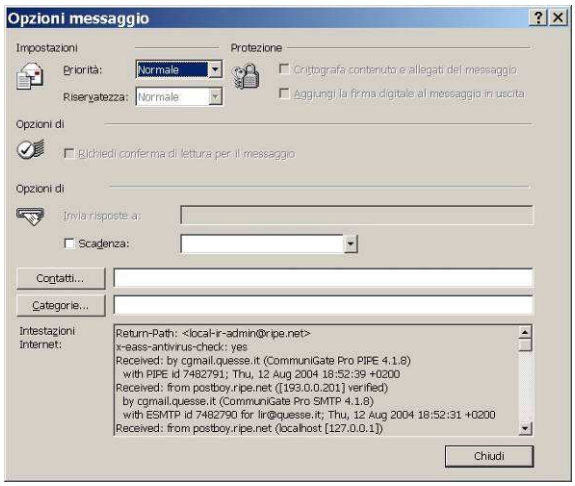


Figura 7 **Figura 8**

- **Outlook 2007/2010**

- aprire Outlook;
- aprire il messaggio del quale si desidera visualizzare le intestazioni;
- fare *click* sulla freccia rivolta verso il basso accanto a **Categorie** nella cartella **Messaggi** (**Figura 15**);
- si aprirà una finestra e nella casella Intestazioni Internet sarà possibile visualizzare *l'header* completo (**Figura 16**);
- si può copiare e incollare il testo nel Blocco Note, in un Word Processor e quindi stamparlo.

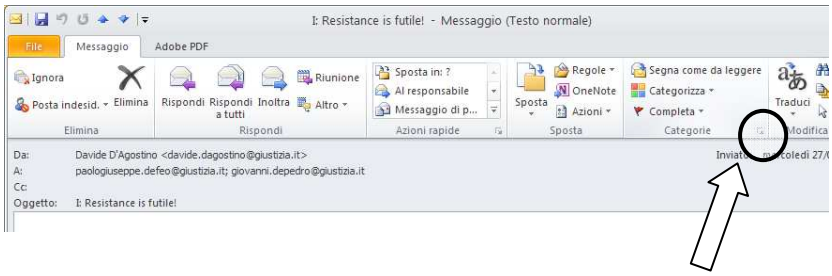


Figura 9

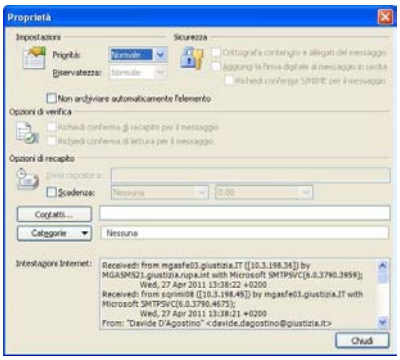


Figura 10

- **Mail di Apple**

- aprire Mail di Apple;
- aprire il messaggio del quale si desidera visualizzare le intestazioni;
- selezionare dal menù **Vista** la voce **Messaggio** e scegliere **Intestazioni lunghe** (è anche possibile una combinazione breve di tasti Mela + Maiuscole + h) (**Figura 17**);
- si può copiare e incollare il testo nel Blocco Note, in un Word Processor e quindi stamparlo.

