Computer Forensics - Corso di Laurea in Informatica
Università di Catania
10 marzo 2011

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

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

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

Art. 600-ter : Pornografia minorile

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 con la reclusione da sei a dodici anni e con la multa da € 25.822 a € 258.228.
2. Alla stessa pena soggiace chi fa commercio del materiale pornografico di cui al primo comma.
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, é punito con la reclusione da uno a cinque anni e con la multa da lire cinque milioni a lire cento milioni.
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 con la reclusione fino a tre anni e con la multa da € 1.549 a € 5.164.(2)
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

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 con la reclusione fino a tre anni e con la multa non inferiore a €1.549.
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

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

1. Nei casi previsti dagli articoli 600-bis, primo comma, 600-ter, primo comma, e 600-quinquies la pena è aumentata da un terzo alla metà se il fatto è commesso in danno di minore degli anni quattordici. Nei casi previsti dagli articoli 600-bis, primo comma, e 600-ter la pena è aumentata dalla metà ai due terzi se il fatto è commesso da un ascendente, dal genitore adottivo, o dal loro coniuge o convivente, dal coniuge o da affini entro il secondo grado, da parenti fino al quarto grado collaterale, dal tutore o da persona a cui il minore e' stato affidato per ragioni di cura, educazione, istruzione, vigilanza, custodia, lavoro, ovvero da pubblici ufficiali o incaricati di pubblico servizio nell'esercizio delle loro funzioni ovvero se è commesso in danno di minore in stato di infermità o minorazione psichica, naturale o provocata. Nei casi previsti dagli articoli 600-bis, primo comma, e 600-ter la pena è aumentata se il fatto è commesso con violenza o minaccia. Nei casi previsti dagli articoli 600-bis e 600-ter la pena è ridotta da un terzo alla metà per chi si adopera concretamente in modo che il minore degli anni diciotto riacquisti la propria autonomia e libertà".

Aspetti chiave - Detenzione

- Consapevolezza
  - 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 con la reclusione da sei a dodici anni e con la multa da € 25.822 a € 258.228"*

Aspetti chiave - Divulgazione

- 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, é punito con la reclusione da uno a cinque anni e con la multa da lire cinque milioni a lire cento milioni"*
    - *"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 con la reclusione fino a tre anni e con la multa da € 1.549 a € 5.164"*
- 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"*
- Commercio
  - Art. 600-ter c.p., comma 2
    - *"Alla stessa pena soggiace chi fa commercio del materiale pornografico di cui al primo comma"*

Le 5 fasi

- Identificazione
- Acquisizione
- **Analisi**
- Valutazione
- Presentazione

Obiettivi dell'analisi forense

- Individuare e quantificare file a contenuto pedopornografico
  - Se possibile, classificare il materiale per età dei soggetti raffigurati
- Individuare le fonti
- Individuare elementi che consentano di stabilire la consapevolezza
- Individuare elementi che consentano di determinare se c'è stata divulgazione e in che quantità
  - Individuare elementi che permettano di determinare 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
- 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
- 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
- Chi porta avanti l'analisi forense non giudica! Si limita a mettere in evidenza elementi, il giudice esprime il giudizio.
- Quali elementi utili per determinare la (in)consapevolezza?
  - Parole chiave di ricerca
  - Organizzazione dei file nel file system
  - File in chiaro o cancellati
  - Metadati
  - Nomi dei file (file *fake*)

Obiettivi dell'analisi forense

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

- 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, dove c'è un server centralizzato
- 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 extraterresti

eMule

Software di file sharing su rete P2P

- Open source
  - Numerose *mod*
    - Versioni alternative con funzionalità aggiuntive
      - eMule Xtream, eMule MorphXT, eMule Adunanza…
  - Ultima versione 0.50a (eseguibile e codice sorgente)

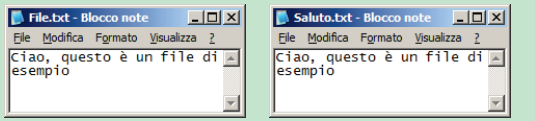
    http://sourceforge.net/projects/emule/

    È il software più scaricato da sourceforge (circa 500.000.000 di download)
  - **Fini forensi**
    - **Dal sorgente è possibile capire e ricostruire come vengono gestiti i file ed i trasferimenti**

eMule - I file

- Ogni file è identificato nella rete con un **File ID**
  - Costituito da 128 bit
  - Calcolato con funzione hash MD4
- **Il filename non è identificativo, né univoco**
  - File con contenuti identici hanno stesso hash ma possono avere nomi diversi
  - File con contenuti diversi hanno hash diversi ma possono avere stesso nome
  - **Le ricerche di file si basano sul filename**
    - Possibilità 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 o di un video pedopornografico

eMule – i file



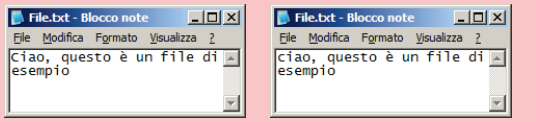
File.txt *Saluto.txt*

Hanno lo stesso contenuto

Hanno nomi diversi, sono salvati/creati in giorni diversi

⇨ Hanno lo stesso hash MD4

⇨ In eMule sono lo stesso file



File.txt *File.txt*

Hanno contenuti diversi *(Ciao vs. ciao)*

Hanno nomi uguali, sono salvati/creati lo stesso giorno

⇨ Hanno hash MD4 diversi

⇨ In eMule sono file diversi

Perché porre attenzione al fake

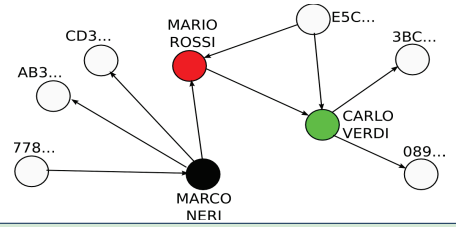
- Ricerca di file con keyword non pedopornografia, file scaricato con contenuto pedopornografico
  - Filename
    - Negativo
  - Hash/contenuto pedopornografico
    - **Positivo**
  - Intenzione di ricercare materiale pedornografico
    - No
- Ricerca di file con keyword della pedopornografia, file scaricato con contenuto non pedopornografico
  - Filename
    - **Positivo**
  - Hash/contenuto pedopornografico
    - Negativo
  - Intenzione di ricercare materiale pedornografico
    - **Si**

eMule – Gli utenti

- Ogni utente di eMule è identificato nella rete da uno **User ID**
  - Costituito da 128 bit
  - Generato casualmente al primo avvio di eMule
  - 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
  - *Link analysis*
    - Identificare i collegamenti tra i nodi (indagati) per verificare divulgazione

