Ciberspazio e diritto 2013, Vol. 14, n. 49 (3-2013), pp. 515-536

Analisi forense di sistemi di *file sharing*

Maurizio Martinelli[1]

Sommario: 1. Introduzione – 2. La diffusione dei sistemi P2P – 3. Architetture delle reti P2P – 4. La disciplina della *Digital Forensics* applicata ai sistemi P2P – 5. Conclusioni

1. Introduzione

Sin dagli esordi della rete Internet, quando la rete si chiamava ancora DARPANET[2] (da DARPA – Defense Advanced Research Project Agency) ed era una rete sperimentale gestita e utilizzata principalmente dal Dipartimento della Difesa americano – DoD, i protocolli e i sistemi di *file sharing* hanno avuto ampia e larga diffusione. In alcuni casi, come ad esempio nel caso del protocollo FTP (*File Transfer Protocol*), essi si sono rivelati addirittura essenziali per il funzionamento della rete. Si pensi, in particolare, agli anni nei quali il protocollo DNS (*Domain Name System*) non era ancora stato ideato e implementato e il sistema di traduzione e associazione di un nome di una risorsa di rete al proprio indirizzo IP (meccanismo della risoluzione diretta) e, viceversa, dell'indirizzo IP al corrispettivo nome (meccanismo della risoluzione inversa) era basato sulla presenza di un unico file centralizzato, denominato HOSTS.TXT e gestito dallo Stanford Research Institute (SRI) in California, che veniva trasferito tra i nodi partecipanti alla rete tramite tipici meccanismi di

[1] Tecnologo presso l'Istituto di Informatica e Telematica del CNR di Pisa (IIT-CNR). Responsabile della Struttura di Servizio "Servizi Internet e Sviluppo Tecnologico" dello IIT-CNR e del Registro .it È responsabile scientifico di vari progetti e collaborazioni di ricerca aventi come tematica principale Internet, i suoi servizi e le sue potenzialità. Ha tenuto oltre 60 corsi di formazione per specialisti e non del settore ed è autore di oltre 90 pubblicazioni.

[2] Successivamente la rete DARPANET ha preso il nome di ARPANET. Nel 1984 è passata sotto la gestione della National Science Foundation (NSF) diventando una rete principalmente accademica e di ricerca e, alla fine degli anni '80, ha preso l'attuale nome di Internet divenendo, con il tempo, la rete a diffusione globale che oggi tutti conosciamo.

file sharing. La definizione delle specifiche del protocollo FTP nel giugno 1980, a cura di John Postel, con l'RFC[3] 765, consentì di formalizzare, nell'ambito delle specifiche del suddetto protocollo, le modalità di trasferimento del file HOSTS.TXT tra le organizzazioni facenti parte della rete. Tuttavia, la soluzione adottata, con il passare degli anni e con il conseguente aumento dei computer connessi alla rete e dei servizi disponibili, non si dimostrò adeguata e, soprattutto, scalabile. La definizione delle specifiche del protocollo DNS nel 1983, con gli RFC 882 e 883, a cura di Paul Mockapetris, un ricercatore dell'Information Science Institute – ISI – in California, e la loro revisione con gli RFC 1034 e 1035 del 1987, consentirono il superamento delle problematiche legate alla risoluzione dei nomi delle risorse di rete e dettero vita a quello che, dopo quasi 30 anni, costituisce ancora il servizio essenziale e fondamentale per il funzionamento della rete.

Oggi Internet è un fenomeno a diffusione mondiale ed è entrata prepotentemente nella vita quotidiana di ognuno di noi, cessando di essere uno strumento utile a una ristretta cerchia di ricercatori e accademici, per diventare un potente e polivalente strumento e mezzo di comunicazione di massa. Utilizzando una semplice, anche se riduttiva definizione, si può affermare che «any entity (household, individual or firm) is considered connected to the Internet if it has the capability of communicating with other entities, via the physical structure of the Internet»[4].

Tale trasformazione della rete ha comportato, necessariamente, che negli anni si modificassero e si evolvessero le modalità di utilizzo e di comportamento dei cosiddetti "internauti". Nomi quali Telnet, FTP, SSH, DNS, SMTP, ecc. sono dei perfetti sconosciuti per la maggior parte di coloro che si sono avvicinati alla rete negli ultimi anni, mentre non lo sono nomi quali Web (oggi nell'accezione più comune identificata, addirittura, con la rete stessa), Google, Youtube, Facebook, Twitter, ecc.

L'utente della rete non si può più definire "utente" nel senso di "utilizzatore" e "mero fruitore di un servizio", perché esso partecipa e collabora, con i propri contenuti, le proprie idee, i propri contributi, i pro-

[3] RFC è l'acronimo di Request for Comments. Costituiscono i documenti standard della rete Internet e sono rilasciati dall'Internet Engineering Task Force (IETF).

[4] Cfr. S. Greenstein, J. Prince, *The Practical Handbook of Internet Computing*, Chapman & Hall/CRC Press, Boca Raton, FL, 2004.

pri servizi, alla crescita e all'evoluzione della rete stessa. Siamo passati da un modello basato principalmente sulla "fruizione dei contenuti", ad un modello di "collaborazione e contribuzione"; da un modello architetturale classico di tipo *client-server*, ad un modello *peer-to-peer*, dove ognuno contribuisce e mette a disposizione degli altri la conoscenza, il sapere, le proprie idee e i propri dati.

Questa modalità di comportamento e di utilizzo della rete, trova un forte riscontro nei sistemi di file *sharing* e di tipo *peer-to-peer* (P2P). La tematica del *file sharing* è molto vasta e abbraccia una varietà enorme di applicazioni che consentono, appunto, la condivisione dei file e dei dati. Si pensi al protocollo FTP, alla condivisione di file in ambienti Windows tramite il protocollo NetBIOS, al protocollo SMB (Samba) per la condivisione di directory e, in generale, di *filesystem* tra Sistemi Operativi diversi (Unix, Linux, Windows, MacOSX), ai protocolli NFS (*Network File System*) e AFS (*Andrew File System*) per la condivisione di *filesystem* principalmente in ambienti Unix e Linux, al *Web file sharing*, ecc.

Tuttavia i sistemi P2P sono quelli ai quali, nell'accezione classica si pensa, quando si fa riferimento ai sistemi di *file sharing*.

Per tale motivo, nel presente studio, saranno presi in considerazione i sistemi di *file sharing* basati sui protocolli P2P.