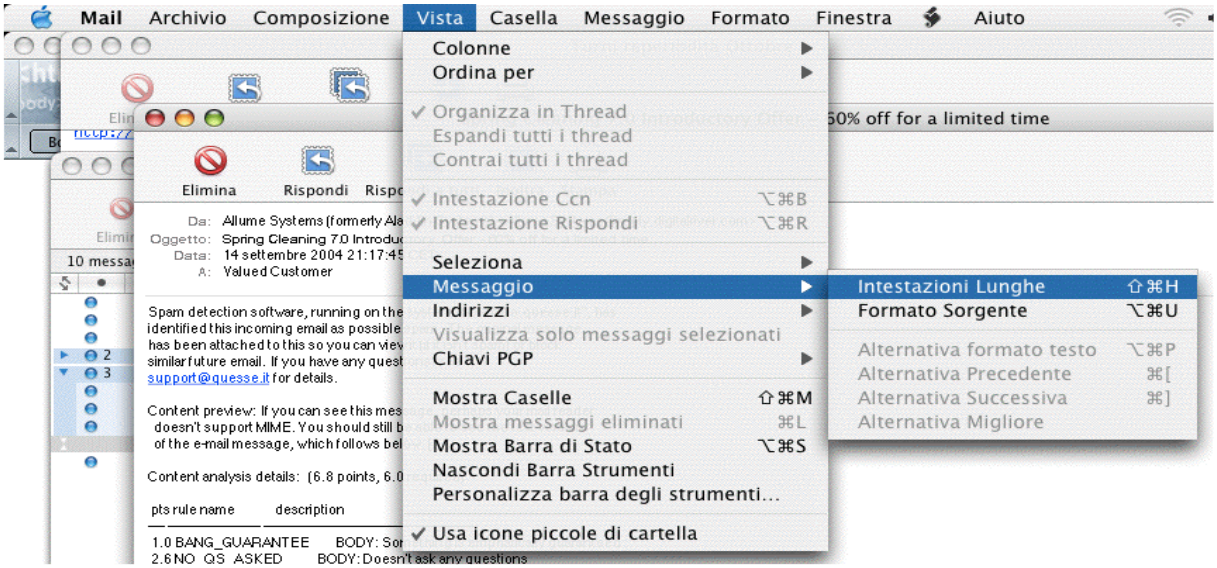


Figura 11

B) Webmail:

- Gmail

- accedere all'*account* Gmail.
- aprire il messaggio del quale si desidera visualizzare le intestazioni.
- fare *click* sulla freccia rivolta verso il basso accanto a **Rispondi**, nell'angolo in alto a destra della finestra del messaggio;
- selezionare **Mostra originale** (**Figura 18**);
- si aprirà una finestra nella quale è cosi possibile visualizzare *l'header* completo (**Figura 19**);
- si può stampare o copiare e incollare il testo nel Blocco Note, in un Word Processor e quindi stamparlo.

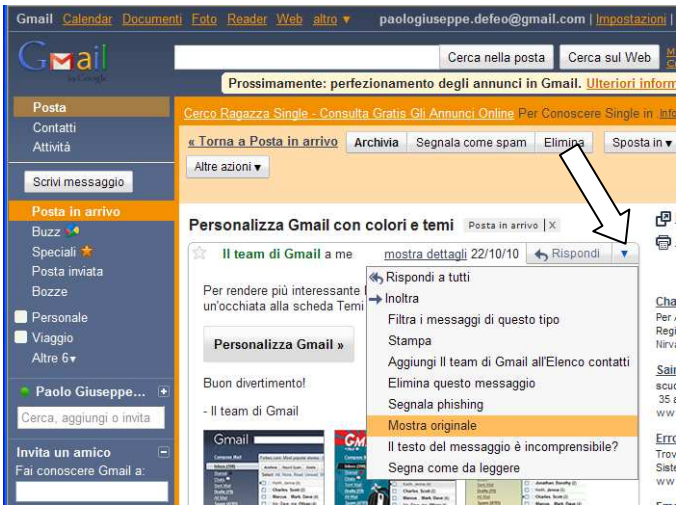


Figura 12

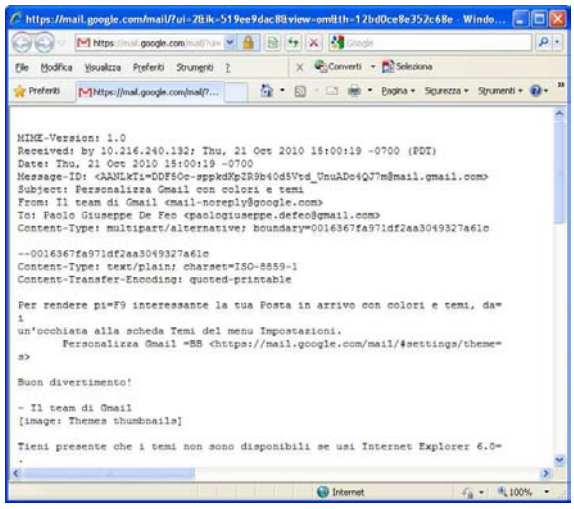


Figura 13

- Windows Live - Hotmail

- accedere all'*account* Gmail;
- selezionare **Posta in arrivo** (*Inbox*) nel menù di sinistra e fare *click* con il pulsante destro del mouse sul messaggio del quale si desidera visualizzare le intestazioni e apparirà un menù a tendina da cui scegliere l'ultima voce **Visualizza intestazione completa** (*View messagge source*) (**Figura 20**);
- si aprirà una finestra nella quale è cosi possibile visualizzare *l'header* completo (**Figura 21**);
- si può stampare o copiare e incollare il testo nel Blocco Note, in un Word Processor e quindi stamparlo.

