

---

## Reati di pedopornografia in ambiente P2P

Analisi dei file di log per ricostruire  
attività di scambio tra vari utenti indagati

*Michele Ferrazzano*  
*michele.ferrazzano@unibo.it*

### Scenario

---

- Verificare detenzione e divulgazione di materiale pedopornografico
- Indice argomenti trattati
  - Scenario normativo
  - Obiettivi dell'analisi forense (nel caso specifico)
  - Aspetti tecnici di eMule
  - Esempio di analisi forense su eMule
    - eMuleForensic

## Scenario normativo – Art. 600-ter c.p.

---

### Art. 600-ter – Pornografia minorile

#### *Produzione e commercio*

1. Chiunque, utilizzando minori degli anni diciotto, **realizza esibizioni pornografiche o produce materiale pornografico** ovvero induce minori di anni diciotto a partecipare ad esibizioni pornografiche è punito [...]
2. Alla stessa pena soggiace chi fa **commercio del materiale pornografico di cui al primo comma**.

## Scenario normativo – Art. 600-ter c.p.

---

### Art. 600-ter – Pornografia minorile

#### *Divulgazione (anche a titolo gratuito)*

3. Chiunque, al di fuori delle ipotesi di cui al primo e al secondo comma, con qualsiasi mezzo, **anche per via telematica, distribuisce, divulga, diffonde o pubblicizza il materiale pornografico di cui al primo comma, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto**, è punito [...]
4. Chiunque, al di fuori delle ipotesi di cui ai commi primo, secondo e terzo, **offre o cede ad altri, anche a titolo gratuito, il materiale pornografico di cui al primo comma**, è punito [...]

## Scenario normativo – Art. 600-ter c.p.

---

### Art. 600-ter – Pornografia minorile

#### *Ingente quantità*

5. Nei casi previsti dal terzo e dal quarto comma la pena è aumentata in misura non eccedente i due terzi ove il materiale sia di **ingente quantità**.

## Scenario normativo – Art. 600-quater c.p.

---

### Art. 600-quater – Detenzione di materiale pornografico

#### *Detenzione*

1. Chiunque, al di fuori delle ipotesi previste dall'articolo 600-ter, **consapevolmente si procura o detiene materiale pornografico realizzato utilizzando minori degli anni diciotto**, è punito [...]
2. La pena è aumentata in misura non eccedente i due terzi ove il materiale detenuto sia di **ingente quantità**.

## Scenario normativo – Art. 600-*quater*.1 c.p.

---

### **Art. 600-*quater*.1 – Pornografia virtuale**

#### *Pornografia virtuale e definizione*

1. Le disposizioni di cui agli articoli 600-ter e 600-*quater* si applicano **anche quando il materiale pornografico rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto o parti di esse**, ma la pena è diminuita di un terzo.
2. Per immagini virtuali si intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

## Scenario normativo – Art. 600-*sexies* c.p.

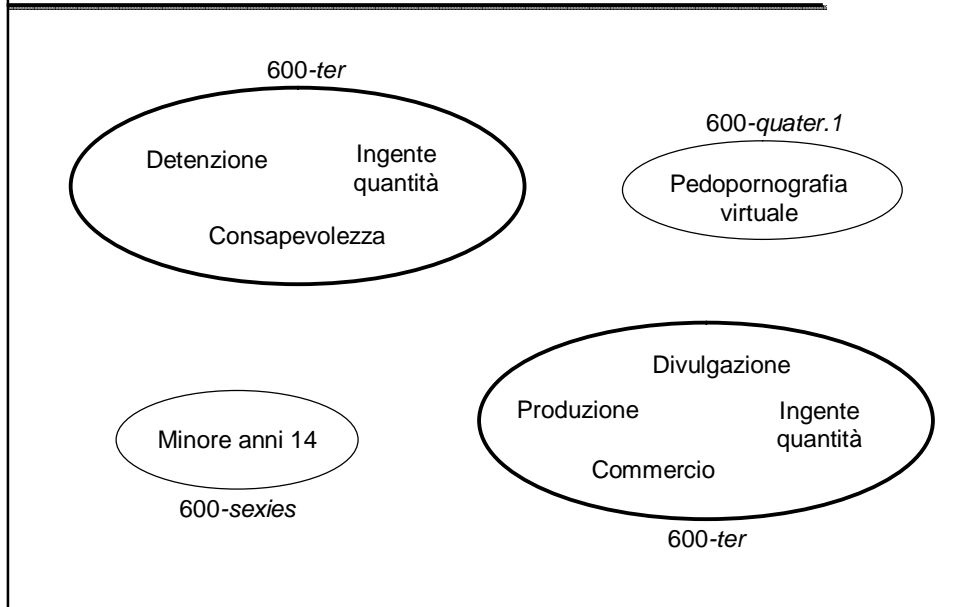
---

### **Art. 600-*sexies* – Circostanze aggravanti ed attenuanti**

#### *Pornografia virtuale e definizione*

1. Nei casi previsti dagli articoli 600-bis, primo comma, 600-ter, primo comma, e 600-*quinqies* la pena è aumentata da un terzo alla metà se **il fatto è commesso in danno di minore degli anni quattordici [...]**

## Aspetti chiave emersi dagli articoli letti



## Aspetti chiave - Detenzione

- La detenzione è consapevole?
  - Art. 600-quater c.p., comma 1
    - *"Chiunque, al di fuori delle ipotesi previste dall'articolo 600-ter, **consapevolmente** si procura o detiene materiale pornografico"*
- Quantità
  - Art. 600-quater c.p., comma 2
    - *"La pena è aumentata in misura non eccedente i due terzi ove il materiale detenuto sia di **ingente quantità**"*
- Provenienza
  - Art. 600-ter c.p., comma 1
    - *"Chiunque, utilizzando minori degli anni diciotto, **realizza esibizioni pornografiche o produce materiale pornografico** ovvero induce minori di anni diciotto a partecipare ad esibizioni pornografiche e' punito [...]"*

## Aspetti chiave - Divulgazione

---

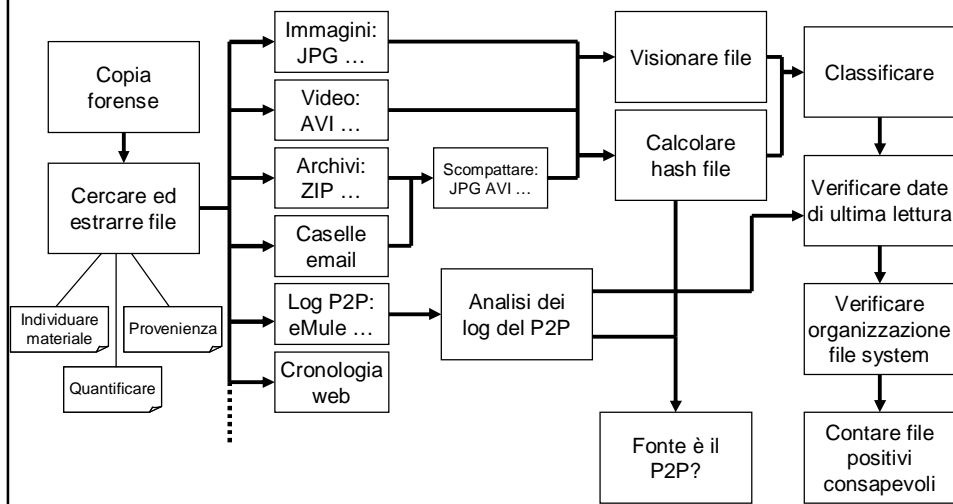
- C'è stata divulgazione?
  - Art. 600-ter c.p., commi 3 e 4
    - *“Chiunque, al di fuori delle ipotesi di cui al primo e al secondo comma, con qualsiasi mezzo, **anche per via telematica, distribuisce, divulga, diffonde o pubblicizza** il materiale pornografico di cui al primo comma, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto, è punito [...]”*
    - *“Chiunque, al di fuori delle ipotesi di cui ai commi primo, secondo e terzo, offre o cede ad altri, anche a titolo gratuito, il materiale pornografico di cui al primo comma, e' punito [...]”*
- Quantità
  - Art. 600-ter c.p., comma 5
    - *“Nei casi previsti dal terzo e dal quarto comma la pena e' aumentata in misura non eccedente i due terzi ove il materiale sia di **ingente quantità**”*

## Aspetti chiave - Divulgazione

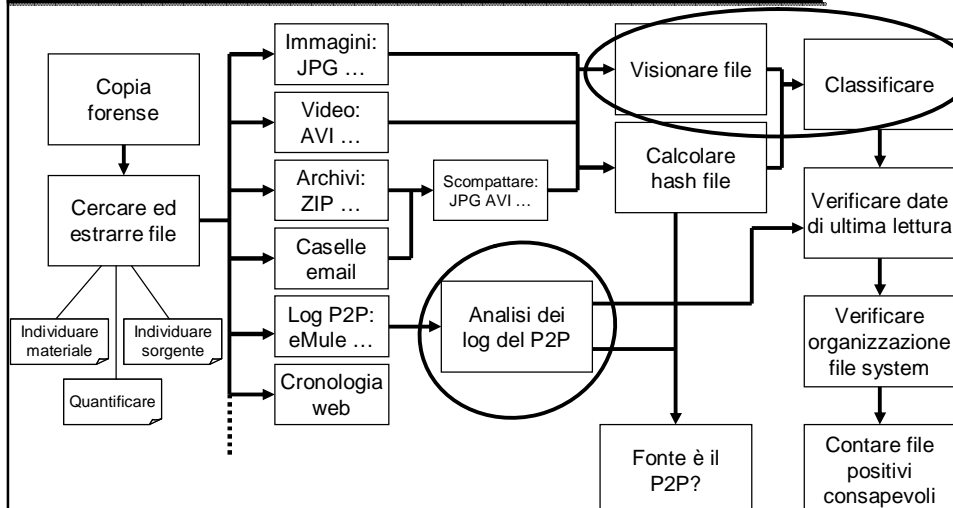
---

- L'invio è avvenuto con profitto?
  - Art. 600-ter c.p., comma 2
    - *“Alla stessa pena soggiace **chi fa commercio** del materiale pornografico di cui al primo comma”*
- Consapevolezza
  - **Nessun riferimento alla consapevolezza nella divulgazione...**

