(XX)

I sottoscritti dott. Antonio d'AMBROSIO e dott. Michele GIGLI, consulenti di parte del dott. Raffaele SOLLECITO, imputato nel procedimento penale n°9066/07, ad integrazione di quanto già dichiarato e sottoscritto nella precedente relazione già depositata, hanno proceduto a una

Analisi del traffico Fastweb

Partendo dal presupposto che il dott. Sollecito Raffaele disponeva all'epoca dei fatti di un contratto con la Società Fastweb, che gli permetteva di restare collegato attraverso la rete telefonica fissa, con utenza 075/9660789, ad **Internet** ininterrottamente 24 ore su 24, abbiamo analizzato i tabulati Fastweb, che sono stati prodotti dalla Società, su richiesta della Polizia Postale e depositati agli Atti del P.M.. Ciò al fine di trovare riscontro oggettivo su quanto da noi affermato nella nostra precedente relazione, stabilire cioè se **l'interazione umana,** riscontrata anche attraverso l'utilizzo di siti che richiedono collegamenti Internet, fosse effettivamente avvenuta attraverso la linea telefonica di rete fissa, corrispondente al numero 075/9660789.
Tutto ciò premesso possiamo affermare che, dai nostri riscontri i tabulati forniti da Fastweb, filtrati per protocollo tcp e poi sulle porte 80 e 25, **confermano** in toto le nostre affermazioni. Il file **Allegato 1** ***"HTTP 30 Ottobre.pdf,"*** annesso a questa nota aggiuntiva, mostra infatti come la risoluzione degli IP dei tabulati conducono ai siti da noi individuati nella cronologia di Safari, mentre il file **Allegato 2** ***"SMTP 30 Ottobre.pdf"*** mostra che la mail è stata effettivamente inviata alle 18.12 del 30 Ottobre 2007 attraverso la connettività in uso a Raffaele Sollecito.

Anche per il giorno 2 Novembre abbiamo trovato riscontro nei tabulati Fastweb come da allegato **Allegato 3,** annesso, ***"HTTP 02 Novembre 12 - 14"***; unica eccezione è stata riscontrata per www.facebook.com per il quale non siamo riusciti a trovare alcuna traccia; stiamo studiando la modalità del funzionamento per verificare se usa protocolli o porte differenti.

Per quanto riguarda il giorno 5 Novembre e 6 Novembre abbiamo individuato traffico Internet verso diversi siti. Di particolare rilievo sono le connessioni al sito dell'Ansa (negli orari da noi evidenziati nella precedente relazione):

IP Nattato	Porta	IP Destinazione	Porta	Data Inizio	Data Fine	Durata	Tipo	Bytes	
213.140.18.128	41814	194.244.5.206	80	05-11-07 23:18	05-11-07 23:18	00:00:00	TCP	25792	www.ansa.it
213.140.18.128	44787	194.244.5.206	80	06-11-07 08:26	06-11-07 08:26	00:00:00	TCP	5956	www.ansa.it
213.140.18.128	10358	194.244.5.206	80	06-11-07 09:26	06-11-07 09:39	00:12:37	TCP	9274	www.ansa.it

Estratti dalla cartella **Allegato 4**
files ***"Allegato 4 - 05 nov ore 23.xls"*** **e** ***"Allegato 4 - 06 nov ore 09 - fine.xls"***

L'analisi mostra sia la presenza di una grande quantità di traffico automatico e ricorsivo (si ricorda che il computer era sempre acceso e collegato alla rete internet attraverso l'operatore in questione), sia la presenza di traffico richiesto da un operatore (**interazione umana**); l'esame degli intervalli in cui sono effettuate le richieste verso gli IP rilevati dai tabulati ci ha permesso di differenziare il traffico automatico da quello non automatico.