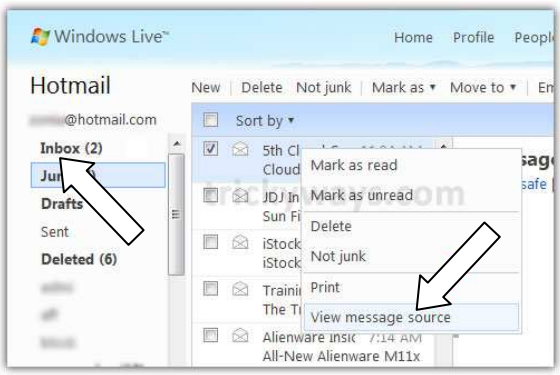


Figura 14

Figura 15

- **Yahoo! Mail**

- accedere all'*account* Yahoo! Mail;
- selezionare **Posta in arrivo** (*Inbox*) ed evidenziare il messaggio del quale si desidera visualizzare le intestazioni (**Figura 22**);
- fare *click* su **Azioni** (*Actions*) e dal menu a discesa scegliere l'ultima voce **Visualizza intestazione completa** (*Full Header*) (**Figura 23**);
- si aprirà una finestra nella quale sarà cosi possibile visualizzare *l'header* completo;
- si può stampare o copiare e incollare il testo nel Blocco Note, in un Word Processor e quindi stamparlo.

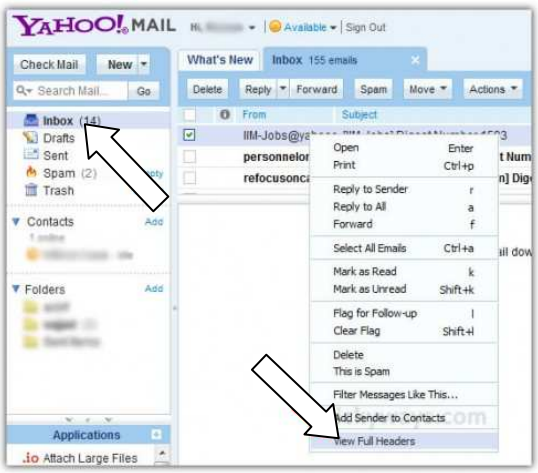


Figura 16

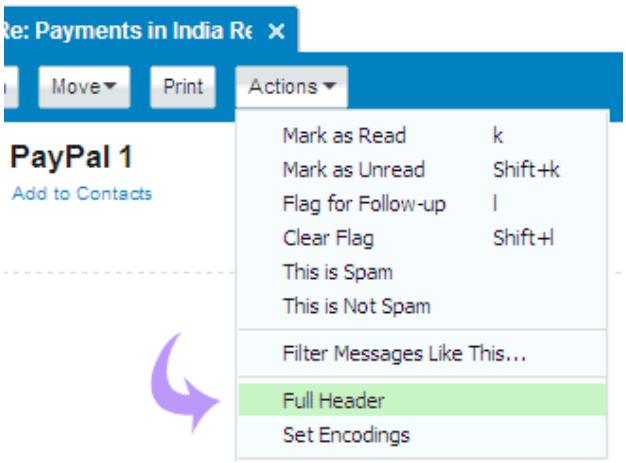


Figura 17

- **Libero**

- accedere all'*account* Libero;
- selezionare **Posta arrivata** ed aprire il messaggio del quale si desidera visualizzare le intestazioni;
- fare *click* su **Altre azioni**, nella parte bassa e dal menu selezionare **Mostra intestazioni** (**Figura 24**);
- verrà visualizzato *l'header* completo (**Figura 25**);
- si può stampare direttamente o copiare e incollare il testo nel Blocco Note, in un Word Processor e quindi stamparlo.