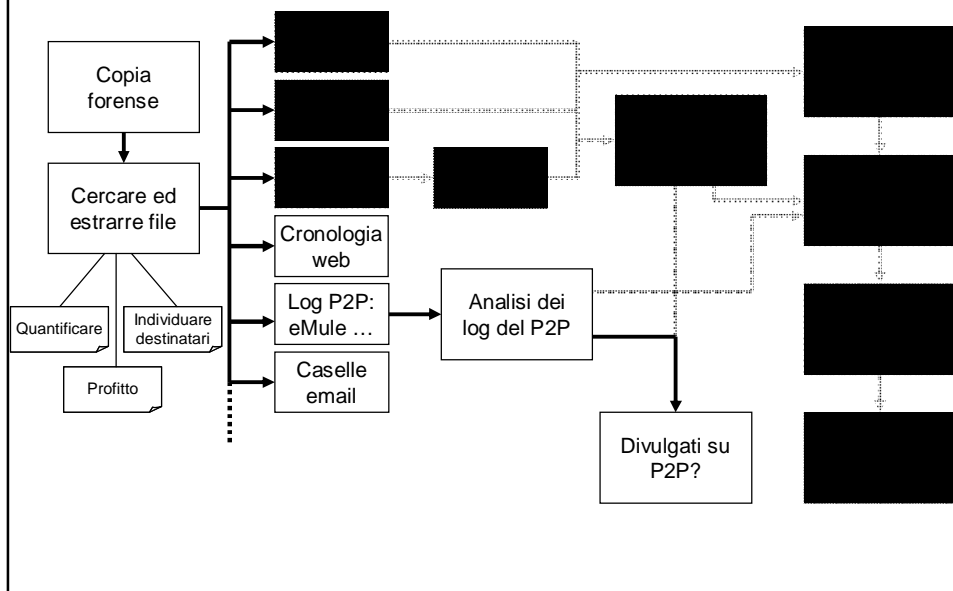
## Analisi per detenzione: workflow



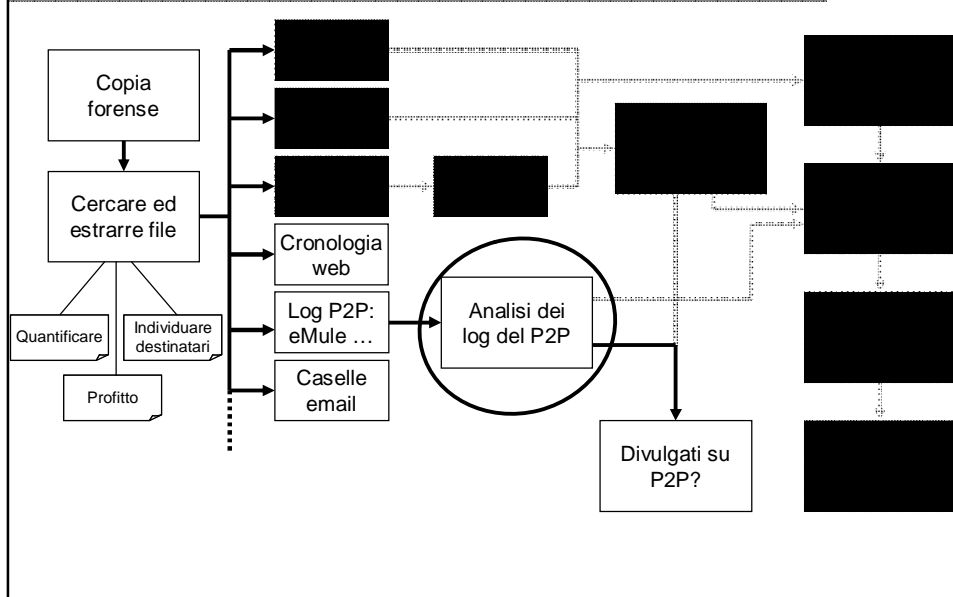
## Analisi per detenzione: workflow



## Analisi per divulgazione: workflow



## Analisi per divulgazione: workflow





## Obiettivi dell'analisi forense

---

- Individuare e quantificare file a contenuto pedopornografico
  - Se possibile, classificare il materiale per età dei soggetti raffigurati
    - *(possibilità di utilizzo di tecniche di riconoscimento automatico)*
- Individuare le fonti
  - P2P, siti, email...
- Individuare elementi che consentano di determinare la consapevolezza
  - Keyword di ricerca, organizzazione del file system, date di accesso...
- Individuare elementi che consentano di determinare se c'è stata divulgazione e in che quantità
  - In subordine, individuare elementi che permettano di capire se lo scambio è avvenuto dietro pagamento

## Obiettivi dell'analisi forense

---

### **Individuare e quantificare file a contenuto pedopornografico e, se possibile, classificare il materiale per età dei soggetti raffigurati**

- Attività più semplice
- Ricerca e conta dei file presenti sui supporti
  - Attenzione ai cambi di estensione, file zippati, file cifrati, cartelle in rete
- Se possibile, classificare il materiale per età dei soggetti raffigurati
  - Tecniche di riconoscimento automatico
  - Chi fa analisi forense è esperto di informatica, non di anatomia!
    - Difficile stabilire con esattezza l'età (es: visi asiatici)

## Obiettivi dell'analisi forense

---

### **Individuare le fonti**

- File sharing
- Siti internet
- Email
- Gruppi di chat
- Copia da altri supporti
- ...

*Concentriamoci sul file sharing...*

## Obiettivi dell'analisi forense

---

### **Individuare elementi che consentano di stabilire la consapevolezza**

- Finora abbiamo parlato di elementi oggettivi (individuare file presenti, contarli, trovare una fonte)
- La consapevolezza è un concetto astratto
  - Il consulente tecnico si limita a mettere in evidenza elementi concreti
  - Il giudice valuta gli elementi ed esprime il giudizio
- Quali elementi utili per determinare la (in)consapevolezza?
  - Parole chiave di ricerca
  - Organizzazione dei file nel file system
  - Date di ultima lettura, ultima modifica e di creazione
  - Nomi dei file (file *fake*)

## Obiettivi dell'analisi forense

---

**Individuare elementi che consentono di determinare se c'è stata divulgazione e in che quantità; in subordine, individuare elementi che permettano di determinare se lo scambio è avvenuto dietro pagamento**

- Esempi “facili”
  - Per le email, vedere la posta inviata
  - Per il web, pubblicazione di materiale su proprio sito
- E per il file sharing su P2P?
  - La divulgazione di file è automatica ed incontrollabile! Anche quando un file è ancora in scaricamento... e magari non è corrispondente ai propri interessi

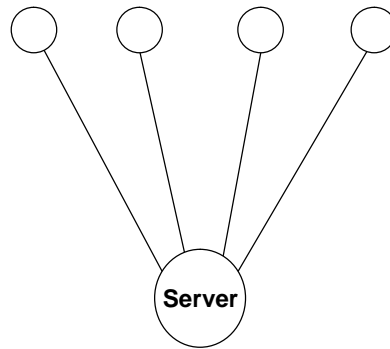
## Peer to peer

---

- Una rete *peer-to-peer* è una rete distribuita in cui ogni partecipante è direttamente disponibile a comunicare con un altro partecipante
  - In antitesi con il paradigma client-server
- Esempio “nobile” di applicazione del peer to peer:
  - GRID
    - SETI@home (oltre 5.000.000 di partecipanti)
      - analizzare segnali radio in cerca di forme di vita extraterrestri