In particolare il traffico verso l'IP 194.244.5.206, riportato nella tabella seguente, è relativo al dominio ansa.it. Quello presente ad intervalli *quasi* regolari di un'ora è identificabile come automatico, mentre la richiesta delle ore 13:16:32 e delle ore 23:18:57 (riga 1 e 8) del 5

Novembre 2007, nonchè e quella delle ore 08:26:27 e delle ore 9:26:42 del 06 Novembre (riga 9 e riga 18), devono intendersi come dovuto ad una richiesta specifica di un operatore e quindi identificarsi come **interazione umana**.

	IP Destinazione	Porta	Data Inizio	Data Fine	Durata	Tipo	Bytes
1.	194.244.5.206	80	05-11-2007 13:16:32	05-11-2007 13:16:32	0:00:00	TCP	10885
	194.244.5.206	80	05-11-2007 16:10:47	05-11-2007 16:19:28	0:08:41	TCP	17608
2.	194.244.5.206	80	05-11-2007 17:10:57	05-11-2007 17:10:57	0:00:00	TCP	17991
3.	194.244.5.206	80	05-11-2007 18:11:12	05-11-2007 18:11:12	0:00:00	TCP	19343
4.	194.244.5.206	80	05-11-2007 19:11:27	05-11-2007 19:11:27	0:00:00	TCP	20767
5.	194.244.5.206	80	05-11-2007 20:11:43	05-11-2007 20:11:43	0:00:00	TCP	22197
6.	194.244.5.206	80	05-11-2007 21:11:57	05-11-2007 21:11:58	0:00:01	TCP	23564
7.	194.244.5.206	80	05-11-2007 22:12:15	05-11-2007 22:12:15	0:00:00	TCP	25177
8.	194.244.5.206	80	05-11-2007 23:18:57	05-11-2007 23:18:57	0:00:00	TCP	25792
9.	194.244.5.206	80	06-11-2007 00:19:11	06-11-2007 00:19:11	0:00:00	TCP	1481
10.	194.244.5.206	80	06-11-2007 01:19:27	06-11-2007 01:32:29	0:13:02	TCP	2512
11.	194.244.5.206	80	06-11-2007 02:19:41	06-11-2007 02:19:41	0:00:00	TCP	1481
12.	194.244.5.206	80	06-11-2007 03:19:56	06-11-2007 03:24:04	0:04:08	TCP	1380
13.	194.244.5.206	80	06-11-2007 04:20:12	06-11-2007 04:24:49	0:04:37	TCP	1380
14.	194.244.5.206	80	06-11-2007 05:20:29	06-11-2007 05:24:44	0:04:15	TCP	1462
15.	194.244.5.206	80	06-11-2007 06:20:42	06-11-2007 06:24:58	0:04:16	TCP	1450
16.	194.244.5.206	80	06-11-2007 07:20:57	06-11-2007 07:20:57	0:00:00	TCP	1481
17.	194.244.5.206	80	06-11-2007 08:26:27	06-11-2007 08:26:27	0:00:00	TCP	5956
18.	194.244.5.206	80	06-11-2007 09:26:42	06-11-2007 09:39:19	0:12:37	TCP	9274

L'interazione umana con il computer delle ore 8.26 del giorno 06 novembre ha inoltre determinato uno spostamento in avanti della richiesta automatica di aggiornamento. E' importante segnalare altresì che il collegamento al sito dell'Ansa del giorno 06 novembre trova riscontro nella cache di Firefox (_CACHE_003_). La conclusione è che c'è stata **interazione umana** con il browser Firefox, accedendo solo ai siti presenti nella sua cronologia.

Oltre al traffico verso l'IP del sito dell'Ansa, è presente traffico verso altri domini tra cui Apple, Washingtonpost, Google e Mozilla.org; queste attività sono di tipo automatico.

Questo approfondimento ci permette infine di affermare con certezza che il traffico delle ore 00:50:58 del 02 Novembre 2007 verso l'indirizzo IP 17.112.152.32 riconducibile al dominio **apple.com** non può essere definito automatico, proprio perchè vi è assenza di altre connessioni verso il suo IP 17.112.152.32 sia nelle ore precedenti che in quelle seguenti, in un lasso temporale che supera le 12 ore.

In fede

Dott. Michele Gigli

In fede

Dott. Antonio d'Ambrosio