2. La diffusione dei sistemi P2P

I sistemi P2P rappresentano, senza dubbio, la tecnologia più efficiente, veloce, scalabile e, per certi versi, "sicura" (dal punto di vista dell'anonimato di chi li utilizza), per condividere e scaricare da Internet file di qualsiasi natura e contenuto.

Secondo Internet World Stats[5], il numero di utenti Internet a fine giugno 2012 era di oltre 2,4 miliardi, su una popolazione mondiale di circa 7,017 miliardi di persone. L'Asia detiene il primato di utenti Internet con il 44,8%, seguita dall'Europa (21,5%), dal Nord America (11,4%), dal Centro-Sud America (10,4%), ecc.

[5] Cfr. Internet World Stats, "Usage and Population Statistics", http://www.internetworldstats.com/stats.htm (19/3/2013).

In termini di "tasso di penetrazione", cioè rapportando il numero di utenti Internet con la popolazione residente, il Nord America detiene il primato con il 78,6% (78,6 internauti ogni 100 abitanti), seguita dall'Oceania (67,6%) e dall'Europa (63,2%). Fanalino di coda è rappresentato dall'Africa, con 15,6 internauti ogni 100 abitanti.

Per quanto riguarda, invece, il fenomeno del P2P, studi condotti dall'Internet Observatory[6], osservatorio della società tedesca Ipoque[7], che memorizza costantemente il traffico di rete in varie zone geografiche del mondo, l'occupazione di banda generata dal traffico P2P in Europa raggiunge livelli pari a circa il 25% della banda totale e, di questo 25%, oltre il 50% è generato dal protocollo BitTorrent[8] durante le ore notturne.

Secondo il recente rapporto "The Application Usage and Threat Report"[9], condotto dalla società californiana Palo Alto Networks[10] (società peraltro produttrice di firewall di prossima generazione di tipo *application based*, in luogo dei tradizionali firewall di tipo *port based*), su un campione di 3.065 organizzazioni dislocate in varie parti del mondo, l'analisi del traffico di rete ha rivelato che i sistemi di *file sharing* basati sulla tecnologia P2P hanno un'occupazione di banda dieci volte superiore a quelli di tipo *Web file sharing* o *Browser-based* (60% rispetto al 10%) e oltre il doppio rispetto a quelli di tipo *client-server* tradizionali (FTP, Dropbox, FASP), con una percentuale pari al 60% rispetto al 28%.

Tuttavia, le reti P2P non sono utilizzate solo per la condivisione dei contenuti. Applicazioni di tipo VoIP (*Voice Over IP*) e di videoconferenza, quali Skype, o applicazioni di *Instant Messaging* quali Messenger, Jabber, Licq, AOLIM, Google Talk, Yahoo Messenger, ecc., si basano sullo stesso paradigma di funzionamento.

[6] http://www.internetobservatory.net.

[7] http://www.ipoque.com.

[8] http://www.bittorrent.com.

[9] Cfr. Palo Alto Networks, "An Analysis of Application Usage and Related Threats – Regional Finding", *The Application Usage and Threat Report*, http://media.paloaltonetworks.com/documents/Application-Usage-and-Risk-Report-Mar2013-regional-findings.pdf, (27/3/2013).

[10] http://www.paloaltonetworks.com.

3. Architetture delle reti P2P

Le reti P2P costituiscono una tra le tecnologie chiave che meglio si adatta alla nuova concezione di Internet, basata sempre più su servizi di rete che consentono l'accesso al dato e all'informazione non tramite una specifica risorsa di rete (tipicamente un server) che la possiede, ma sulla base del contenuto che si sta cercando (concetto del *Content-Centric Networks* – CCN). In sostanza, ciò significa che un dato può essere recuperato da qualsiasi dispositivo di rete che lo possegga e non necessariamente da una specifica locazione sulla rete. In generale, le reti P2P si basano, infatti, su una propria rete logica, detta di *overlay*, che si sovrappone a Internet e dove, nella maggior parte dei casi, non prevale il principio di server o gestore (controllore) centrale. Vale, invece, il concetto che gli utenti mettono a disposizione le proprie informazioni, condividendo parte della potenza computazionale, della capacità di storage e di banda del proprio computer e ricevendo, in cambio, servizi *content-centric*, ossia servizi che consentono di ottenere i contenuti cercati.

I nodi della rete sono "paritari" (e da qui il termine *peer*) e contribuiscono tutti al mantenimento e alla crescita della rete stessa, svolgendo, allo stesso tempo, la funzione di client e server (e da qui il termine *servent*, coniato appositamente per identificare il ruolo dei nodi delle reti P2P).

Esistono due architetture principali di reti P2P:

- strutturate;
- non strutturate.

Le reti P2P strutturate si pongono come principale obiettivo quello di migliorare la localizzazione delle risorse. A tal fine, prevedono che la rete di *overlay* sia organizzata secondo principi piuttosto rigidi, che siano presenti vincoli sul grafo e sul posizionamento delle risorse stesse e, di conseguenza, che i peer non siano organizzati in un grafo *random*: ogni volta che un peer si connette alla rete ottiene un identificatore univoco che gli consente di occupare una posizione ben definita nella rete di *overlay* e di selezionare i *peer* con i quali eventualmente stabilire un contatto.

Per brevità di esposizione, sarà esaminata nel dettaglio soltanto l'architettura delle reti P2P non strutturate, anche in considerazione del fatto che sono quelle che meglio riflettono il comportamento di funzionamento delle reti P2P comunemente conosciute.

3.1 Le reti P2P non strutturate

A differenza delle strutturate, le reti P2P non strutturate non prevedono, come dice il nome stesso, una ben definita struttura della rete di *overlay*. A parte alcuni casi specifici (come vedremo meglio in seguito), esse possono essere considerate, a tutti gli effetti, delle reti *mesh*, con un'architettura completamente magliata e grafi casuali e non predicibili. Tuttavia, in alcune reti P2P non strutturate, i peer sono organizzati secondo modalità diverse e non tutti ricoprono la stessa funzione. Da qui la classificazione delle reti P2P non strutturate in tre principali categorie:

1. ibride;
2. decentralizzate pure;
3. parzialmente decentralizzate.