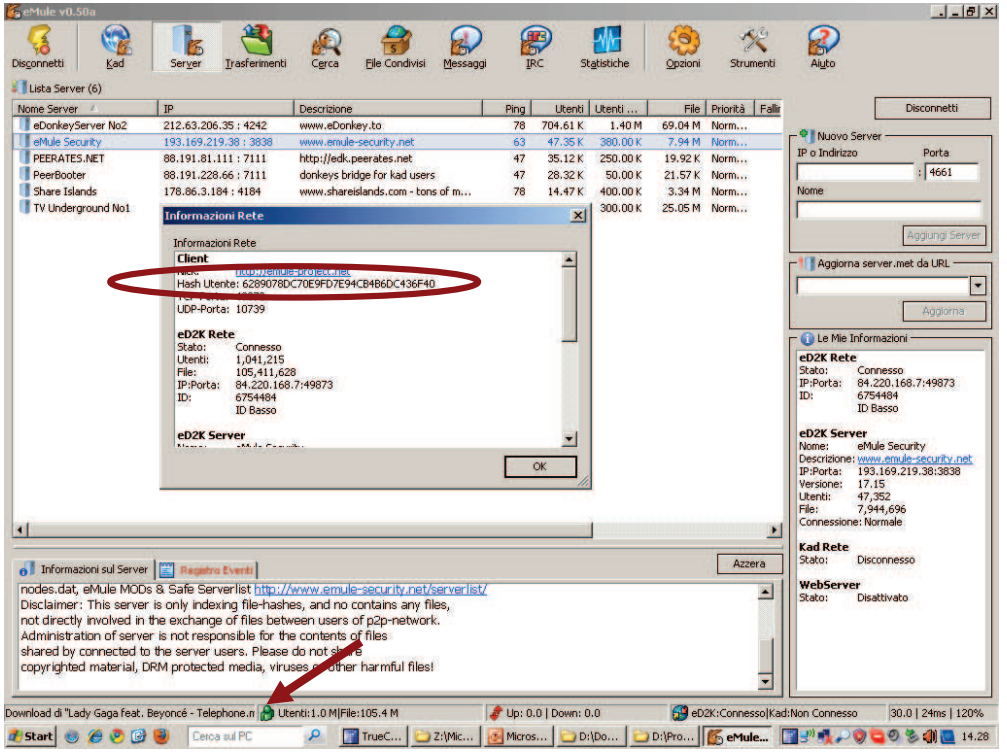


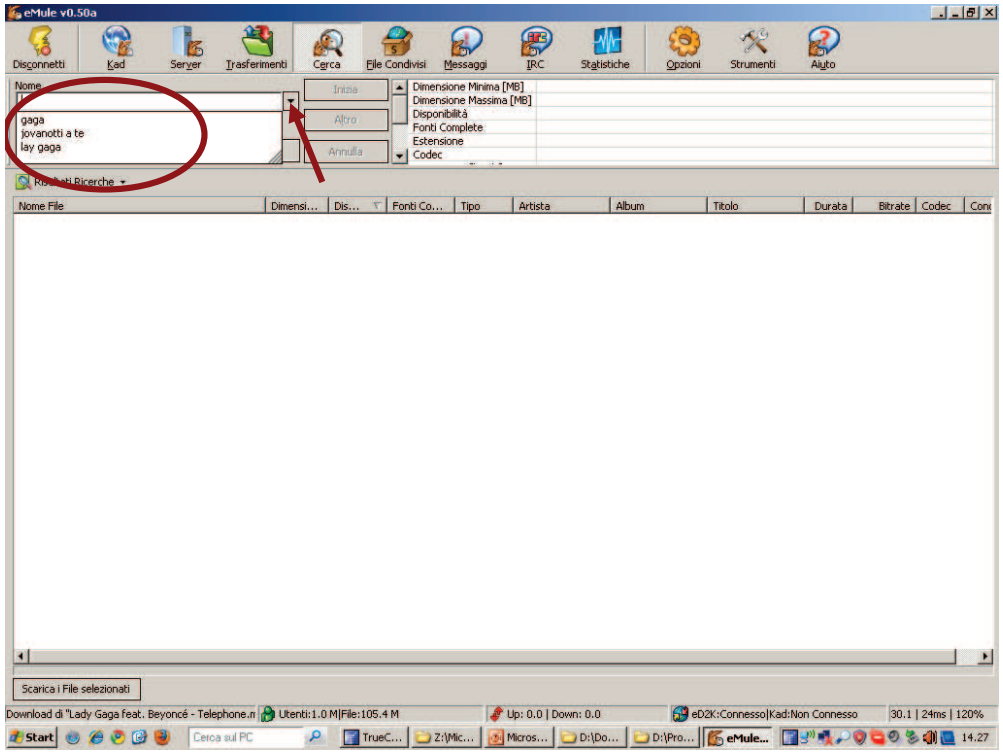
Ricerca di materiale pedopornografico nel disco