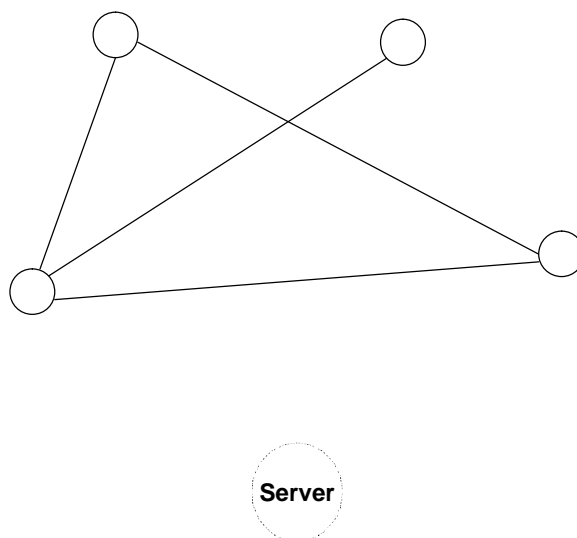
## Client-server

---

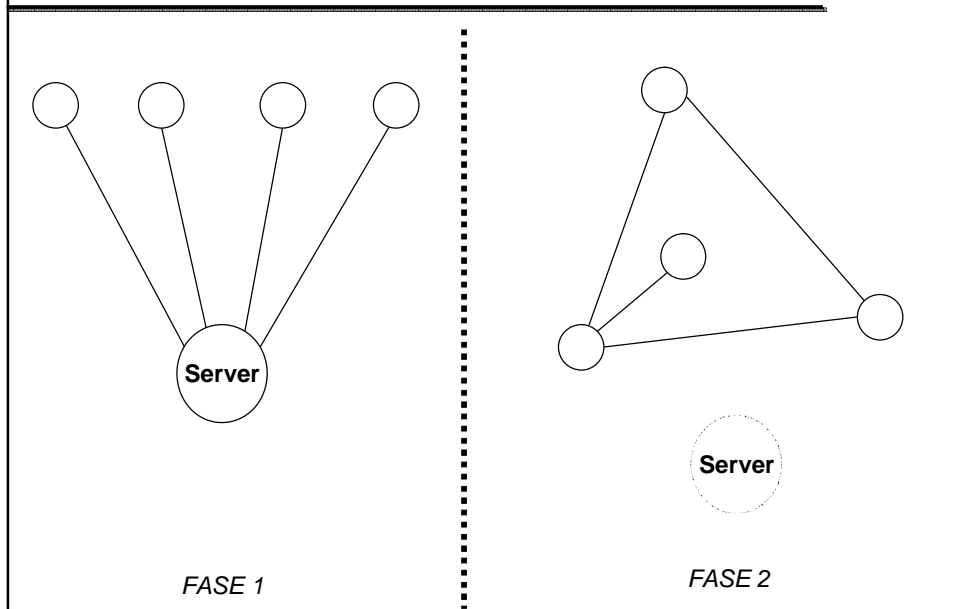


## Peer-to-peer puro

---



## Peer-to-peer ibrido



## eMule

- Software di file sharing su rete P2P (eDonkey, ibrida)
- Open source
  - Numerose mod
    - Versioni alternative con funzionalità aggiuntive
      - eMule Xtream, eMule MorphXT, eMule Adunanza...
    - Ultima versione 0.50a (eseguibile e codice sorgente)
      - <http://sourceforge.net/projects/emule/>
      - È il software più scaricato da sourceforge (oltre 500.000.000 di download)
- Fini forensi
  - **Dal sorgente è possibile comprendere come vengono gestiti i file e i trasferimenti, procedendo alla ricostruzione dopo che si sono verificate**

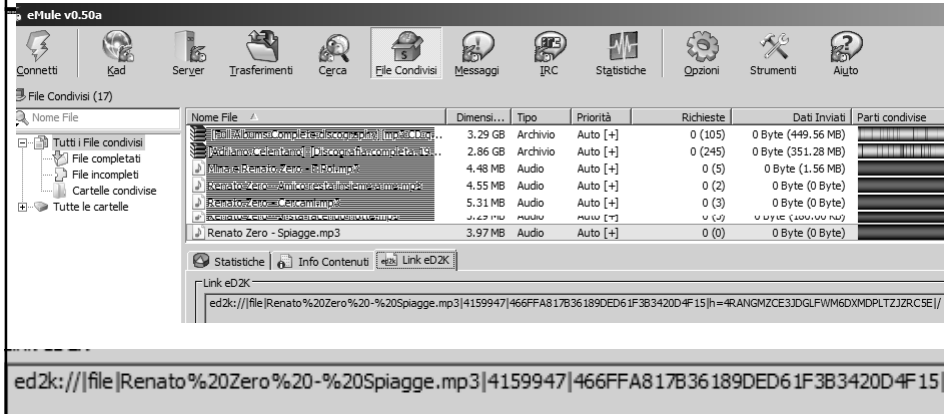
## eMule - I file

- Ogni file è identificato nella rete con un **File ID**
  - Calcolato con funzione hash MD4 (128 bit)
- Il nome del file non è identificativo del file
  - È utilizzato unicamente in fase di ricerca
  - Dopo aver individuato il file, eMule prende in considerazione il file-id associato al file su cui si fa doppio click
  - Il nome del file su cui si fa doppio click sarà utilizzato anche come nome del file nel sistema in cui si scarica il file

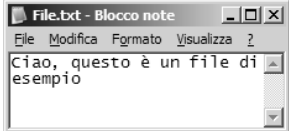
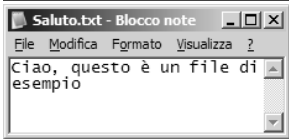
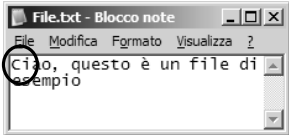
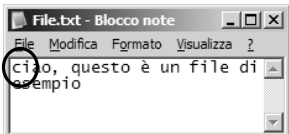
## eMule - I file (ricerca)

Nome File	ID File	Dimensi...	Dis...
Renato Zero - Spiagge.mp3	466FFA817B36189DED61F3B3420D4F15	3.97 MB	75
Renato Zero - 09 - Spiagge.mp3	3A9FBD375D9B99DDF9AEA256AF0AED33	7.07 MB	28
08 - Renato Zero - Prometeo (CD 1) - Spiagge.mp3	9A6DEB356B83997F05392FA1145A62A0	3.82 MB	12
01 - Renato Zero - Calore - Spiagge.mp3	6555980A74A0D044AED2E51FE9145C5F	4.02 MB	10

## eMule - I file (scaricamento)



# eMule – i file

<div> <div>File.txt</div> <div>  </div> </div> <div> <div>Saluto.txt</div> <div>  </div> </div>	<p>Hanno lo stesso contenuto (cioè hanno lo stesso hash MD4)</p> <p>Hanno nomi diversi, sono salvati/creati in giorni diversi</p> <p>=&gt;</p> <p>In eMule sono lo stesso file</p>
<div> <div>File.txt</div> <div>  </div> </div> <div> <div>File.txt</div> <div>  </div> </div>	<p>Non hanno lo stesso contenuto (cioè non hanno lo stesso hash MD4)</p> <p>Hanno nomi uguali, sono salvati/creati lo stesso giorno</p> <p>=&gt;</p> <p>In eMule sono file diversi</p>

## eMule - I file

---

- **Il filename non è identificativo, né univoco**

- File con contenuti identici hanno stesso hash, ma possono avere nomi diversi
  - Renato Zero - spiagge.mp3
  - Renato\_Zero-spiagge.mp3
  - Vasco Rossi - Bollicine.mp3
  - 13yo sex ass young raygold.zip
- File con contenuti diversi hanno hash diversi, ma possono avere stesso nome
- Le ricerche di file si basano sul filename
  - **Rischio di fake**
    - Il filename e l'estensione non forniscono una rappresentazione del contenuto
    - Esempio: il file "Pinocchio.avi" non necessariamente contiene un cartone animato; potrebbe trattarsi di un film di altro genere, di un brano musicale, di un file zippato, di un video pedopornografico...

## Effetti dei file fake

---

- Utente Tizio

- Ricerca con keyword "Vasco Rossi"
- Doppio click su "Discografia Vasco Rossi al 2011.zip"
- File scaricato con contenuto pedopornografico

---

- Filename

- Negativo

- Hash/contenuto pedopornografico

- **Positivo**

- Intenzione di ricercare materiale pedopornografico

- No

- Utente Tizio

- Ricerca con keyword "sex young"
- Doppio click su "13yo sex ass young raygold.zip"
- File scaricato con contenuto pedopornografico

---

- Filename

- **Positivo**

- Hash/contenuto pedopornografico

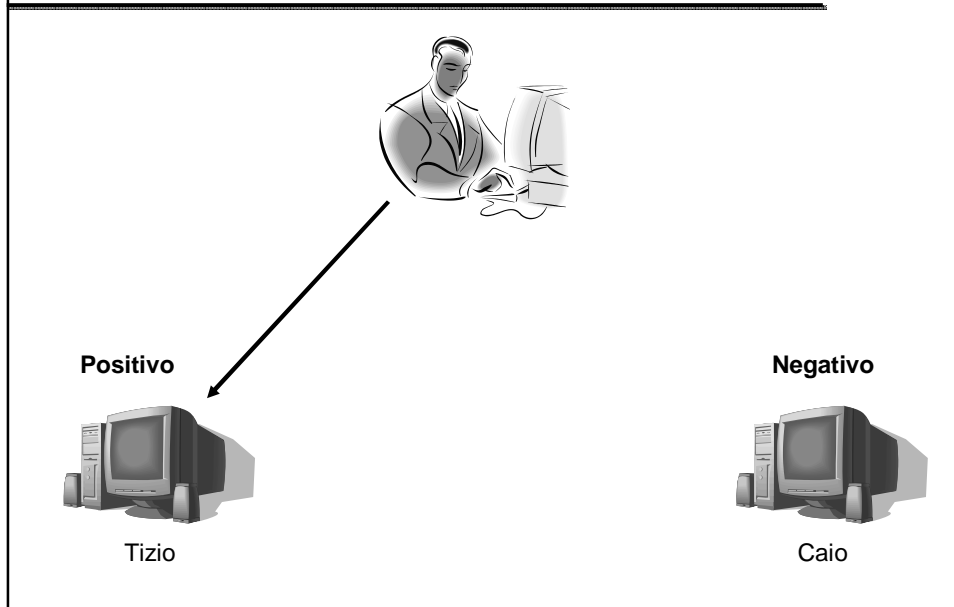
- Negativo

- Intenzione di ricercare materiale pedopornografico

- **Si**



## Effetti dei file fake



## eMule – Gli utenti

- Ogni istanza di eMule è identificata nella rete da uno **User ID**
  - Costituito da 128 bit
  - Generato casualmente al primo avvio di eMule
    - Simile ad un hash, ma non lo è
  - Scopi
    - Sistema dei crediti
    - Ogni utente di mantenere traccia degli utenti remoti con i quali c'è stato almeno uno scambio in download e in upload
      - Ogni utente conserva in un file (*clients.met*) l'elenco degli User ID dei corrispondenti remoti e il volume dello scambio
- **Scopo forense**
  - Utilizzando opportunamente gli User ID e incrociando gli hash dei file è possibile ricostruire la divulgazione dei file utilizzando eMule