Le reti ibride sono state tra i primi modelli di reti non strutturate. Ogni peer mette a disposizione i propri contenuti, ma è necessario un server centrale (uno o più) che svolga la funzione di "indice dei contenuti" dell'intera rete e fornisca il servizio di ricerca delle risorse. In questo caso, tutti i peer interrogano il server per effettuare la ricerca del contenuto e, successivamente, stabiliscono una connessione (tipicamente TCP) con il peer che possiede il contenuto cercato.

Napster[11], il primo sistema P2P di *file sharing* di massa, affacciatosi sulla rete Internet il 1 giugno 1999, era basato su tale modello. I principali limiti di tale architettura possono essere così sintetizzati:

- gestione onerosa del server centrale;
- *bottleneck* costituito dal nodo centrale e, quindi, scalabilità limitata;
- *single point of failure*, sia dal punto di vista tecnico che, eventualmente, legale.

Le reti decentralizzate pure costituiscono il modello più collaborativo delle reti P2P. Tutti i peer ricoprono lo stesso ruolo e hanno le stesse responsabilità. I nodi sono organizzati in una rete di *overlay*, dove la posizione assunta è casuale. Quando un nuovo peer si connette alla rete, deve conoscere l'indirizzo IP di almeno un nodo (*bootstrap node*) che lo accet-

[11] http://www.napster.com.

ta come *neighbour*. Successivamente, il nuovo nodo stabilisce connessioni con gli altri peer attraverso un meccanismo di *ping flooding* che, inizialmente, viene veicolato attraverso il *bootstrap node* e, successivamente, tramite i peer che hanno accettato il nuovo nodo come *neighbour*. È chiaro che, in un'architettura del genere, il limite principale risiede nell'identificazione di un *bootstrap node* e, pertanto, le reti decentralizzate pure hanno seguito, per tale motivo, approcci diversi che vanno dalla presenza di un *bootstrap server* (server che memorizza una lista di peer attivi), alla *peer cache* (ogni peer mantiene nella propria *cache* una lista di peer contattati precedentemente), alla *well known host* (non esiste alcuna entità che registra i peer attivi). Gnutella v0.4 è un esempio di sistema P2P basato su quest'ultimo modello.

Le reti parzialmente centralizzate suddividono i peer in due classi: i "supernodi" (o *superpeer* o *ultrapeer*) e i "nodi semplici" (o *ordinary peer* o *leaf peer*). I *superpeer* sono quei nodi dotati di buona connettività e buona capacità computazionale che formano, a loro volta, delle reti non strutturate dove essi agiscono come server locali. In tali sottoreti, i *superpeer* mantengono l'indice delle risorse disponibili presenti nei *leaf peer* che gestiscono e svolgono, per essi, una funzione di directory centralizzata. I *superpeer* sono identificati dinamicamente tramite uno specifico algoritmo di elezione. I vantaggi di questa soluzione sono la riduzione del tempo di *discovery* delle risorse, la limitazione del *ping flooding* ai soli *superpeer* e lo sfruttamento delle effettive potenzialità dei nodi peer partecipanti alla rete. Gnutella v0.6 e Skype sono esempi di sistemi P2P basati su questo modello.

4. La disciplina della Digital Forensics applicata ai sistemi P2P

I sistemi P2P, grazie alla loro versatilità, velocità di trasmissione, semplicità d'uso e di configurazione dei client disponibili in rete, indipendenza, nella maggior parte dei casi, da server centralizzati, possibilità di utilizzo da computer senza elevate potenze computazionali e, una elevata forma di garanzia di anonimato, sono, ormai da anni, utilizzati largamente per la condivisione di materiale digitale protetto da copyright, in particolare musica e film. Tuttavia, negli anni più recenti, la loro tecnologia si è rivelata un canale di trasmissione "sicuro" e particolarmen-

te attraente, anche per soggetti atti a delinquere, quali terroristi e pedofili. A ciò si aggiunga, sempre recentemente, l'utilizzo delle reti P2P per la diffusione massiva e incontrollata di virus, malware e spyware. È naturale, pertanto, che se Internet e la rivoluzione digitale, avvenuta negli ultimi 10-15 anni, hanno portato indubbi vantaggi sia a livello di diffusione delle informazioni, che a livello comunicativo e sociale, la rete ha tuttavia modificato, inevitabilmente, i tradizionali sistemi di analisi e di indagine dei crimini. È in questo contesto, che bene si inquadra l'analisi forense e, in particolare, la *Digital Forensics*, cioè quella scienza che, attraverso un "processo teso alla manipolazione controllata e, più in generale, al trattamento di dati e/o informazioni digitali e/o sistemi informativi per finalità investigative e di giustizia"[12] e, adottando procedure tecnico-organizzative che garantiscano l'integrità e l'autenticità delle informazioni, studia il valore che un'informazione digitale può avere in ambito giuridico.

Nell'accezione più comune, per *Digital Forensics* o *Computer Forensics* (se il campo di indagine principale è costituito dai computer), si intende anche quel processo investigativo che, tramite l'adozione di opportune tecniche informatiche, consente di identificare, acquisire, conservare e analizzare reperti informatici che potrebbero avere valore probatorio in giudizio e costituire, pertanto, delle *digital evidence*, ossia delle evidenze digitali. È una disciplina che trova le sue origini negli anni '80-'90 negli Stati Uniti e in Gran Bretagna e integra competenze tecnico-informatiche con competenze giuridiche. Tuttavia, con l'aumentare dei crimini informatici e la necessità, per le forze dell'ordine e per i cosiddetti *forensicator* (cioè coloro che praticano la *Computer Forensics*), di avere sistemi, strumenti e norme standard a livello internazionale da poter seguire e applicare, a partire dagli anni 2000, vari gruppi di lavoro e organismi si sono cimentati nella realizzazione e pubblicazione di linee guida in tale settore. L'attuazione della *Convention on Cybercrime*, conosciuta anche come "Convenzione di Budapest" (pubblicata il 23 novembre 2001 e entrata in vigore il primo luglio 2004[13]), con l'obiettivo di armonizzare

[12] Cfr. S. Aterno, F. Cajani, G. Costabile, M. Mattiucci, G. Mazzaraco, *Computer Forensics e Indagini Digitali. Manuale tecnico-giuridico e casi pratici*, vol. I, Esperta S.r.l., p. 3.