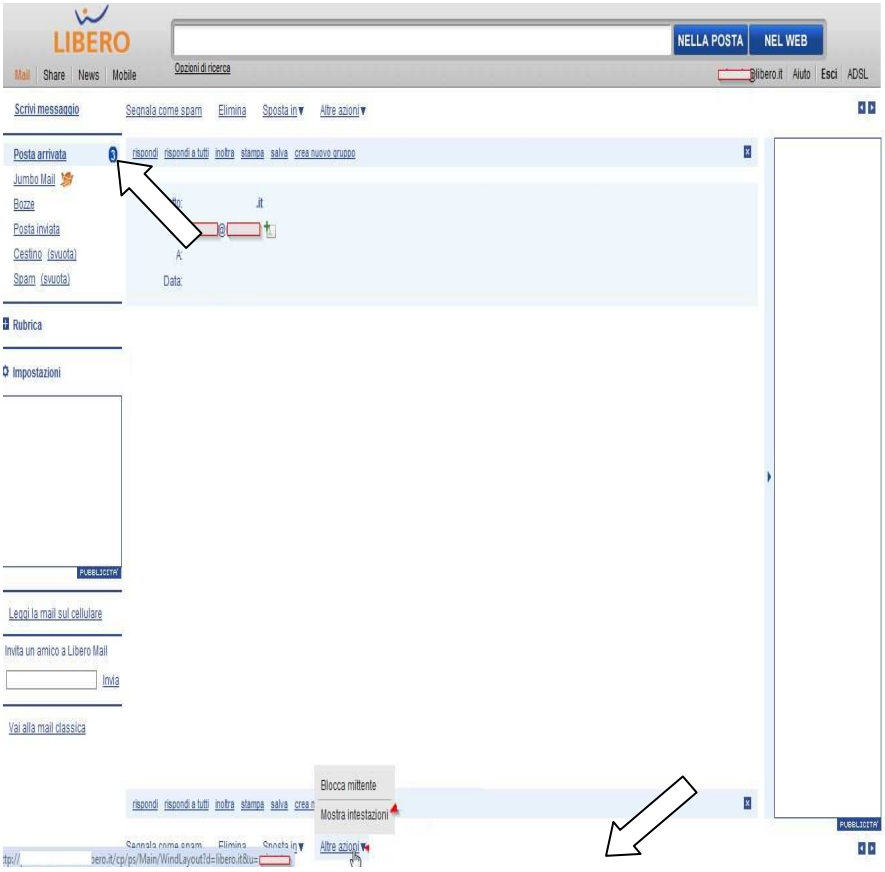


Figura 18

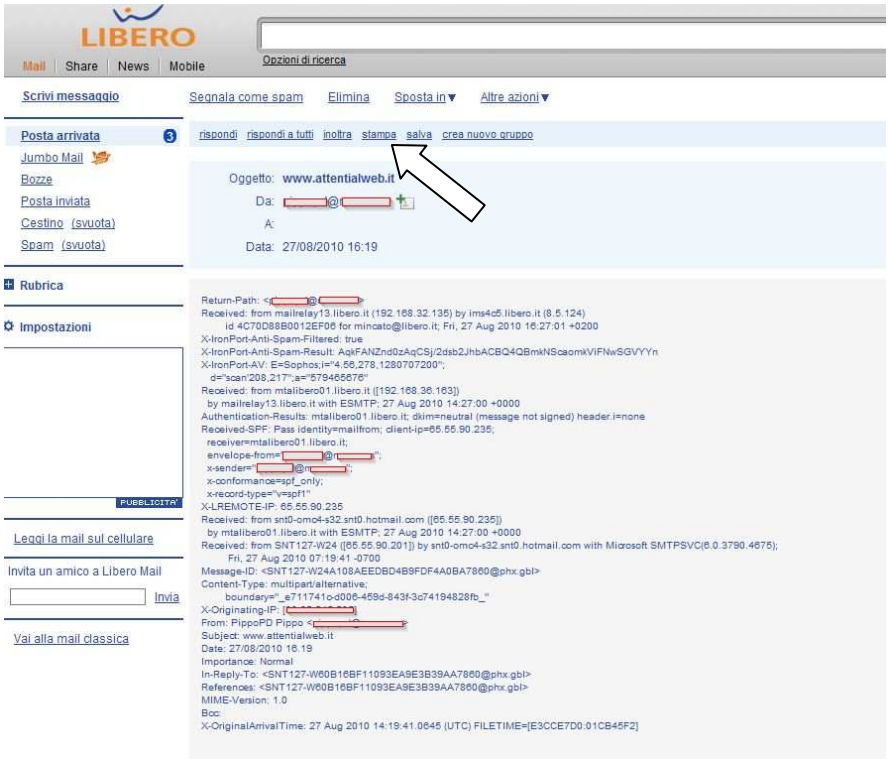


Figura 19