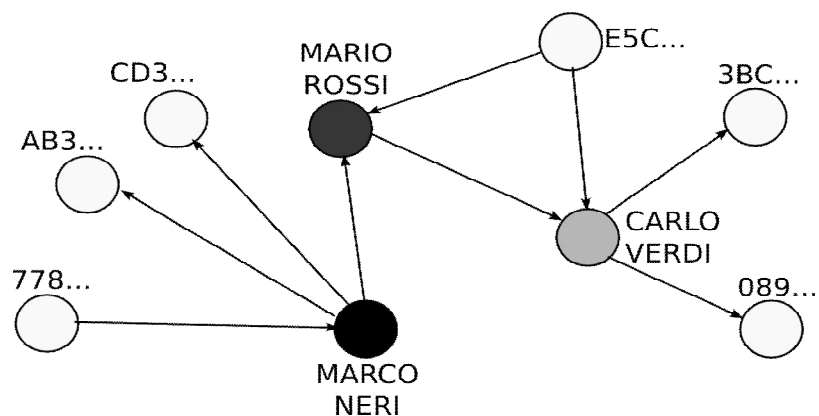
## eMuleForensic

---

- Caso pratico
  - *Massive forensics*: grosse quantità di dati
    - Molti indagati
      - circa 100
    - Molti dischi
      - Media di 4 hard-disk a testa, per un totale di circa 400
    - Molti file
      - Alcuni dischi con oltre 1.000 file a contenuto illecito
      - Alcuni utenti con oltre 10.000 file scambiati con eMule

## eMuleForensic

---



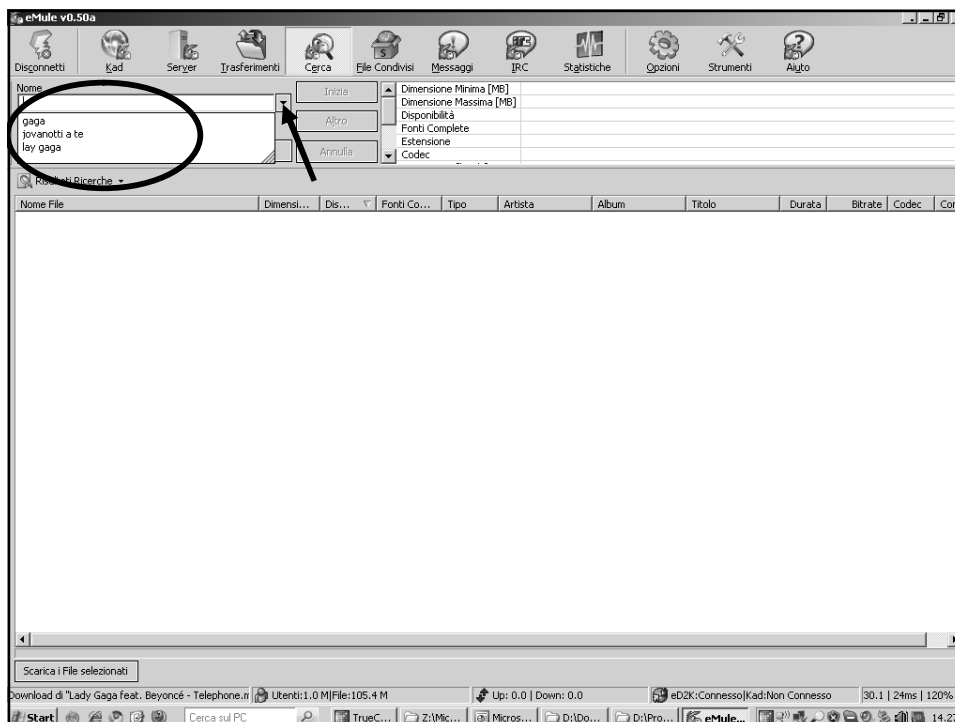
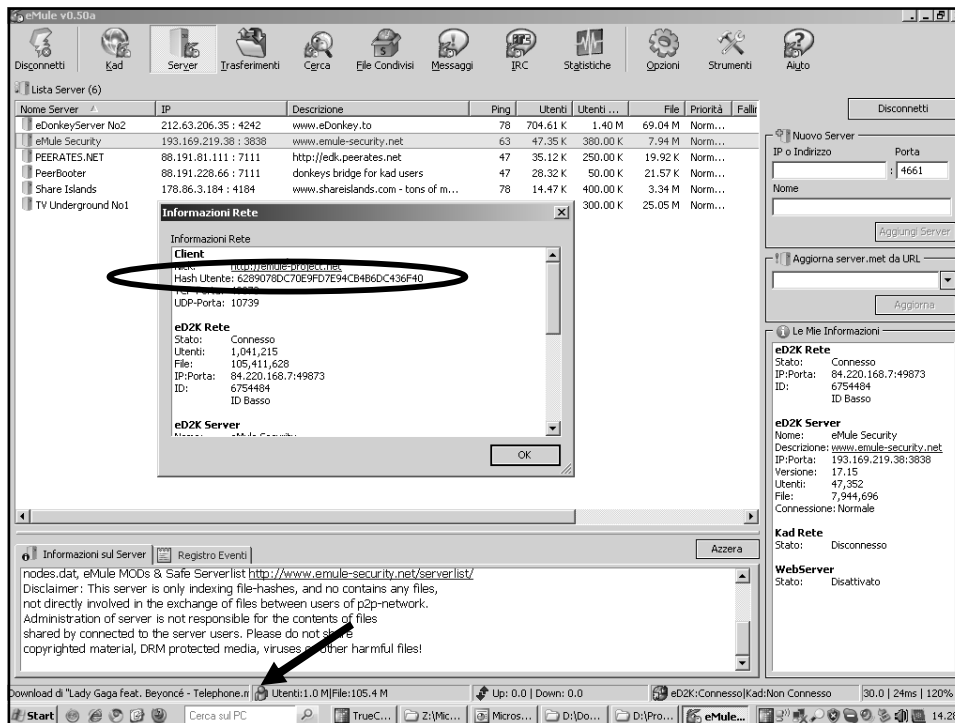
# Analisi forense

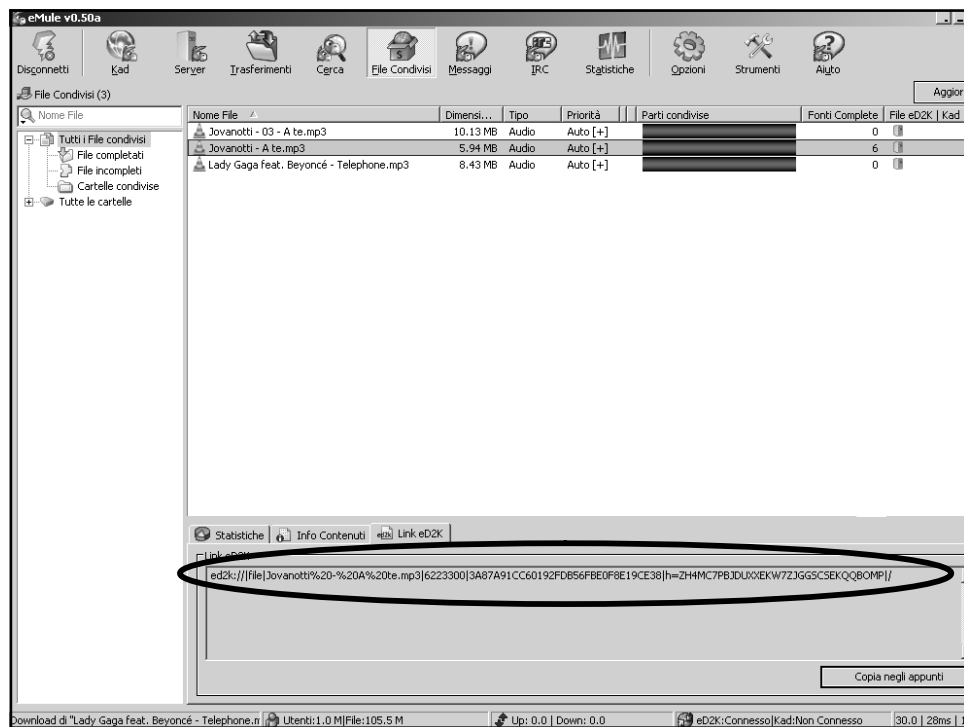
senza eMuleForensic

## Ricerca di file nel disco

---

- Indipendente dalla fonte
  - File sharing, siti web...
- Identificazione dei file “positivi”
  - Visualizzazione del contenuto
    - Visualizzazione delle varie immagini e dei vari video
      - *Con alcuni software di riconoscimento automatico*
  - Parole chiave nel filename (insufficiente)
    - Alcuni esempi: *lolita, 9yo, 13yo, preteen, raygold...*
  - Hash dei file
    - Calcolo del digest tutti i file presenti sul disco
    - Necessità di un database di hash di file positivi





Analisi forense di eMule  
utilizzando eMuleForensic

## eMuleForensic

---



- Semplifica e velocizza l'analisi forense per ricostruire le attività dell'utente di eMule
  - Analizza file di configurazione di eMule per evidenziare
    - **Parole chiave** utilizzate per la ricerca di file
      - Elemento forte per stabilire la consapevolezza
    - **File condivisi**
      - Conoscenza di nome, hash, dimensione, data di ultima modifica dei file senza necessità di visualizzarli
    - **Utenti remoti** con cui c'è stata comunicazione
      - Ricostruire agevolmente **relazioni** di scambio tra utenti
    - **File divulgati**
      - Quantità di invii (volte e quantità di byte)

## eMuleForensic

---

- Semplifica e velocizza l'analisi forense per ricostruire le attività dell'utente di eMule
  - Output in formato XML
    - Linguaggio di markup, definisce documenti strutturati
    - Possibilità di incrociare dati di utenti diversi
- La versione “base” è disponibile via web (<http://emuleforensic.cirsfid.unibo.it>) e nella distribuzione DEFT 7.1.
- Quasi ultimata una versione Java che comprende anche analisi degli hash e analisi incrociata