[13] L'entrata in vigore della Convenzione di Budapest prevedeva la sua ratifica da parte di cinque nazioni, delle quali almeno tre appartenenti al Consiglio d'Europa.

le normative nazionali in tale settore e favorire la cooperazione tra i vari Paesi e recepita in Italia con la legge 48/2008, ha costituito, senz'altro, una pietra miliare nella storia della legislazione italiana in materia di reati informatici, in considerazione anche del fatto che, con tale normativa, viene sancito il principio secondo il quale la validità delle informazioni prescinde dal supporto fisico nel quale esse sono contenute e va a colmare, di fatto, un vuoto formale nella giurisprudenza sulla necessità di operare sui sistemi e sui dati informatici con modalità tecnico-organizzative adeguate (artt. 244, 247, 254-bis e 260 c.p.p., solo per citarne alcuni).

Tuttavia, essendo Internet, per sua natura, un luogo virtuale e parallelo a quello reale, non facilmente localizzabile e, al tempo stesso, sovranazionale, esso pone concreti rischi di attuazione della legislazione di un Paese in relazione ad un determinato reato e, in alcuni casi, rischi di sovrapposizione tra diverse giurisdizioni sulla persecuzione del reato stesso.

Risulta, quindi, fondamentale valorizzare e adottare un approccio investigativo che sia maggiormente orientato verso la cooperazione internazionale tra i Paesi e che sia basato su modalità di cooperazione snelle che prevedano rapporti diretti tra le autorità giudiziarie e tempi di intervento rapidi.

Relativamente ai sistemi P2P, le attuali regolamentazioni e linee guida non disciplinano esplicitamente le modalità di espletamento dell'analisi forense, anche a causa della struttura e architettura complessa di detti sistemi che vedono il coinvolgimento di molti attori (colui che effettua il download dell'informazione, coloro che la rendono disponibile, gli *Internet Service Provider* coinvolti, gli *Access Provider*, ecc.), alcuni dei quali spesso localizzati oltre i confini nazionali e in Paesi dove l'attività perseguita può anche non costituire reato. Valgono, tuttavia, i criteri fondamentali della *Digital Forensics*, sintetizzabili nelle seguenti quattro fasi principali:

1. fase di identificazione o individuazione del supporto contenente la potenziale prova (computer desktop, server, smartphone, hard disk, tablet, ecc.);
2. fase di acquisizione e preservazione delle informazioni digitali presenti sul supporto, al fine di garantirne l'autenticità e l'integrità (fase di *system preservation*);

3. fase di ricerca e analisi della prova, che può prevedere anche la combinazione di dati provenienti da fonti diverse, soprattutto nel caso di applicazioni e sistemi distribuiti (fase di *evidence searching*). Tale fase può prevedere, a sua volta, due possibili scenari:
   a. acquisizione di un sistema *live*, che viene effettuata mentre il sistema è ancora acceso e consente di non perdere le cosiddette "evidenze volatili", cioè quelle informazioni che vengono cancellate nel momento in cui il sistema viene spento (dati in RAM, processi attivi, connessioni di rete attive, utenti attivi sul sistema, ecc.);
   b. acquisizione di un sistema *dead*, detta anche acquisizione *post mortem*, che consiste nella modalità di acquisizione classica e che, come dice il termine stesso, avviene a sistema spento;
4. fase di presentazione, che prevede la verifica dei risultati ottenuti e la documentazione e la reportizzazione di tutto quanto fatto durante il processo di investigazione digitale.

È importante, tuttavia, tenere in considerazione che i sistemi P2P, per la natura delle informazioni scambiate e per l'utilizzo che spesso viene fatto di essi, sono molteplici, variegati e in continua evoluzione. Di conseguenza, anche il numero delle applicazioni client che li utilizzano è molto elevato e lo sviluppo di sistemi di analisi forense che riescano a star dietro all'evoluzione della tecnologia in tale settore, costituisce un'impresa assai ardua.

Le *suite* più note per l'analisi forense[14] (Encase, FTK, X-Ways Forensics, OSForensics, ecc.) non offrono funzionalità per l'analisi delle informazioni dei sistemi P2P. Risulta, quindi, indispensabile dotarsi di software specifici per l'analisi dei singoli applicativi e, talvolta, integrare tali software con altri *tool* che consentano di svolgere parti del processo di analisi che il software principale non consente di fare.

La stragrande maggioranza dei software per l'analisi dei sistemi P2P è di tipo commerciale. Esistono, tuttavia, anche software *freeware* e *open source*, molti dei quali supportano, principalmente, il client P2P eMule.

[14] Alcune *suite* sono validate e certificate dal NIST (National Institute for Standards and Technology - http://www.nist.gov) e possiedono una *Recognition in Court*, ovvero la loro validità ha riconoscimento in sede giudiziaria.

Pertanto, nell'ambito di questo elaborato, sarà preso in considerazione il sistema eMule e i principali aspetti dell'analisi forense rivolta a tale applicativo.

4.1 Il software P2P eMule

eMule[15] è uno dei client P2P più diffusi, che utilizza le reti P2P ed2k (eDonkey) e KAD, quest'ultima basata sul protocollo Kademlia. eMule è stato sviluppato dal programmatore tedesco Hendrik Breitkrenz, conosciuto anche come Merkur, che l'ha reso disponibile in rete nell'agosto del 2002. Il client è *open source*, distribuito sotto licenza GPL[16], ed è stato sviluppato per ambiente Windows. L'ultima versione disponibile è la 0.50a. Tuttavia, può essere utilizzato anche negli ambienti Mac OSX e Linux tramite *Wine*[17]; in alternativa è disponibile, per detti ambienti, il *client aMule*, sviluppato nell'ambito di un progetto affiliato con eMule, che consente l'utilizzo della tecnologia eMule su Linux, Mac OSX, BSD e Solaris.

L'architettura della rete ed2k è di tipo "ibrida", costituita da client e server. I server contengono gli indici dei file disponibili e gestiscono le connessioni tra gli utenti, comunicano tra di loro e si distribuiscono il carico di lavoro. Le informazioni sono, invece, disponibili sui client che partecipano alla costituzione della rete.

La rete KAD, basata sul protocollo Kademlia, è invece una rete P2P priva di server e di tipo "decentralizzata pura". Si basa sulla tecnologia *Distributed Hash Table* (DHT), che rappresenta la più recente evoluzione dei sistemi P2P strutturati.