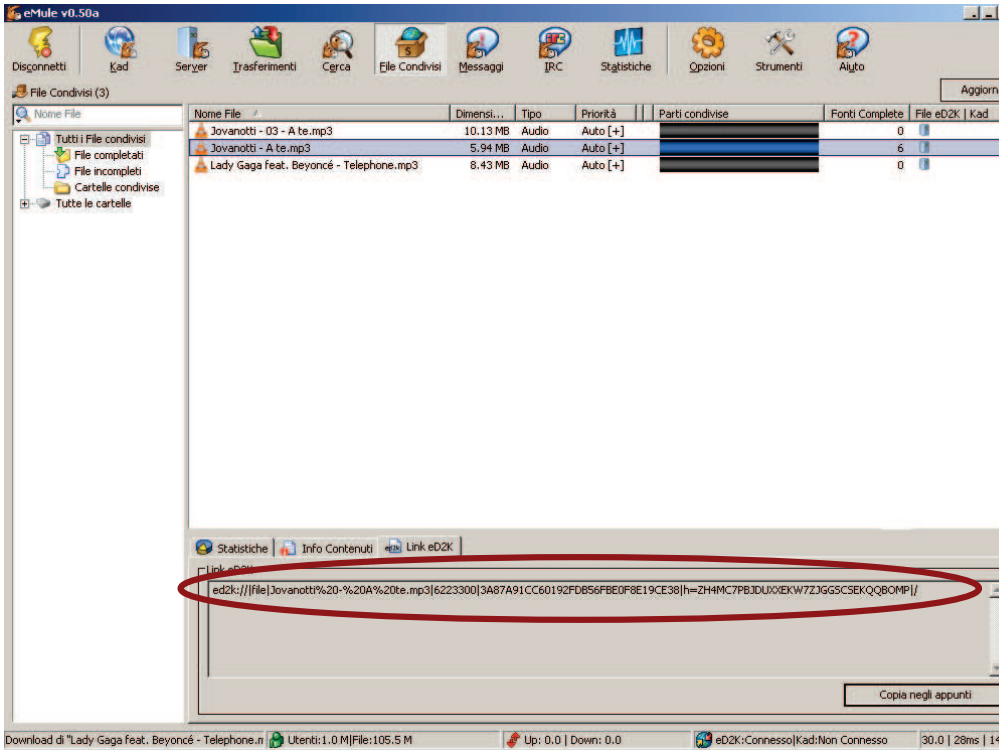
- Indipendente dalla fonte
  - File sharing, siti web…
- Identificazione dei file “positivi”
  - Visualizzazione del contenuto
    - Visualizzazione delle varie immagini e dei vari video
    - *Con alcuni software di riconoscimento automatico*
  - Parole chiave nel filename
    - Alcuni esempi: *lolita*, *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

senza eMuleForensic







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)
  - Output in formato XML
    - Linguaggio di markup, definisce documenti strutturati
    - Possibilità di incrociare dati di utenti diversi

Analisi forense con eMuleforensic
Detenzione e consapevolezza

- File di configurazione di eMule
  - *AC_SearchString.dat*
    - Elenco di keyword di ricerca
  - *Known.met*
    - Filename
      - È possibile associare i file scaricati con le keyword utilizzate in fase di ricerca
    - Hash
      - 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/3$ hexdump known.met
0000000 8a0e 0035 4600 5046 8547 d21b 71cb b480
0000010 5a79 c58c 6f7e ae83 0068 0500 0000 0200
0000020 0001 0c01 6c00 3070 3136 3936 2e32 706a
0000030 0367 0001 5c02 0239 0300 0001 0519 0000
0000040 0200 0001 2027 3600 4555 4b36 3741 4c42
0000050 4f54 3737 4148 524e 514d 4b54 4233 5634
0000060 535a 3258 5834 0356 0001 7421 effd b847
0000070 9cf4 7145 38ca 0dbe efb2 be9b 2485 650d
0000080 0551 1bea 3000 3b79 664c cb49 5e53 9c22
0000090 37a7 7196 e46f 5d60 33b6 7194 157b 3b59
```

File "known.met" visualizzato con un editor esadecimale

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

Analisi forense con eMuleforensic
Divulgazione

- File di configurazione di eMule
  - *Preferences.dat*
    - User ID dell'utente indagato
      - nell'esempio 90257D2DB80E4CEC6D386092B0936F1D
  - *Clients.met*
    - User ID utenti remoti
      - Possibilità di determinare il volume di dati scambiati in upload e in download
  - Possibilità di incrociare questi due file e il file *known.met* per definire le relazioni di scambio