## Detenzione e consapevolezza

- File di configurazione di eMule
  - *AC\_SearchString.dat*
    - Elenco di keyword di ricerca
  - *Known.met*
    - 
      - È possibile associare i file scaricati con le keyword utilizzate in fase di ricerca
    - 
      - Disponendo di un archivio di hash di file positivi, è possibile determinare le informazioni presenti in un file senza visualizzarne il contenuto

```

notroot@ubuntu:~/Desktop/esempi/35_hexdump_known.met
00000000 8a0e 0035 4600 5046 0000 0000 0000 0000
00000010 0000 0000 0000 0000 0000 0000 0000 0000
00000020 0001 0c01 6c00 3070 3130 3936 2e32 706a
00000030 0367 0001 5c02 0239 8300 0001 0519 0000
00000040 0200 0001 2027 3600 5155 4b36 3741 4c42
00000050 4f54 3737 4148 524e 4540 4534 4233 5634
00000060 535a 3258 533a 0356 0001 72d1 e4ff b847
00000070 9cf4 7145 38ca 0000 efb2 be9b 2485 650d
00000080 0551 1bea 3000 3b79 6646 cb49 9553 9c22
00000090 37a7 7196 e46f 0000 6366 7194 157b 3b59

```

**File "known.met" visualizzato con un editor esadecimale**

[illegible]

File "known.met" visualizzato con un editor di testo

## Vari file (principale srchybrid/Packet.cpp)

<known.met>	::= 0x0e <File details list>
<File details list>	::= DWORD <File details>*
<File details>	::= 0x02 <Date> <File hash> <Meta tag list>
<known.v04.met>	::= 0x0e DWORD <File details v04>*
<File details v04>	::= <Date> <File hash> <Part hash list> <Meta tag list>
<Date>	::= DWORD
<File hash>	::= HASH
<Part hash list>	::= WORD HASH*
<Meta tag list>	::= DWORD <Meta tag>*
<Meta tag>	::= 0x00 Undefined
	= 0x01 <Meta tag name> HASH
	= 0x02 <Meta tag name> <String>
	= 0x03 <Meta tag name> DWORD
	= 0x04 <Meta tag name> FLOAT
	= 0x05 <Meta tag name> BOOL
	= 0x06 <Meta tag name> BOOL Array
	= 0x07 <Meta tag name> BLOB

## Vari file (principale srchybrid/Packet.cpp)

<Meta tag name>	::= WORD <Special tag>	<Special tag>	::= 0x01 // name
	= <String>		= 0x02 // size: size of file
<eMule special tag>	::= 0x20 // Compression		= 0x03 // type: Audio, Video...
	= 0x21 // UDP client port		= 0x04 // format: file extension
	= 0x22 // UDP version		= 0x05 // Collection (depricated)
	= 0x23 // Source exchange		= 0x06 // Part Path
	= 0x24 // Comments		= 0x07 // Part Hash
	= 0x25 // Extended request		= 0x08 // copied
	= 0x26 // Compatible client		= 0x09 DATA // gap start
<String>	::= <String length> DATA		= 0x0a DATA // gap end
<String length>	::= WORD		= 0x0b // description
DATA	: Data of custom length		= 0x0c // ping
DWORD	: 4 bytes integer		= 0x0d // fail
HASH	: MD4 (16 byte)		= 0x0e // preference
			= 0x0f // port
			= 0x10 // ip
			= 0x11 // version
			= 0x12 // tempfile
			= 0x13 // priority
			= 0x14 // status
			= 0x15 // availability
			= 0x16 // QTime
			= 0x17 // Parts
			= <eMule special tag>

## Analisi forense con eMuleforensic

### Divulgazione

- File di configurazione di eMule

- Preferences.dat

- [redacted] dell'utente indagato
    - nell'esempio  
90257D2DB80E4CEC6D386092  
B0936F1D

- Clients.met

- [redacted]
    - Possibilità di determinare il volume di dati scambiati in [redacted] e in [redacted]

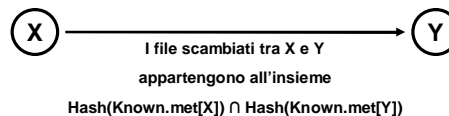
```
notroot@ubuntu:~/Desktop/esempi$ hexdump 3/preferences.dat
00000000 4a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000010 2d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000020 ffff ffff ffff ffff ffff ffff 0aff 0000
00000030 0a00 0000 1700 0003 5300 0002 0000
0000003d
```

File "preferences.dat" visualizzato con un editor esadecimale

```
notroot@ubuntu:~/Desktop/esempi$ hexdump 3/clients.met
00000000 9012 0038 00 49 5dc8
00000010 0047 0000 0000 0000 0000 4c00 4a30 0d30
00000020 0906 862a 8648 0df7 0101 0501 0300 0039
00000030 3630 3102 b000 5866 91ef c814 d080 96d3
00000040 bdac 2f18 d391 dc9f 6ad7 e48c 61a9 2894
00000050 c01c 6979 8c37 ea82 d485 05b8 4484 bb99
00000060 f554 60c6 020f 1101 0000 0000 7fa4 16c1
00000070 0ef9 9f2f f206 1059 98b7 976f 6a0f 0093
00000080 0000 0000 7e72 4789 0000 0000 0000 0000
00000090
```

File "clients.met" visualizzato con un editor esadecimale

- Possibilità di incrociare questi due file con il file *known.met* per definire le relazioni di scambio





## srchybrid/preferences.h

---

```
struct Preferences_Ext_Struct{
    uint8          version;
    uchar          userhash[16];
    WINDOWPLACEMENT EmuleWindowPlacement;
};
```

## srchybrid/ClientCredits.h

---

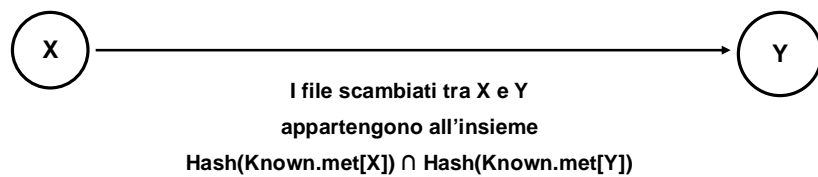
```
struct CreditStruct_29a{
    uchar          abyKey[16];        // userhash
    uint32          nUploadedLo;      // uploaded TO him
    uint32          nDownloadedLo;    // downloaded from him
    uint32          nLastSeen;
    uint32          nUploadedHi;      // upload high 32
    uint32          nDownloadedHi;    // download high 32
    uint16          nReserved3;
};

struct CreditStruct{
    uchar          abyKey[16];        // userhash
    uint32          nUploadedLo;      // uploaded TO him
    uint32          nDownloadedLo;    // downloaded from him
    uint32          nLastSeen;
    uint32          nUploadedHi;      // upload high 32
    uint32          nDownloadedHi;    // download high 32
    uint16          nReserved3;
    uint8          nKeySize;
    uchar          abySecureIdent[MAXPUBKEYSIZE];
};
```

## Analisi forense con eMuleforensic

### Associazione tra utenti

- Possibilità di incrociare dati dei file
    - Preferences.dat
    - Clients.met
    - Known.met
- per definire le relazioni di scambio



## Analisi forense con eMuleforensic

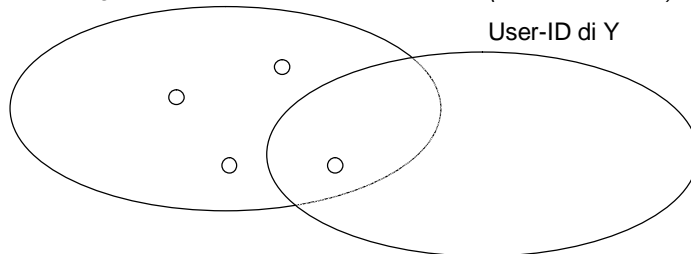
### Associazione tra utenti

(Clients.met)

User-ID degli utenti remoti di X

(Preferences.dat)

User-ID di Y



## Analisi forense con eMuleforensic

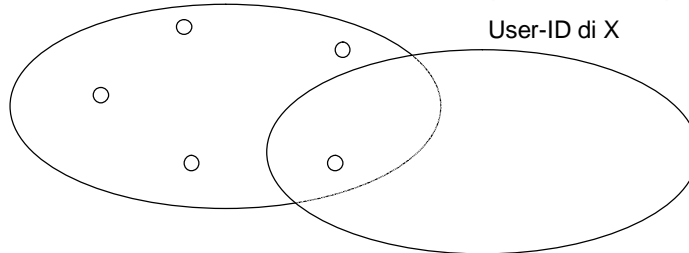
### Associazione tra utenti

(Clients.met)

User-ID degli utenti remoti di Y

(Preferences.dat)

User-ID di X



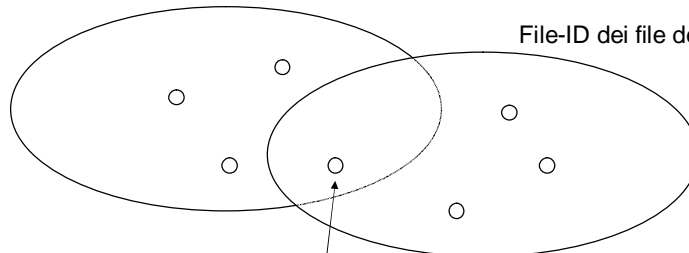
**X conosce Y, Y conosce X => X e Y hanno scambiato dei file**

## Analisi forense con eMuleforensic

### Associazione tra utenti

File-ID dei file dell'utente X

File-ID dei file dell'utente Y




**File scambiato**

## eMuleForensic - Esempio

```
notroot@ubuntu: ~/Desktop
File Modifica Visualizza Terminale Ajuto
notroot@ubuntu:~/Desktop$ date
ven mag 7 05:29:56 EDT 2010
notroot@ubuntu:~/Desktop$ emuleforensic -i esempi/3/ -o 3.xml -c 00001 -d
Descrizione -e Michele
Converting AC_SearchStrings.dat... [OK]
Converting preferences.dat... [OK]
Converting clients.met... [OK]
Converting known.met... [OK]
All operations completed with success!
notroot@ubuntu:~/Desktop$ date
ven mag 7 05:29:59 EDT 2010
notroot@ubuntu:~/Desktop$
```

## eMuleForensic – Esempio web

# emuleforensic




[Homepage](#) [Use it!](#) [My account](#) [Contact](#) [Logout](#)

### emuleforensic - Use it

Please, filenames must be "known.met", "clients.met", "preferences.dat" and "AC\_SearchStrings.dat".