4.2 Analisi forense di eMule

L'ambiente di lavoro utilizzato nello specifico, ai fini dell'analisi forense di un computer sul quale sia utilizzato il software P2P eMule, prevede un sistema operativo Windows XP (o Windows 7) sul quale sia installato il client eMule 0.50a e due *tool* specifici per l'analisi forense di eMule: eMule Reader 1.0 e eMule MET Viewer 1.1.2.0.

[15] http://www.emule-project.net.

[16] GNU *General Public License* – http://www.gnu.org.

[17] Wine è un applicativo che consente di far girare programmi sviluppati per Windows anche su sistemi Mac OSX, Linux e BSD - http://www.winehq.org.

Di *default* eMule viene installato nella *directory* C:\Programmi\eMule. Tale directory contiene, a sua volta, altre sette *directory*, delle quali, ai fini dell'analisi forense, quelle rilevanti sono la *directory Incoming* e la *directory config*. Esiste, infatti, anche una *directory* denominata *logs*, ma sfortunatamente, eMule non genera alcun file di *log* durante la sua attività e, pertanto, essa risulta irrilevante ai fini dell'analisi. La *directory Incoming* contiene i file condivisi, cioè quelli scaricati dalla rete e quelli messi a disposizione di altri client P2P. La *directory config* contiene, invece, alcuni file fondamentali per il corretto funzionamento di eMule e un insieme di file che risultano determinanti per l'indagine investigativa. Essi contengono, infatti, un'ingente quantità di informazioni relative alle attività di scambio di dati effettuate, quali, ad esempio, i file condivisi con altri utenti, i client che sono riusciti a scaricare file dal computer locale, i client con i quali il computer locale ha aperto una connessione ed ha scaricato file, l'identificativo del client locale nell'ambito della rete P2P, ecc. Alcuni di questi file hanno l'estensione *.dat*, mentre gli altri hanno l'estensione *.met*. In alcuni casi, i primi sono leggibili tramite un comune editore di testo (ad esempio Notepad), gli altri non sono mai in formato leggibile (testuale, xml, csv, ecc.), ma sono codificati secondo una struttura dati definita nel codice sorgente di eMule stesso. Fortunatamente tale codice sorgente è disponibile in rete, essendo eMule distribuito sotto licenza GPL e, pertanto, ciò ha consentito la realizzazione di *tool* ad hoc per la loro decodifica e, quindi, per l'analisi forense. Esempi di tali strumenti sono eMule Reader™ e eMule MET Viewer.

Tuttavia, prima di analizzare il contenuto di tali file mediante i suddetti *tool*, vale la pena soffermarci su un altro fattore rilevante ai fini dell'analisi forense di eMule, vale a dire la possibilità per tale client, di essere utilizzato in modalità condivisa tra gli utenti del computer sul quale è installato. Infatti, al momento dell'installazione, eMule chiede, tra le varie cose, se si desidera modificare il *default path* di installazione e se si vuole rendere utilizzabile in maniera condivisa con gli altri utenti di Windows presenti sul sistema.

Per poter capire ciò, è necessario analizzare alcune "chiavi" del registro di sistema di Windows, che costituisce il *database* nel quale sono memorizzate tutte le impostazioni e opzioni secondo le quali Windows e le applicazioni su di esso installate funzionano. Regedit.exe costituisce

un editor del registro di sistema di Windows che, tramite un'interfaccia grafica simile all'*utility* Esplora di Windows, consente di visualizzare (ed eventualmente anche modificare, cancellare e aggiungere) la struttura del registro e, quindi, le "chiavi" e i "valori" ad esse associati.

Nel caso preso in considerazione, alla chiave *HKEY_CLASSES_ROOT\eMule\DefaultIcon\shell\open\command* è associato il valore *C:\Programmi\eMule\eMule.exe* e ciò sta ad indicare che il software eMule è installato nella *directory C:\Programmi\eMule* e che il suo eseguibile si chiama *eMule.exe*.

Un'altra chiave di registro interessante ai fini dell'analisi, è la chiave *HKEY_CURRENT_USER\Software\eMule*. Visualizzandone il contenuto, si ricava l'*Install Path* (comunque ricavabile anche dalla chiave mostrata precedentemente), l'*Installer Language* (che nel caso in oggetto contiene il valore 1040, corrispondente alla lingua italiana) e la chiave *UsePublicUserDirectories*, che può assumere i seguenti tre valori:

- "0", che sta ad indicare che ogni utente del computer ha una propria personalizzazione di eMule, sia a livello di configurazione che di file condivisi;
- "1", che eMule è condiviso tra gli utenti del sistema e che vi è un'apposita *directory* sotto la quale i file di configurazione e quelli condivisi sono memorizzati;
- "2", che eMule è condiviso tra gli utenti del sistema e che utilizza la *program directory*, cioè la *directory* dove eMule è installato, per contenere le directory *Incoming* e *config* dedicate ai file condivisi e ai file di configurazione.

Passiamo, adesso, all'analisi dei file contenuti nella *directory config*.

Il numero di tali file è piuttosto ingente e non tutti risultano rilevanti ai fini dell'analisi forense di eMule. Esamineremo, pertanto, soltanto quelli ritenuti più idonei allo scopo. Per visualizzare il contenuto dei file con estensione *.met* e, quelli con estensione *.dat* non in formato leggibile, utilizzeremo il *tool* eMule Reader™.

Il software eMule Reader™[18] è costituito da un insieme di programmi, eseguibili da linea di comando, che consentono di analizzare sia i file di configurazione *.dat* e *.met* di eMule, che quelli da esso utilizzati per lo scambio di dati sulla rete.

[18] http://cybermarshal.com/index.php/cyber-marshal-utilities/emule-reader.

È stato sviluppato dalla ATC-NY, una sussidiaria della società statunitense Architecture Technology Corporation[19], specializzata nella ricerca e sviluppo di prodotti per la *computer e digital forensics*, quali, ad esempio, i prodotti commerciali P2P Marshal, Live Marshal, Mac Marshal, Mobile Marshal, ecc., utilizzati dalle forze dell'ordine americane.

È costituito da dieci programmi, ognuno dei quali ha il compito di analizzare il contenuto di uno o più file:

- *ParseCancelled.exe* analizza *cancelled.met*;
- *ParseClients.exe* analizza *clients.met*;
- *ParseKeyIndex.exe* analizza *key_index.dat*;
- *ParseKnown.exe* analizza *known.met*, *known2.met* e *known2_64.met*;
- *ParseLoadIndex.exe* analizza *load_index.dat*;
- *ParseNodes.exe* analizza *nodes.dat*;
- *ParsePartMet.exe* analizza i file con estensione *part.met*;
- *ParseServer.exe* analizza *server.met*;
- *ParseSourceIndex.exe* analizza *src_index.dat*;
- *ParseStoredSearches.exe* analizza *StoredSearches.met*.