```
notroot@ubuntu:~/Desktop/esempi$ hexdump 3/preferences.dat
0000000 9014 7d25 b82d 4c0e 6dec 6038 b092 6f93
0000010 2c1d 0000 0000 0000 0300 0000 ff00 ffff
0000020 ffff ffff ffff ffff ffff ffff 0aff 0000
0000030 0a00 0000 1700 0003 5300 0002 0000
000003d
```

File "preferences.dat" visualizzato con un editor esadecimale

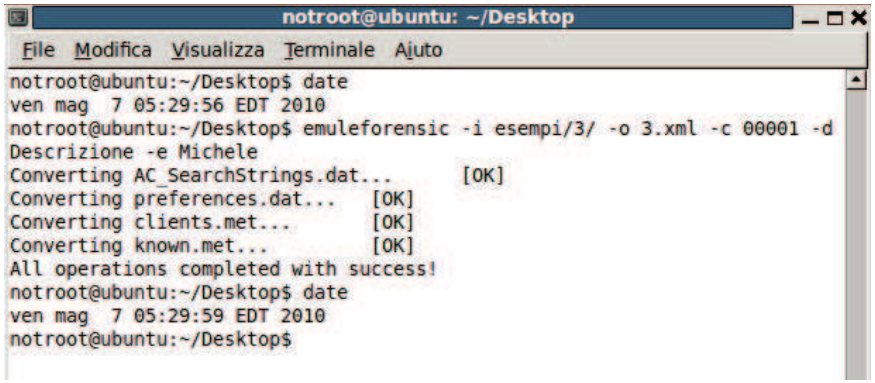
```
notroot@ubuntu:~/Desktop/esempi$ hexdump 3/clients.met
0000000 9012 0038 6c00 e58a fd77 ec0e b2cf 6e6e
0000010 7dc5 6f24 2478 92e1 0000 0000 4900 5dc8
0000020 0047 0000 0000 0000 0000 4c00 4a30 0d30
0000030 0906 862a 8648 0df7 0101 0501 0300 0039
0000040 3630 3102 b000 5866 91ef c814 d080 96d3
0000050 bdac 2f18 d391 dc9f 6ad7 e48c 61a9 2894
0000060 c01c 6979 8c37 ea82 d485 05b8 4484 bb99
0000070 f554 60c6 020f 1101 0000 0000 7fa4 16c1
0000080 0ef9 9f2f f206 1059 98b7 976f 6a0f 0093
0000090 0000 0000 7e72 4789 0000 0000 0000 0000
```

File "clients.met" visualizzato con un editor esadecimale

I file scambiati tra X e Y appartengono all'insieme

Hash(Known.met[X]) ∩ Hash(Known.met[Y])

eMuleForensic - Esempio



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$
ffisting
printmusic
printmusic.ita
```

```
notroot@ubuntu:~/Desktop/esempi$ hexdump 3/prefe
0000000 9014 7d25 b82d 4c0e 6dec 6038 b092 6f93
0000010 2c1d 0000 0000 0000 0300 0000 ff00 ffff
0000020 ffff ffff ffff ffff ffff ffff 0aff 0000
0000030 0a00 0000 1700 0003 5300 0002 0000
000003d
```

```
<?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>90257D2DB80E4CEC6D386092B0936F1D</userhash>
 </userinfo>
```

eMuleForensic – Esempio

```
notroot@ubuntu:~/Desktop/esempi$ hexdump 3/clien
0000000 9012 0038 6c00 e58a fd77 ec0e b2cf 6e6e
0000010 7dc5 6f24 2478 92e1 0000 0000 4900 5dc8
0000020 0047 0000 0000 0000 0000 4c00 4a30 0d30
0000030 0906 862a 8648 0df7 0101 0501 0300 0039
0000040 3630 3102 b000 5866 91ef c814 d080 96d3
0000050 bdac 2f18 d391 dc9f 6ad7 e48c 61a9 2894
0000060 c01c 6979 8c37 ea82 d485 05b8 4484 bb99
0000070 f554 60c6 020f 1101 0000 0000 7fa4 16c1
0000080 0ef9 9f2f f206 1059 98b7 976f 6a0f 0093
0000090 0000 0000 7e72 4789 0000 0000 0000 0000
```

```
...
<clients>
 <client id="1">
  <code>001</code>
  <hash>6C8AE577FD0EECCFB26E6EC57D246F78</hash>
  <nUploaded>9625892</nUploaded>
  <nDownloaded>0</nDownloaded>
  <nLastSeen>Mon Dec 10 23:14:17 2007</nLastSeen>
 </client>
 [...]
</clients>
...
```