Case number:	<input type="text" value="1"/>
Case description:	<input type="text" value="Descrizione"/>
Examiner name	<input type="text" value="Michele"/>
File <i>known.met</i> to upload	<input type="text" value="C:\Documents and Settings\michele.ferrazza"/> <a href="#">Sfoglia...</a>
File <i>clients.met</i> to upload	<input type="text" value="C:\Documents and Settings\michele.ferrazza"/> <a href="#">Sfoglia...</a>
File <i>preferences.dat</i> to upload	<input type="text" value="C:\Documents and Settings\michele.ferrazza"/> <a href="#">Sfoglia...</a>
File <i>AC_SearchStrings.dat</i> to upload	<input type="text" value="C:\Documents and Settings\michele.ferrazza"/> <a href="#">Sfoglia...</a>
<input type="button" value="Convert in xml"/>	



(C) 2011 Michele Ferrazzano  
emuleforensic is a forensics software for eMule, hosted on [CIRSID](#) server

<http://emuleforensic.cirsid.unibo.it>

## eMuleForensic – Esempio web

# emuleforensic



[Homepage](#) [Use it!](#) [My account](#) [Contact](#) [Logout](#)

### emuleforensic - Use it

#### Report

- *Date and time:* 22/02/11-11:36:55
- *Case 1:* Descrizione
- *Examinator:* Michele
- *User hash:* AED572D4A90E863FF609DBC237476F4D

[Keywords](#) | [Client](#) | [File](#)

#### Keywords (from AC\_SearchString.dat)

- shakira loca
- shakira loca
- shakira - loca
- ...
- ...
- ...

## eMuleForensic – Esempio web

...

...

...

- la notte mod
- Only Girl rihanna
- The Time black

^ TOP ^

#### Clients (from clients.met): 3007

Index	Userhash	Sent byte	Received byte	Last seen
1	3B8CA2BDBF0EEB27E1EA4C4FC9EB6F87	1111500	0	Thu Dec 30 12:35:37 2010
2	E25ED763490E1A38769419910EF26F5E	11744032	0	Sat Dec 4 23:32:54 2010
3	13298404D90E88C4AF5447DD42EA6F1E	598944	0	Thu Nov 4 00:32:20 2010
4	B0DC8F05F90ED39761FEE1E7B3576FC2	0	4835686	Thu Dec 30 11:15:06 2010
5	2BA8BC67D70E72FA28D79AADE4326FF1	1967444	3049711	Wed Nov 10 22:01:53 2010
6	274B36C98C0E80A80675512DEAA46F4E	0	18200	Mon Nov 8 16:10:36 2010
7	F49C0B1D9C0EFC1FBF4B83EB501F6F36	2428056	0	Thu Dec 30 12:19:51 2010

...

...

...

## eMuleForensic – Esempio web

...

...

...

3006	IECD213D4D0EA3B2C37350C0B1656FA0	8362417	3133317	Thu Feb 3 23:57:45 2011
3007	77099476EE0EFA8ABC511E6643268F91	8520019	0	Fri Dec 10 17:10:10 2010

^ TOP ^

File (from known.met): 69

Index	Date	Hashfile <small>[ Click on a hash and you can see how the file is known in eDonkey network ]</small>	Size	Filename	Request Download Received	Request Download Accepted
0	Thu Dec 30 11:50:16 2010	<a href="#">A188AB011901C6817F41B5BBECD2694D</a>	7124375	James Blunt - Stay the Night.mp3		
1	Sat Jan 29 14:14:56 2011	<a href="#">25270BD4B33E9F420A8624B93594A16D</a>	5605250	Madonna - Like a prayer.mp3		
2	Thu Dec 30 11:23:10 2010	<a href="#">25E4C0719C91FBF09ACA64D80F03E04D</a>	8220094	-- Cant Be Tamed - Miley Cyrus 2.mp3		
3	Sat Jan 29 14:20:08 2011	<a href="#">4705B9F161DBCCFC0DA8DA7F11975175</a>	3293262	- Rihanna Drake - Whats My Name.mp3	2	2
4	Thu Feb 3 21:18:36 2011	<a href="#">D750A79C67B376F93B638D14CF16E0D4</a>	4952119	cold play - coldplay - the scientist.mp3	1	1

...

...

...

## eMuleForensic – Esempio web


Hash-id information report for **new search**

**25270BD4B33E9F420A8624B93594A16D**

presumed file name

**Madonna - Like A Prayer.mp3**

last update :  
02/22/11 11:41 am

 This file is very widespread, its download should be very fast

302 available sources indexed by 10 eDonkey servers.  
(302 full sources - 0 partial sources)

Type audio  
Format mp3  
Size 5.35Mb

File sources evolution

graph by updates

800000  
600000  
400000  
200000  
0

800  
600  
400  
200  
0

22/02/11

302

full sources

Servers statistics for the last update

servers	sources (full+part)	rates	bp	reported filename
Master Server 2	37 = 0	12.25%	100%	Madonna - Like A Pra ...
BINVERSE BIZ	44 = 0	14.57%	100%	Madonna - Like a pra ...
EMULE-SECURITY.NET	34 = 0	11.24%	100%	Madonna - Like A Pra ...
Emule Server No1	33 = 0	10.93%	100%	madonna - madonna - l...
TV Underground No1	50 = 0	16.56%	100%	Madonna - Like A Pra ...
Share Islands	43 = 0	14.24%	100%	Madonna - Madonna - L ...
I= Pom Fit =I	17 = 0	5.63%	100%	Madonna - Like A Pra ...
Master Server 1	35 = 0	12.58%	100%	Madonna - Like A Pra ...
VeryCD eDonkey Server	2 = 0	0.66%	100%	Madona - Madonna - L ...
Chong Qing eMule Fans	4 = 0	1.32%	100%	Madona - Madonna - L ...

total:302

Low ID Invalid ID  
High ID Peers ID

Results collected the 02/22/11 (11:41 am) from 10 online servers on wich 745,513 users are connected and 216,428,666 files are indexed .

Reported file names for the last update (5)

10.00%	50%	reported filename
10.00%	50%	madona - madonna - like a prayer.mp3
10.00%	50%	Madonna - Like a prayer.mp3
10.00%	50%	Madonna - Like A Prayer.mp3
40.00%	50%	Madonna - Like A Prayer.mp3
30.00%	50%	Madona - Madonna - Like a prayer.mp3

File names history (5)

40.00%	02/22/11	reported filename
10.00% <td>02/22/11</td> <td>Madonna - Like A Prayer.mp3</td>	02/22/11	Madonna - Like A Prayer.mp3
10.00% <td>02/22/11</td> <td>Madonna - Like a prayer.mp3</td>	02/22/11	Madonna - Like a prayer.mp3
10.00% <td>02/22/11</td> <td>madona - madonna - like a prayer.mp3</td>	02/22/11	madona - madonna - like a prayer.mp3
30.00% <td>02/22/11</td> <td>Madona - Madonna - Like a prayer.mp3</td>	02/22/11	Madona - Madonna - Like a prayer.mp3
10.00% <td>02/22/11</td> <td>Madonna - Like A Prayer.mp3</td>	02/22/11	Madonna - Like A Prayer.mp3

## eMuleForensic – esempio web

(output xml)

```

- <case>
  - <info>
    <timeStart>22/02/11-11:36:55</timeStart>
    <code>1</code>
    <description>Descrizione</description>
    <examinator>Michele</examinator>
  </info>
  - <search>
    <keyword>shakira loca</keyword>
    <keyword>shakira loca</keyword>
    <keyword>shakira - loca</keyword>
    ...
    ...
    ...

```

## eMuleForensic – Esempio

```

notroot@ubuntu:~/Desktop$ emuleforensic -i
esempi/3/ -o 3.xml -c 0001 -d Descrizione -e
Michele

notroot@ubuntu:~/Desktop$ cat esempi/3/AC_Search$
fisting
printmusic
printmusic.ita

notroot@ubuntu:~/Desktop$ hexdump 3/prefe
00000000 14
00000010 2 0000 0000 0000 0300 0000 ff00 ffff
00000020 ffff ffff ffff ffff ffff ffff 0aff 0000
00000030 0a00 0000 1700 0003 5300 0002 0000
0000003d

<?xml version="1.0"?>
<case>
  <info>
    <timeStart>07/05/10-04:46:30</timeStart>
    <code>001</code>
    <description>Descrizione</description>
    <examinator>Michele</examinator>
  </info>
  <search>
    <keyword>fisting</keyword>
    <keyword>printmusic</keyword>
    [...]
  </search>
  <userinfo>
    <code>001</code>
    <userhash>[redacted]</userhash>
    <ash>[redacted]</ash>
  </userinfo>

```

## eMuleForensic – Esempio

```
notroot@ubuntu:~/Desktop/esempi$ hexdump 3/client
00000000 9012 0038 0000 0000 0000 0000 4c00 4a30 0d30
00000010 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000020 0047 0000 0000 0000 0000 0000 4c00 4a30 0d30
00000030 0906 862a 8648 0df7 0101 0501 0300 0039
00000040 3630 3102 b000 5866 91ef c814 d080 96d3
00000050 bdac 2f18 d391 dc9f 6ad7 e48c 61a9 2894
00000060 c01c 6979 8c37 ea82 d485 05b8 4484 bb99
00000070 f554 60c6 020f 1101 0000 0000 7fa4 16c1
00000080 0ef9 9f2f f206 1059 98b7 976f 6a0f 0093
00000090 0000 0000 7e72 4789 0000 0000 0000 0000
```

```
<clients>
<client id="1">
  <code>001</code>
  [REDACTED]
  <nLastSeen>Mon Dec 10 23:14:17
    2007</nLastSeen>
</client>
[...]
```