La sintassi di utilizzo dei singoli programmi è la seguente:

NomeProgramma [-dh] -i <infile> -o <outfile>

Nel caso in cui l'opzione "-o" non sia utilizzata, il risultato del comando viene visualizzato a schermo.

Oltre ai file indicati precedentemente, la *directory config* di eMule contiene, in realtà, anche altri file che possono risultare utili ai fini di individuare le attività compiute sul sistema. In particolare, il file *AC_SearchStrings.dat*, che contiene un elenco ciclico (al massimo costituito da 30 elementi) delle parole chiave utilizzate dall'utente per cercare informazioni sulla rete. Tale file, che può essere visualizzato tramite un comune editore di testo, quale Notepad di Windows, può risultare utile ai fini delle indagini in quanto consente di profilare le abitudini di utilizzo del software eMule da parte dell'utente (o degli utenti) che lo utilizzano.

Nel caso esaminato, tale file contiene un'unica parola chiave di ricerca, che corrisponde a "*phil collins*".

[19] http://www.atc-nycorp.com.

Il file *cancelled.met* contiene l'elenco dei file per i quali l'utente ha annullato il processo di *download* dalla rete. Tale file può contenere informazioni a patto che l'utente abbia selezionato l'opzione di configurazione di eMule "Ricorda i File Cancellati". Nel caso in questione, il tool *ParseCancelled.exe* rivela che esso non contiene alcun valore.

Il file *known.met* contiene l'elenco dei file scaricati e condivisi dall'utente. Per ogni file, sono indicati: il nome del file; la dimensione; la data di ultima modifica (che consente di ricavare, con una granularità che arriva ai secondi, quando è stato completato il download del file sul computer); l'*hash* del file (che costituisce il suo identificatore sulla rete); l'*hash* delle varie parti che lo compongono; la data di ultima condivisione sulla rete; il numero di richieste di download del file da parte di client remoti e il numero di richieste di download remoto effettivamente accettate; la velocità di trasferimento, ecc.

Tale file costituisce, pertanto, un vero e proprio archivio in grado di fornire informazioni molto utili ai fini dell'indagine forense. Nel caso in esame, la sua visualizzazione, tramite il tool *ParseKnown.exe*, ha un formato di output testuale simile al seguente:

File Descriptor Values:
File Name: Phill Collins – Phil Collins – Sussudio.mp3
File Size: 4199916
Last Modified: Wed Mar 20 19:07:36 2013

Part Descriptor Values:
Part Name: 005.part
Hash Values:
AICH Master Hash: 1D AF E1 67 1E AE 23 3E P6 06 65 CA 87 FD 26 40 97 DA 08 9D
……

Allo scopo di rendere il contenuto di tale file maggiormente fruibile, comprensivo e dettagliato ma, soprattutto, esportabile in un formato utilizzabile e elaborabile anche da altre applicazioni, un programmatore austriaco, di nome Werner Rumpeltesz[20], ha sviluppato un *tool*, denominato

[20] http://www.gaijin.at.

eMule Met Viewer (la versione utilizzata per questa analisi è l'ultima rilasciata e cioè la v1.1.2.0), che consente di visualizzare graficamente tutte le informazioni presenti nel file *known.met* e esportarle in formato CSV[21].

Nel caso in cui l'analisi forense di eMule non veda coinvolto un singolo computer, ma sia condotta parallelamente su più sistemi utilizzati da soggetti diversi, oltre al file *known.met*, acquistano importanza e rilevanza anche i contenuti dei file *clients.met* e *preferences.dat*.

Il file *clients.met* contiene, infatti, l'elenco degli utenti (client) con i quali si è svolta attività di scambio e condivisione di informazioni, sia in download che in *upload* e, per ciascuno di essi, fornisce informazioni quali: la chiave identificativa del client dal quale è stato trasferito un file o parte di esso (operazione di download); la chiave identificativa del client che ha, invece, scaricato un file, o parte di esso, dal sistema locale (operazione di upload); la data (con granularità fino ai secondi) di ultimo contatto con un client, ecc. Il file serve, inoltre, a calcolare i crediti per la gestione locale della coda di upload.

La sua visualizzazione, tramite il *tool ParseClients.exe*, mostra, nel caso in oggetto, il seguente risultato:

Key: 49 1A 5F E8 CB 0E 1D 30 6D A6 F2 53 B9 88 6F D1
Uploaded: 0
Downloaded: 733958
Last Seen: Wed Mar 20 19:07:50 2013
Reserved: 0
Key Size: 76
Secure Identity: 30 4A 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 39 00 30 36 02 ……
_____Key: 5D 3A 0F CE 94 0E 50 7C 0C 0B 37 6D 3F 55 6F 14
Uploaded: 32529
Downloaded: 0
Last Seen: Wed Mar 20 19:37:01 2013
Reserved: 0
Key Size: 76

[21] *Comma Separated Values* (CSV) è un formato testuale molto comune utilizzato per l'esportazione e l'importazione di dati.

Secure Identity: 30 4A 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 39 00 31 00 A9 ……

Preferences.dat[22] è un file di 61 byte che contiene l'*hash* dell'utente (16 byte). Il valore di tale *hash* è calcolato, in maniera *random*, al momento del primo avvio di eMule sul sistema ed è utilizzato per identificare il client nella rete P2P.

È chiaro, pertanto, che dall'analisi della combinazione del contenuto dei file *clients.met* e *preferences.dat* presenti su più computer coinvolti in un'indagine, è possibile stabilire le relazioni che quei computer hanno avuto con altri client della rete e, eventualmente, tra di loro. Viene effettuata, cioè, quella che in gergo tecnico, viene definita *link analysis*[23], una metodologia che consente di valutare le relazioni tra i nodi di una rete.

L'applicazione della *link analysis* ad una rete P2P, quale quella in esame, ha come risultato un grafo nel quale ad ogni nodo corrisponde un client eMule e, per ogni nodo, entrano e/o escono archi orientati. I nodi senza archi uscenti indicano che non vi è stata, verosimilmente, una diffusione delle informazioni ad altri client della rete.