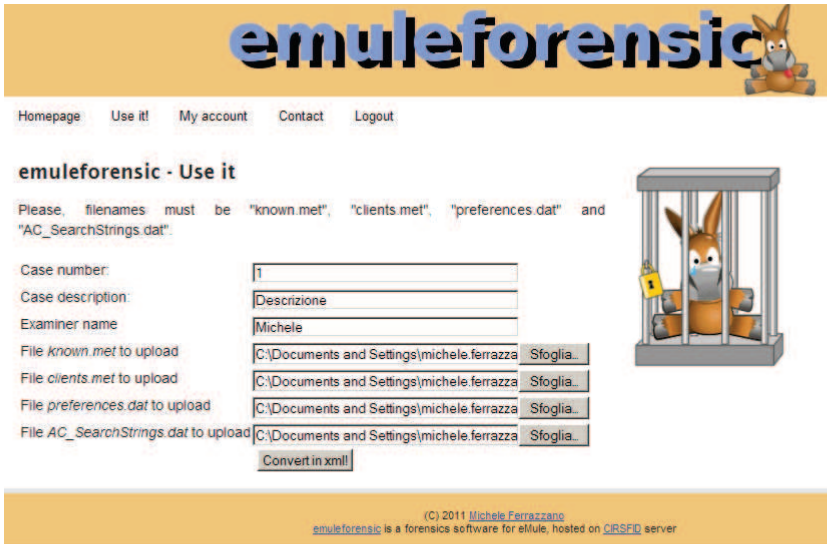
eMuleForensic – Esempio

```
notroot@ubuntu:~/Desktop/esempi/3$ hexdump known.met
0000000 8a0e 0035 4600 5046 8547 d21b 71cb b480
0000010 5a79 c58c 6f7e ae83 0068 0500 0000 0200
0000020 0001 0c01 6c00 3070 3136 3936 2e32 706a
0000030 0367 0001 5c02 0239 0300 0001 0519 0000
0000040 0200 0001 2027 3600 4555 4b36 3741 4c42
0000050 4f54 3737 4148 524e 514d 4b54 4233 5634
0000060 535a 3258 5834 0356 0001 7421 effd b847
0000070 9cf4 7145 38ca 0dbe efb2 be9b 2485 650d
0000080 0551 1bea 3000 3b79 664c cb49 5e53 9c22
0000090 37a7 7196 e46f 5d60 33b6 7194 157b 3b59
```

```
L^@lp061692.jpg^C^A^@^B\9^B^@^C^A^@^Y^E^@^@^
ZSX24XV^C^A^@!t<FD><EF>G<B8><F4><9C>Eq<CA>8<
G0y;LfI<CB>S^"<9C><A7>7<96>qq<E4>]<B6>3<94>
Oo<CD><E1><C4>{^V5<AF><D9>^E ~<99><E6><DB>r<
Z^KD^NG<A3>/;
<AE><86><8C>^T^C<8B><C2>^@^^tqK<CE>aB5<AB><C
<EE>D/C<AC><87><C5><F6><DE><EA>z<EB><C9><D2>
<CD>^Z<D2>ESCD<C9>)<B6>'<E3><B8>^D^O<EB><BC>
<F7>Jz<FA><8D>Dg<DC><C6>G<85><8E>S+.<BE><FF>
<83><A8>m^K<F7><AF><C3>{^Q^Z<9B><95>xD'^A<A
[<93><E2><FC><9B>k,^Hj7#W<AD><B5>^E?<EC><FD>
```

```
...
<knownMet files="13706">
 <file id="0">
  <code>001</code>
  <date>Fri Nov 30 17:20:06 2007</date>
  <hashfile>851BD2CB7180B4795A8CC57E6F83AE68</hashfile>
  <filename>lp061692.jpg</filename>
  <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 – Esempio web



http://emuleforensic.cirsfid.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	274B36C98C0E60A80675512DEAA46F4E	0	18200	Mon Nov 8 16:10:36 2010
7	F49C0B1D9C0EFC1FBF4B83EB501F6F36	2428056	0	Thu Dec 30 12:19:51 2010

...

...

...

eMuleForensic – Esempio web

...

...

...

3006	ECD213D44D0EA3B2C37350C0B1656FA0	8362417	3133317	Thu Feb 3 23:57:45 2011
3007	77099476EE0EFA6ABC511E6543266F91	8520019	0	Fri Dec 10 17:10:10 2010

^ TOP ^

File *(from known.met)*: 69

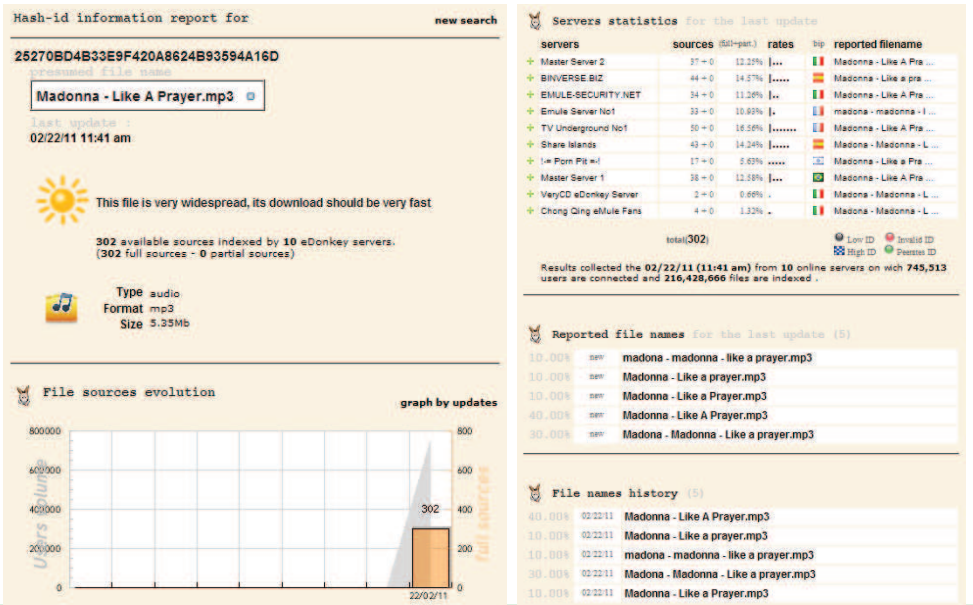
Index	Date	Hashfile *[Click on a hash and you can see how the file is known in eDonkey network]*	Size	Filename	Request Download Received	Request Download Accepted
0	Thu Dec 30 11:50:16 2010	A188ABD11901C6817F41B5BBECD2694D	7124375	James Blunt - Stay the Night.mp3		