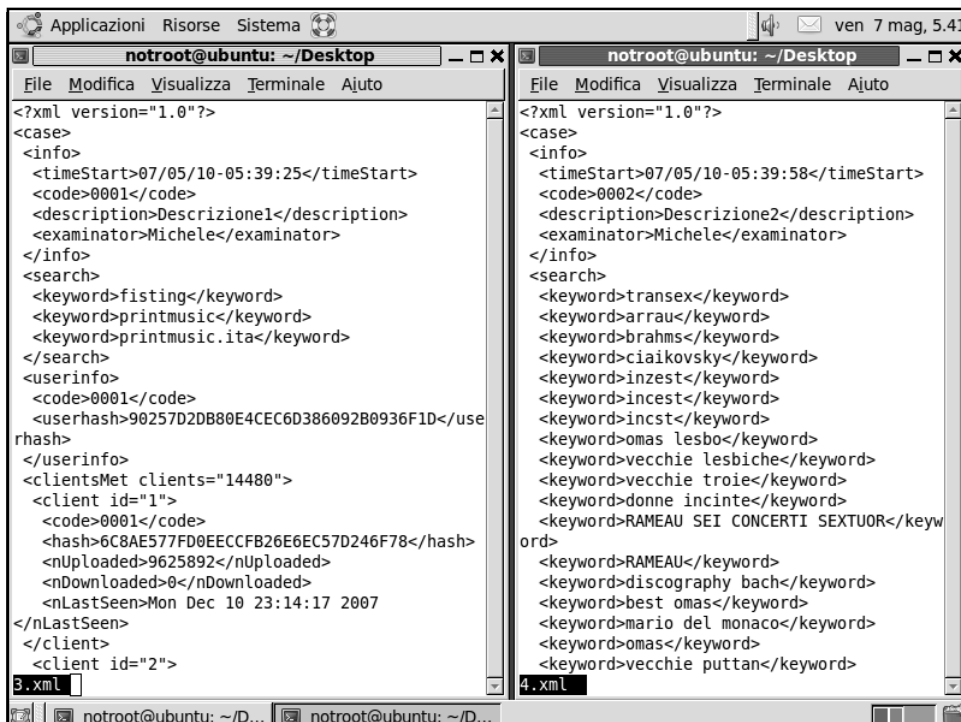
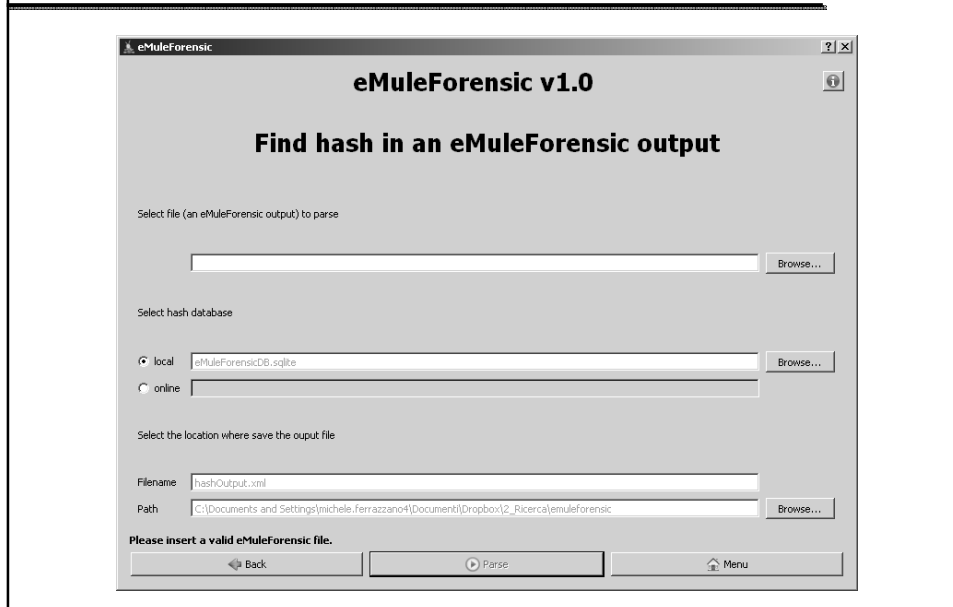
## eMuleForensic – Esempio

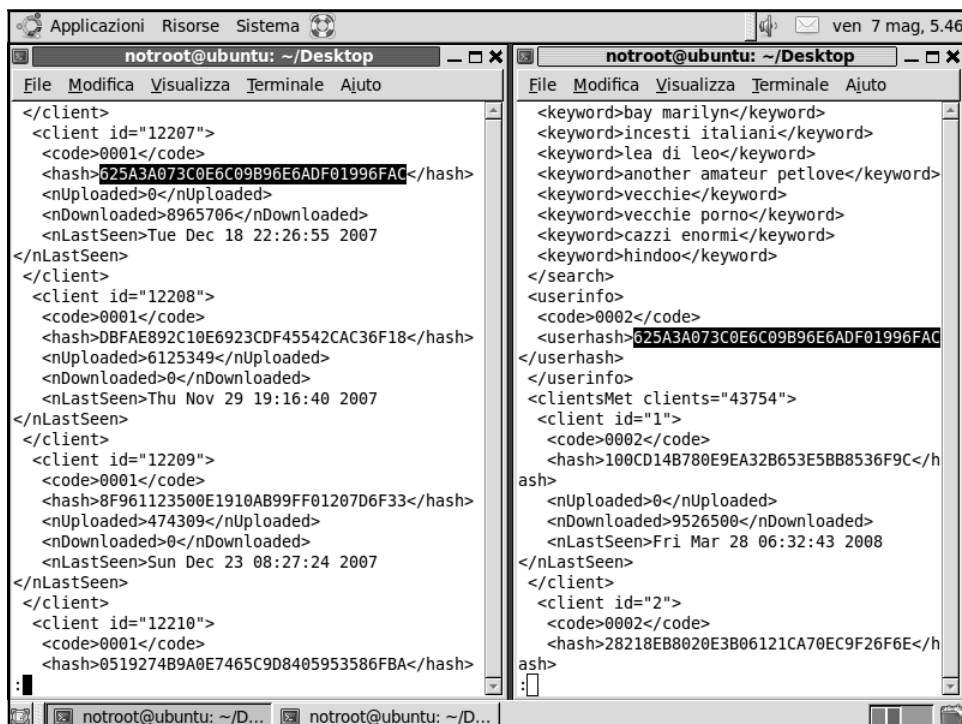
```
notroot@ubuntu:~/Desktop/esempi/3$ hexdump known.met
00000000 8a0e 0035 4600 5046 0047 0000 0000 0200
00000010 0000 0000 0000 0000 0000 0000 0000 0000
00000020 0001 0c01 6c00 3070 3136 3936 2e32 706a
00000030 0367 0001 5c02 0239 0300 0001 0519 0000
00000040 0200 0001 2027 3600 4555 4b36 3741 4c42
00000050 4f54 3737 4148 524e 514d 4b54 4233 5634
00000060 535a 3258 5834 0356 0001 7421 effd b847
00000070 9cf4 7145 38ca 0dbe efb2 be9b 2485 650d
00000080 0551 1bea 3000 3b79 664c cb49 5e53 9c22
00000090 37a7 7196 e46f 5d60 33b6 7194 157b 3b59
```

```
<knownMet files="13706">
  <file id="0">
    <code>001</code>
    <date>Fri Nov 30 17:20:06 2007</date>
    [REDACTED]
    <size>145756</size>
  </file>
  <file id="1">
    <code>001</code>
    <date>Thu Jan 4 12:36:08 2007</date>
    <hashfile>71CA38BE0DB2EF9BBE85240D655105EA</hashfile>
    <filename>NEW! pedo 9yo Tori 006 lsm kdquality
      childlover pthc kidzilla(2).mPG</filename>
    <size>262223208</size>
  </file>
  [...]
</knownMet>
</case>
```



## eMuleForensic (versione Java in sviluppo)





```

notroot@ubuntu: ~/Desktop
File Modifica Visualizza Terminale Ajuto
<client id="12207">
  <code>0001</code>
  <hash>625A3A073C0E6C09B96E6ADF01996FAC</hash>
  <nUploaded>0</nUploaded>
  <nDownloaded>8965706</nDownloaded>
  <nLastSeen>Tue Dec 18 22:26:55 2007
</nLastSeen>
</client>
<client id="12208">
  <code>0001</code>
  <hash>DBFAE892C10E6923CDF45542CAC36F18</hash>
  <nUploaded>6125349</nUploaded>
  <nDownloaded>0</nDownloaded>
  <nLastSeen>Thu Nov 29 19:16:40 2007
</nLastSeen>
</client>
<client id="12209">
  <code>0001</code>
  <hash>8F961123500E1910AB99FF01207D6F33</hash>
  <nUploaded>474309</nUploaded>
  <nDownloaded>0</nDownloaded>
  <nLastSeen>Sun Dec 23 08:27:24 2007
</nLastSeen>
</client>
<client id="12210">
  <code>0001</code>
  <hash>0519274B9A0E7465C9D8405953586FBA</hash>
  <nUploaded>9692702</nUploaded>
  :

notroot@ubuntu: ~/D... notroot@ubuntu: ~/D...

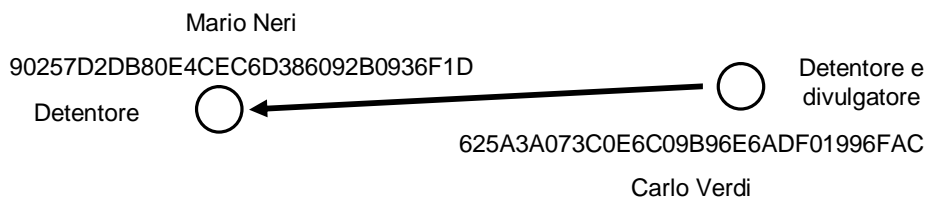
notroot@ubuntu: ~/Desktop
File Modifica Visualizza Terminale Ajuto
<client id="39437">
  <code>0002</code>
  <hash>90257D2DB80E4CEC6D386092B0936F1D</h
ash>
  <nUploaded>8966051</nUploaded>
  <nDownloaded>0</nDownloaded>
  <nLastSeen>Tue Dec 18 23:16:26 2007
</nLastSeen>
</client>
<client id="39438">
  <code>0002</code>
  <hash>10C65B5EFE0E73813B4DFE1D544A6F98</h
ash>
  <nUploaded>0</nUploaded>
  <nDownloaded>20480</nDownloaded>
  <nLastSeen>Tue Nov 27 11:15:14 2007
</nLastSeen>
</client>
<client id="39439">
  <code>0002</code>
  <hash>9DDFFE06A00EC2EE776FD34DA91B6F42</h
ash>
  <nUploaded>3293373</nUploaded>
  <nDownloaded>0</nDownloaded>
  <nLastSeen>Tue Mar 25 18:00:00 2008
</nLastSeen>
</client>
<client id="39440">
  :