È naturale che, tali considerazioni sono basate su quanto rinvenuto nei file di configurazione di eMule. Tuttavia, è bene sottolineare che tale analisi presenta, indubbiamente, alcuni limiti. Infatti, nonostante ciò non rappresenti una prassi comportamentale comune, l'utilizzatore di eMule può cancellare, se lo desidera, alcune informazioni contenute nelle *directory config* e *Incoming*, andando ad alterare, di conseguenza, le tracce lasciate da eMule sul computer e la storia delle attività compiute dall'utente sulla rete. I file *known.met* e *clients.met*, se cancellati, sono, infatti, rigenerati automaticamente da eMule al suo successivo riavvio. Ciò significa che, se cancello il file "abc" dalla directory *Incoming* e cancello anche il file *known.met*, al successivo riavvio eMule genererà un nuovo *known.met* privo del file "abc". Analogamente, se cancello il file *clients.met* elimino, in maniera semplice e immediata, tutta la storia delle connessioni avute con altri peer.

[22] Il contenuto di tale file non è decodificabile tramite il software eMuleReader™.

[23] Uno dei campi di applicazione dove, negli ultimi anni, la *link analysis* ha avuto larga diffusione, è quello dei *Social Network* per studiare e capire le relazioni e gli interessi degli utenti.

Tuttavia, va anche detto che, se le condizioni lo permettono, tali limiti potrebbero essere superati da un'analisi forense di tipo *live* e non *post-mortem*. L'analisi *live* permetterebbe, infatti, di intercettare il traffico di rete tra i nodi peer oggetto dell'indagine. Questo tipo di analisi, che si colloca nell'ambito della cosiddetta *Network Forensics*, oltre a prevedere l'utilizzo di strumenti ad hoc quali *sniffer* e analizzatori di rete (TCPdump, Wireshark, ecc.), presuppone che si possa fare un'indagine forense nel momento in cui il crimine viene perpetrato. Tramite l'analisi *live*, oltre a intercettare i file oggetto di scambio, sarebbe possibile individuare anche gli indirizzi IP dei nodi coinvolti nello scambio stesso. Effettuando poi, tramite un client whois[24], una richiesta allo specifico Regional Internet Registry[25] (RIR), si potrebbe risalire al nome dell'organizzazione assegnataria di quel particolare indirizzo IP (e del Local Internet Registry[26] (LIR) che ha avuto dal RIR la delega alla gestione del blocco di indirizzi IP del quale l'IP in oggetto fa parte), nonché ad informazioni relative alla geo-localizzazione di tale organizzazione (stato, città, indirizzo) e ai relativi contatti di riferimento (telefono, fax e, in alcuni casi, e-mail). In pratica, in molti casi si potrebbe riuscire a risalire al soggetto che ha effettivamente commesso il reato.

Infine, sempre nell'ambito delle tecniche di indagine forense basate sull'acquisizione *live*, si potrebbe ipotizzare una soluzione che preveda la realizzazione di "nodi *peer* civetta", mantenuti e controllati dalle for-

[24] WHOIS è un servizio di tipo *client-server* nato sulla rete ARPANET nel 1982, con lo scopo di mantenere informazioni sull'allocazione delle reti IP e sulle organizzazioni e i contatti di riferimento per tali reti. Successivamente, è entrato a far parte dei cosiddetti "servizi essenziali" offerti dai country code Top Level Domain (ccTLD) e general Top Level Domain (gTLD) per la consultazione dei nomi a dominio registrati e dei relativi contatti.

[25] Allo stato attuale, lo spazio di allocazione degli indirizzi IPv4 e IPv6 è assegnato da ICANN (Internet Corporation for Assigned Names and Numbers) a cinque Regional Internet Registries che sono: RIPE-NCC per l'Europa, l'Asia Centrale e il Medio Oriente; ARIN per il Nord America; LATNIC per il Centro e Sud America; AfriNIC per L'Africa e APNIC per l'Asia Meridionale e l'Area del Pacifico.

[26] Un Local Internet Registry (LIR) è un'organizzazione, accreditata presso un Regional Internet Registry (RIR), alla quale il RIR ha delegato la gestione di uno o più blocchi di reti IP (IPv4 e IPv6). I LIR, che generalmente sono *Internet Service Provider*, ma anche grandi istituzioni accademiche e di ricerca, assegnano, a loro volta, reti o sotto-reti IP ai loro clienti.

ze dell'ordine e che siano parte integrante della rete P2P che si desidera monitorare. In tal caso, il campo di azione e di monitoraggio sarebbe molto più vasto (con tutti i vantaggi e gli svantaggi che ne derivano) in conseguenza dell'elevato numero di attori coinvolti ma, tuttavia, consentirebbe di poter fare uso sia degli strumenti tipici della *Network Forensics*, che di quelli specializzati nell'analisi forense dei software P2P, sopra esposti.

5. Conclusioni

Internet è diventato, ormai, un fenomeno di diffusione di massa. La rete, negli anni, si è fortemente evoluta e, con essa, le sue tecnologie e modalità di utilizzo. Basti pensare che, soltanto a livello europeo, le stime parlano di circa 600 milioni di cellulari abilitati a Internet e si ipotizza che, in meno di due anni, i dispositivi wireless supereranno, in numero, i tradizionali computer cablati. È naturale che, con questo scenario, se da un lato il cittadino della rete trae indubbi vantaggi a livello comunicativo, sociale e conoscitivo, dall'altro, le caratteristiche che contraddistinguono Internet e che sono alla base del suo sviluppo e della sua enorme diffusione, vale a dire la sua natura transnazionale, la non regolamentazione da parte dei governi, l'apertura e la conoscenza dei suoi protocolli, la collaborazione nello sviluppo di applicazioni e sistemi, ecc., fanno sì che la rete costituisca un ambiente ideale per poter svolgere determinate tipologie di attività illegali. Tra di esse, ricordiamo le frodi su transazioni ed acquisti, sia in relazione al materiale acquistato su Internet che sui mezzi di pagamento; la violazione del *copyright*; il commercio di materiale pedopornografico; il coordinamento di attività terroristiche, di traffici di armi, di droga, di persone, ecc.; le azioni di pirateria informatica criminale volte a realizzare atti di spionaggio industriale, *cyber* terrorismo, diffusione di *virus*, *trojan*, *malware*, *worm*, con lo scopo di distruggere sistemi e servizi; attacchi di tipo *Denial of Service* (DoS) e *Distributed Denial of Service* (DDoS) e così via.