1	Sat Jan 29 14:14:56 2011	25270BD4B33E9F420A8624B93594A16D	5605250	Madonna - Like a prayer.mp3		
2	Thu Dec 30 11:23:10 2010	75E4C0719C91FBF09ACA64D80F03E04D	8220094	- - Cant Be Tamed - Miley Cyrus 2.mp3		
3	Sat Jan 29 14:20:08 2011	4705B9F161DBCCFC0DA8DA7F11975175	3293262	- Rihanna Drake - Whats My Name.mp3	2	2
4	Thu Feb 3 21:18:35 2011	D750A79C67B376F93B638D14CF16E0D4	4952119	cold play - coldplay - the scientist.mp3	1	1

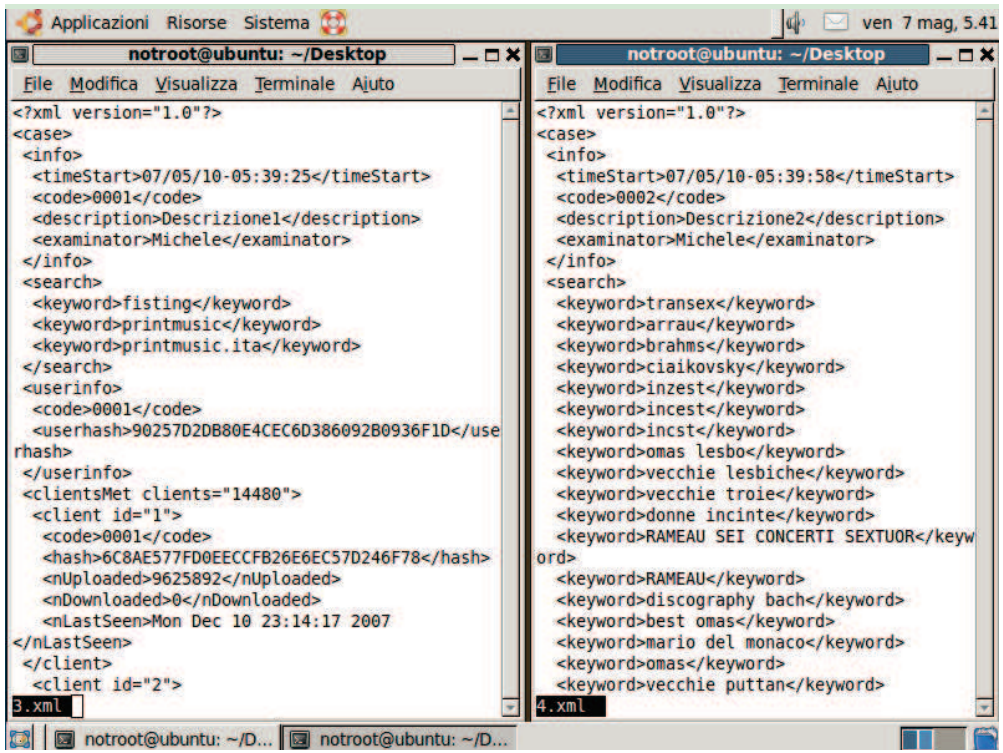
...

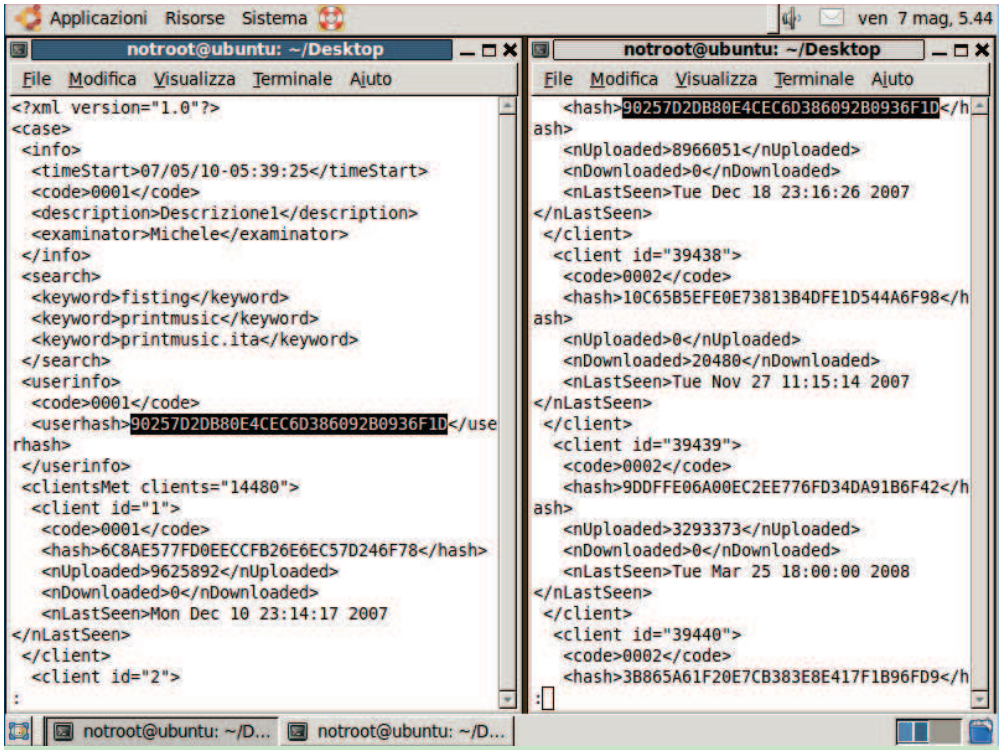
...

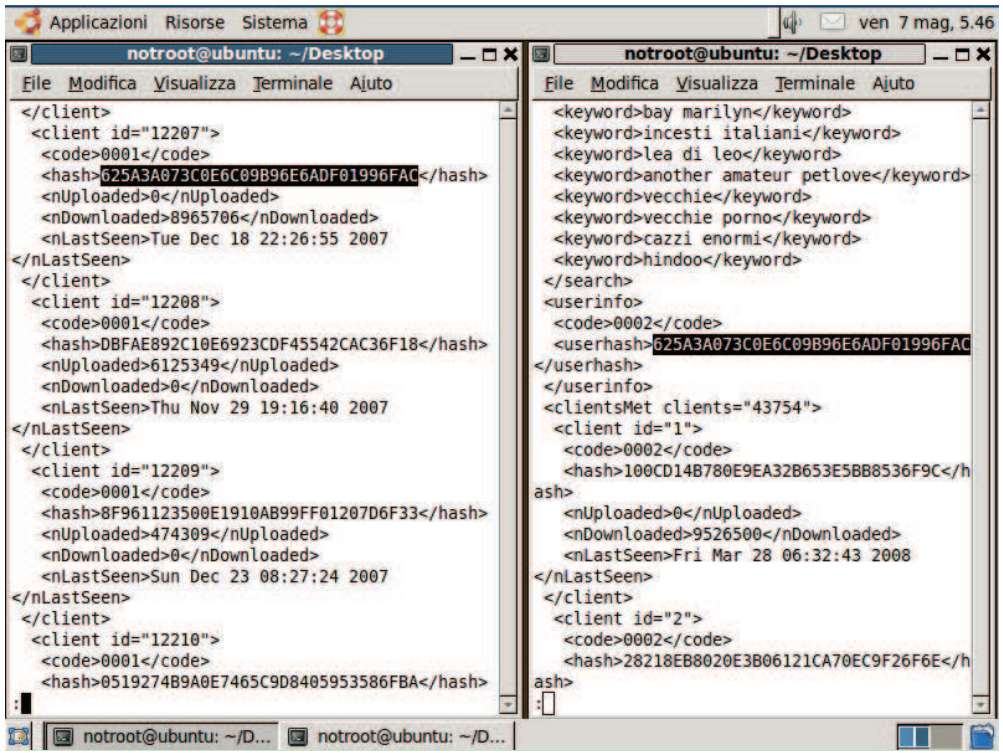
...

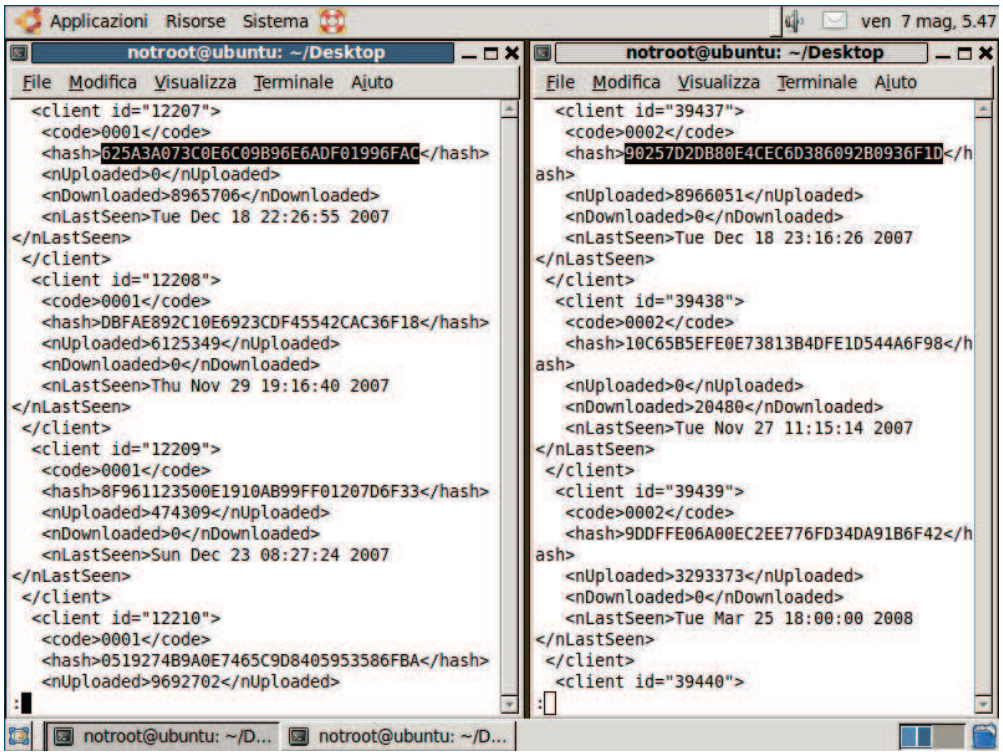
eMuleForensic – Esempio web




Applicazioni Risorse Sistema
ven 7 mag, 5.41
notroot@ubuntu: ~/Desktop
File Modifica Visualizza Terminale Aiuto
<?xml version="1.0"?>
<case>
<info>
<timeStart>07/05/10-05:39:25</timeStart>
<code>0001</code>
<description>Descrizione1</description>
<examinator>Michele</examinator>
</info>
<search>
<keyword>fisting</keyword>
<keyword>printmusic</keyword>
<keyword>printmusic.ita</keyword>
</search>
<userinfo>
<code>0001</code>
<userhash>90257D2DB80E4CEC6D386092B0936F1D</userhash>
</userinfo>
<clientsMet clients="14480">
<client id="1">
<code>0001</code>
<hash>6C8AE577FD0EECCFB26E6EC57D246F78</hash>
<nUploaded>9625892</nUploaded>
<nDownloaded>0</nDownloaded>
<nLastSeen>Mon Dec 10 23:14:17 2007
</nLastSeen>
</client>
<client id="2">
3.xml
notroot@ubuntu: ~/Desktop
File Modifica Visualizza Terminale Aiuto
<?xml version="1.0"?>
<case>
<info>
<timeStart>07/05/10-05:39:58</timeStart>
<code>0002</code>
<description>Descrizione2</description>
<examinator>Michele</examinator>
</info>
<search>
<keyword>transex</keyword>
<keyword>arrau</keyword>
<keyword>brahms</keyword>
<keyword>ciaikovsky</keyword>
<keyword>inzest</keyword>
<keyword>incest</keyword>
<keyword>incst</keyword>
<keyword>omas lesbo</keyword>
<keyword>vecchie lesbiche</keyword>
<keyword>vecchie troie</keyword>
<keyword>donne incinte</keyword>
<keyword>RAMEAU SEI CONCERTI SEXTUOR</keyword>
<keyword>RAMEAU</keyword>
<keyword>discography bach</keyword>
<keyword>best omas</keyword>