```

## eMuleForensic

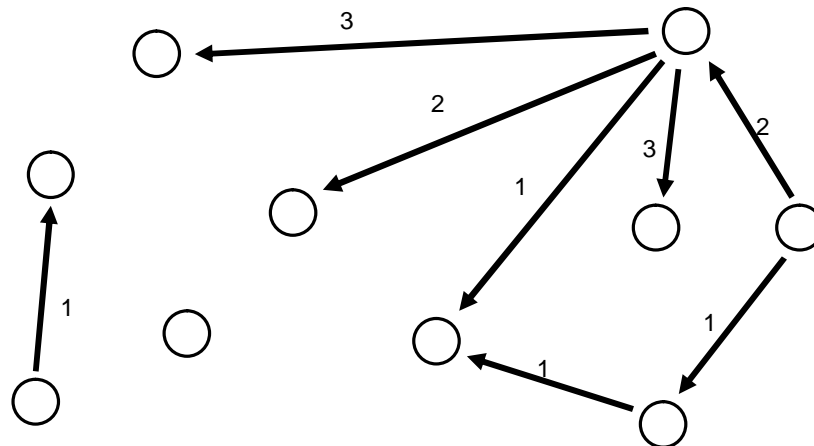
### Esempio di divulgazione

- Incrociando gli output è possibile dedurre possibili connessioni tra due utenti.
  - Non ci sono dati chiari ed espliciti nei log
  - La funzione di incrocio dei dati non è attualmente implementata ma può essere realizzata in maniera molto semplice (es: Access)

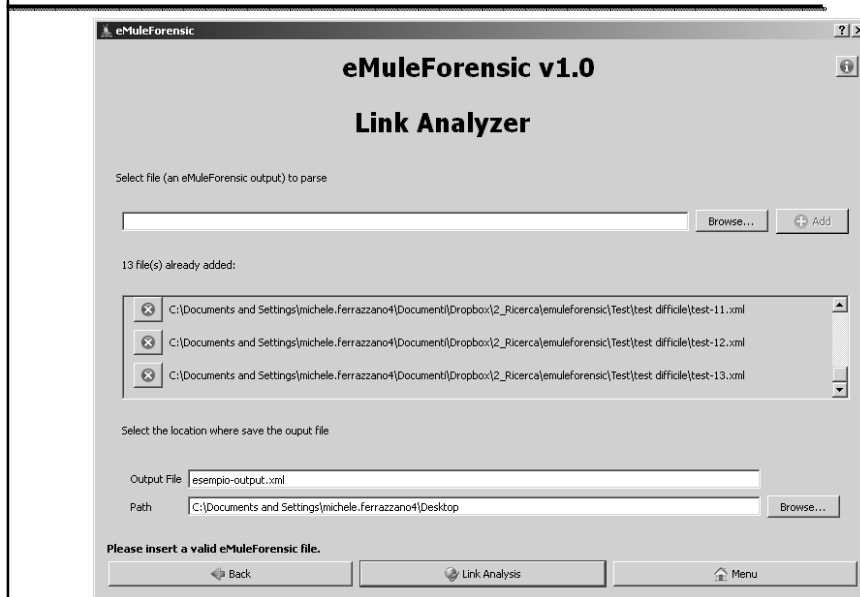


## eMuleForensic

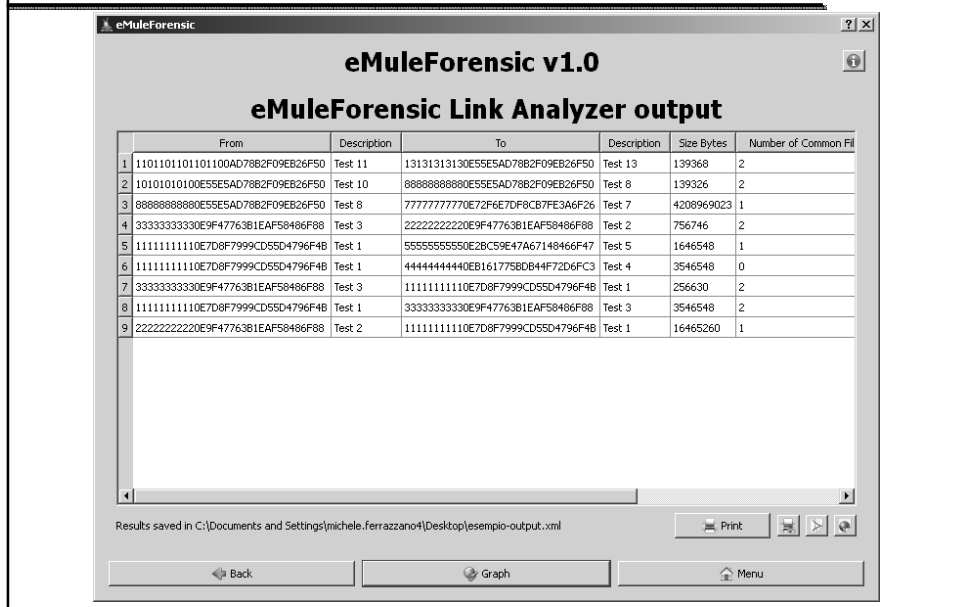
Rappresentazione grafica delle divulgazioni



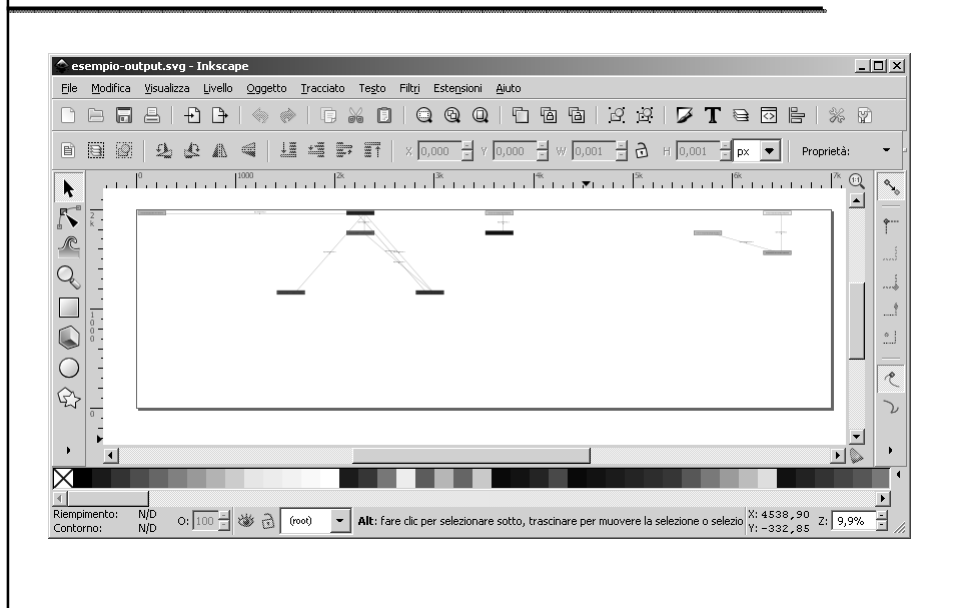
## eMuleForensic (versione Java in sviluppo)



## eMuleForensic (versione Java in sviluppo)



## eMuleForensic (versione Java in sviluppo)



[illegible]

- Aspetti rilevanti
  - Detenzione
    - Presenza di file aventi hash identificati come positivi
  - Consapevolezza
    - Parole chiave di ricerca e nomi dei file
  - Ingente quantità
  - Divulgazione di materiale, notizie e informazioni
- Utilizzo
  - In fase di perquisizione, per ottimizzare i sequestri
    - Rapida identificazione dei computer utilizzati per il file sharing
    - Rapida verifica per l'ingente quantità
  - In fase di analisi, per ottimizzare i tempi e fornire risultati più accurati

## Conclusioni

---

- Limiti
  - Log di eMule poveri, non è possibile trovare in maniera chiara alcune informazioni
  - Se la cartella config è cancellata, vengono rigenerati tutti i file
    - Se sono stati cancellati anche dei file in condivisione si perde l'informazione
    - Se un file viene modificato, avrà un hash diverso
    - Si perde l'informazione relativa agli utenti remoti
  - Le ricerche per parole chiave possono essere condotte utilizzando motori di ricerca su siti web
    - Nessuna traccia nel log di eMule