Per cercare di contrastare tale fenomeno, molti Paesi stanno sviluppando e adottando strategie per individuare e prevenire la criminalità informatica. Tuttavia, affinché la problematica possa essere affrontata in modo efficace e concreto, è ormai opinione comune che gli strumenti legislativi propri di una giurisdizione nazionale non siano suffi-

cienti. Risulta fondamentale, pertanto, migliorare la cooperazione a livello internazionale tra i vari Paesi, iniziando dall'ambito europeo sino ad arrivare ad una copertura mondiale, prevedendo una strategia giuridica che consenta alle autorità di un Paese di poter avere, ad esempio, accesso alle informazioni detenute da una società residente in un'altra nazione e utilizzando protocolli di comunicazione snelli, basati su rapporti diretti tra le autorità giudiziarie, con procedure e modalità di intervento rapide e comuni. La Convenzione di Budapest sul *cybercrime* ha rappresentato un enorme passo avanti in tale direzione ma, tuttavia, resta ancora molta strada da percorrere. Basta pensare, infatti, che soltanto 61 Stati su 204 hanno partecipato alla sua elaborazione e che, ad oggi, appena 39 di essi hanno provveduto a ratificarla, dei quali ben 13 negli ultimi tre anni.

A tutto ciò si aggiunga che, l'evoluzione della rete e delle sue tecnologie impongono un continuo sviluppo, miglioramento e aggiornamento delle applicazioni e dei sistemi impiegati nella *Digital Forensics* e, di conseguenza, sforzi non trascurabili dovranno essere impiegati anche nella formazione di personale esperto e competente in tale settore.

Bibliografia

J. Postel, *RFC 765: File Transfer Protocol*, June 1980, http://tools.ietf.org/html/rfc765.

K. Harrenstien, V. White, *RFC 812: NICNAME/WHOIS*, March 1982, http://tools.ietf.org/html/rfc812.

P. Mockapetris, *RFC 882: Domain Names - Concept and Facilities*, November 1983, http://tools.ietf.org/html/rfc882.

P. Mockapetris, *RFC 883: Domain Names - Implementation and Specification*, November 1983, http://tools.ietf.org/html/rfc883.

P. Mockapetris, *RFC 1034: Domain Names - Concept and Facilities*, November 1987, http://tools.ietf.org/html/rfc1034.

P. Mockapetris, *RFC 1035: Domain Names - Implementation and Specification*, November 1987, http://tools.ietf.org/html/rfc1035.

Council of Europe, *Convention on Cybercrime*, November 2001, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

D. Brezinski, T. Killalea, *RFC 3227: Guidelines for Evidence Collection and Archiving*, February 2002, http://tools.ietf.org/html/rfc3227.

S. Greenstein, J. Prince, "The geographical diffusion of the Internet in the United States", in *The Practical Handbook of Internet Computing*, Chapman & Hall/CRC Press, Boca Raton, FL 2004.

Strumenti di investigazione e forensic, Gennaio 2009, http://www.swappa.it.

Digital Investigation e Digital Forensics, Gennaio 2009, http://www.swappa.it.

V. Cardellini, *Corso di Sistemi Distribuiti: Sistemi peer-to-peer*, a.a. 2009-2010, Università degli Studi di Roma "Tor Vergata" - Facoltà di Ingegneria.

G. Costabile, "Computer forensics e informatica investigativa alla luce della Legge n. 48 del 2008", in *Ciberspazio e diritto*, vol. 11, n. 3, 2010, Mucchi Editore, Modena, pp. 465-508.

C. Maioli, M. Ferrazzano, *Control of File Exchange of Illicit Materials in Peer-to-Peer Environments*, Proceedings of the 4th International Conference on Information Law - ICIL, Tessalonica 2011.

D. Laforenza, M. Martinelli, D. Gualerzi, "The Internet Phenomenon", in *JCOM - Journal of Science Communication*, 2011.

M. Epifani, "Strumenti per l'analisi dei software P2P", in *IISFA Italy Chapter*, n. 2, Marzo 2011, pp. 3-6.

S. Aterno, F. Cajani, G. Costabile, M. Mattiucci, G. Mazzaraco, *Computer Forensics e Indagini Digitali. Manuale tecnico-giuridico e casi pratici*, vol. I, II e III, Novembre 2011, Esperta S.r.l.

A. Passarella, "A survey on content-centric technologies for the current Internet: CDN and p2p solutions", in *Elsevier Computer Communications*, vol. 35, Issue 1, January 2012, pp. 1-32.

Palo Alto Networks, "An Analysis of Application Usage and Related Threats - Regional Finding", in *The Application Usage and Threat Report*, 10th Edition, 2013.

P. Stirparo, *Investigazioni ed Analisi Forense*, CLUSIT - Associazione Italiana per la Sicurezza Informatica.

Internet World Stats, *Usage and Population Statistics*, http://www.internetworldstats.com/stats.htm.

Internet Observatory, *Real-time Internet Statistics*, http://www.internetobservatory.net.

Abstract

Analisi forense di sistemi di file sharing

La *Digital Forensics* è un processo investigativo che fa uso di tecniche informatiche per identificare, acquisire, conservare e analizzare indizi o fonti di prova digitali. Nell'ambito del presente studio, è stata applicata la disciplina della *Digital Forensics* ai sistemi di *file sharing* e, in particolare, ai sistemi P2P che rappresentano, senza alcun dubbio, la tecnologia più efficiente, scalabile e con elevate garanzie di anonimato, per condividere e scaricare dalla rete materiale illegale. In particolare, è stata esaminata l'analisi forense del sistema eMule e sono stati impiegati gli strumenti *open source* eMuleReader™ e eMule MET Viewer, per analizzare un caso concreto di utilizzo della rete P2P.

Forensic analysis of file sharing systems

The *Digital Forensics* is an investigative process that makes use of computer techniques to identify, acquire, store, and analyze digital evidence or sources of evidence. In the present study, the *Digital Forensics* has been applied to file sharing systems and, in particular, to the P2P systems that are, without a doubt, the most efficient, scalable, and with high guarantees of anonymity, technologies to share and download illegal material from the network. In particular, we have taken into account the forensic analysis of the eMule system and we have used open source tools such as eMuleReaderTM and eMule MET Viewer to analyze an actual case of use of the P2P network.

Maurizio Martinelli