<keyword>mario del monaco</keyword>
<keyword>omas</keyword>
<keyword>vecchie puttan</keyword>
4.xml
notroot@ubuntu: ~/D...
notroot@ubuntu: ~/D...

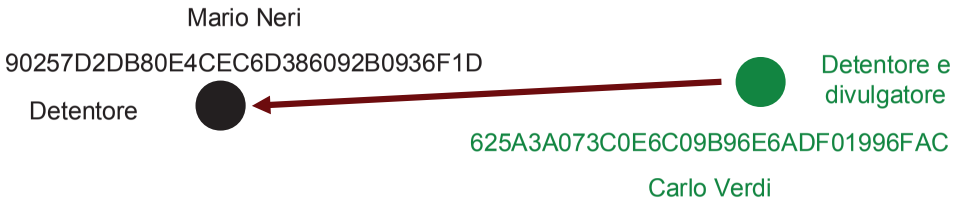

Applicazioni Risorse Sistema
ven 7 mag, 5.44
notroot@ubuntu: ~/Desktop
File Modifica Visualizza Terminale Aiuto
<?xml version="1.0"?>
<case>
<info>
<timeStart>07/05/10-05:39:25</timeStart>
<code>0001</code>
<description>Descrizione1</description>
<examinator>Michele</examinator>
</info>
<search>
<keyword>fisting</keyword>
<keyword>printmusic</keyword>
<keyword>printmusic.ita</keyword>
</search>
<userinfo>
<code>0001</code>
<userhash>90257D2DB80E4CEC6D386092B0936F1D</userhash>
</userinfo>
<clientsMet clients="14480">
<client id="1">
<code>0001</code>
<hash>6C8AE577FD0EECCFB26E6EC57D246F78</hash>
<nUploaded>9625892</nUploaded>
<nDownloaded>0</nDownloaded>
<nLastSeen>Mon Dec 10 23:14:17 2007
</nLastSeen>
</client>
<client id="2">
notroot@ubuntu: ~/Desktop
File Modifica Visualizza Terminale Aiuto
<hash>90257D2DB80E4CEC6D386092B0936F1D</hash>
<nUploaded>8966051</nUploaded>
<nDownloaded>0</nDownloaded>
<nLastSeen>Tue Dec 18 23:16:26 2007
</nLastSeen>
</client>
<client id="39438">
<code>0002</code>
<hash>10C65B5EFE0E73813B4DFE1D544A6F98</hash>
<nUploaded>0</nUploaded>
<nDownloaded>20480</nDownloaded>
<nLastSeen>Tue Nov 27 11:15:14 2007
</nLastSeen>
</client>
<client id="39439">
<code>0002</code>
<hash>9DDFFE06A00EC2EE776FD34DA91B6F42</hash>
<nUploaded>3293373</nUploaded>
<nDownloaded>0</nDownloaded>
<nLastSeen>Tue Mar 25 18:00:00 2008
</nLastSeen>
</client>
<client id="39440">
<code>0002</code>
<hash>3B865A61F20E7CB383E8E417F1B96FD9</hash>
notroot@ubuntu: ~/D...
notroot@ubuntu: ~/D...


Applicazioni Risorse Sistema
ven 7 mag, 5.46
notroot@ubuntu: ~/Desktop
File Modifica Visualizza Terminale Aiuto
</client>
<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>
notroot@ubuntu: ~/Desktop
File Modifica Visualizza Terminale Aiuto
<keyword>bay marilyn</keyword>
<keyword>incesti italiani</keyword>
<keyword>lea di leo</keyword>
<keyword>another amateur petlove</keyword>
<keyword>vecchie</keyword>
<keyword>vecchie porno</keyword>
<keyword>cazzi enormi</keyword>
<keyword>hindoo</keyword>
</search>
<userinfo>
<code>0002</code>
<userhash>625A3A073C0E6C09B96E6ADF01996FAC
</userhash>
</userinfo>
<clientsMet clients="43754">
<client id="1">
<code>0002</code>
<hash>100CD14B780E9EA32B653E5BB8536F9C</hash>
<nUploaded>0</nUploaded>
<nDownloaded>9526500</nDownloaded>
<nLastSeen>Fri Mar 28 06:32:43 2008
</nLastSeen>
</client>
<client id="2">
<code>0002</code>
<hash>28218EB8020E3B06121CA70EC9F26F6E</hash>
notroot@ubuntu: ~/D...
notroot@ubuntu: ~/D...

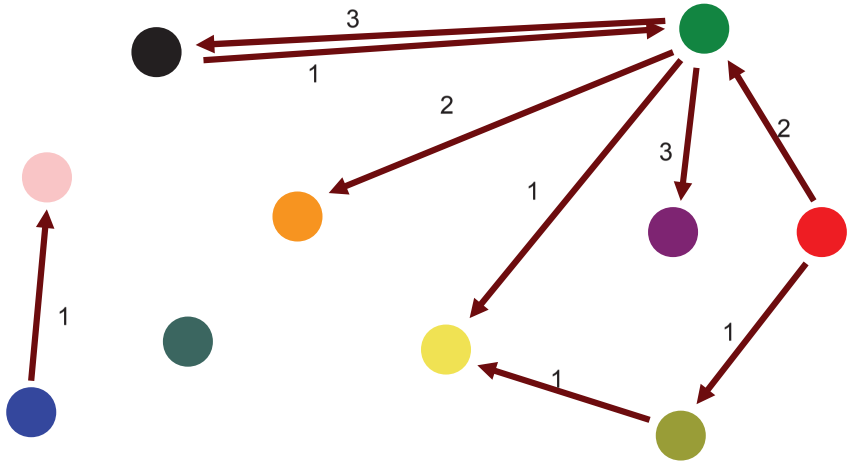

Applicazioni Risorse Sistema
ven 7 mag, 5.47
notroot@ubuntu: ~/Desktop
File Modifica Visualizza Terminale Aiuto
<client id="12207">
<code>0001</code>
<hash>625A3A073C0E6C09B96E6ADF01996FAC</hash>
<nUploaded>0</nUploaded>
<nDownloaded>8965706</nDownloaded>
<nLastSeen>Tue Dec 18 22:26:55 2007
</nLastSeen>
</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: ~/Desktop
File Modifica Visualizza Terminale Aiuto
<client id="39437">
<code>0002</code>
<hash>90257D2DB80E4CEC6D386092B0936F1D</hash>
<nUploaded>8966051</nUploaded>
<nDownloaded>0</nDownloaded>
<nLastSeen>Tue Dec 18 23:16:26 2007
</nLastSeen>
</client>
<client id="39438">
<code>0002</code>
<hash>10C65B5EFE0E73813B4DFE1D544A6F98</hash>
<nUploaded>0</nUploaded>
<nDownloaded>20480</nDownloaded>
<nLastSeen>Tue Nov 27 11:15:14 2007
</nLastSeen>
</client>
<client id="39439">
<code>0002</code>
<hash>9DDFFE06A00EC2EE776FD34DA91B6F42</hash>
<nUploaded>3293373</nUploaded>
<nDownloaded>0</nDownloaded>
<nLastSeen>Tue Mar 25 18:00:00 2008
</nLastSeen>
</client>
<client id="39440">
notroot@ubuntu: ~/D...
notroot@ubuntu: ~/D...

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 con un database (anche Access)



eMuleForensic
Rappresentazione grafica delle divulgazioni



Conclusioni

- 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 senza necessità di leggere i file binari

Conclusioni

- Limiti
  - Log di eMule poveri
    - No informazioni chiare
  - 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
  - Alcune versioni di eMule nascondono i file di config in altri file