Web ブラウザの
SOCKS 実装状況について

ＮＴＴ コミュニケーションズ株式会社
経営企画部
マネージドセキュリティサービス推進室
セキュリティオペレーション担当

2013 年 03 月 11 日

Ver. 1.0

1. 調査概要 3
1.1. 調査概要 3
2. SOCKSとは 3
2.1. SOCKSとは 3
2.2. SOCKSv4 でのアドレス解決の必須性 4
2.3. SOCKSv4 以外での、ホスト名指定のサーバへの接続 4
2.4. SOCKSとIPv6 5
3. 各WEBブラウザのSOCKS実装の調査 5
3.1. 環境 5
3.2. 調査前の処理 5
3.3. MS-IE8.0.6001.18702 SP0 (MS-WinXP SP3 [Win32{patched 2013/02/28}])の場合 . 6
3.4. MS-IE9.0.8112.16421 更新バージョン 9.0.13(KB2792100) (MS-Win7 SP1 [Win32{patched 2013/02/28}])の場合 7
3.5. MS-IE10.0.9200.16521 更新バージョン RTM(KB2718695) (MS-Win7 SP1 [Win32{patched 2013/02/28}])の場合 8
3.6. Safari5.0.5(7533.21.1) (MS-Win7 SP1 [Win32{patched 2013/02/28}])の場合 9
3.7. Opera12.14 Build 1738 (MS-WinXP SP3 [Win32{patched 2013/02/28}])の場合 .. 10
3.8. Google-Chrome25.0.1364.97m (2013/02/28 時点) (MS-WinXP SP3 [Win32{patched 2013/02/28}])の場合 11
3.9. Firefox19.0 (MS-WinXP SP3 [Win32{patched 2013/02/28}])の場合 12
3.10. polipo 1.0.4.1 の場合 19
3.11. DropBox 1.6.17 for Win32 の場合 20
3.12. まとめ 22
4. 検証作業者 23
5. 履歴 23
6. 最新版の公開URL 23
7. 参考 23
8. 本レポートに関する問合せ先 24

1. 調査概要

1.1. 調査概要

SOCKS には、「version4」「version4a」「version5」の 3 タイプある。
Web ブラウザに搭載されている SOCKS プロキシ機能の実装状況について調査した結果を記述する。

2. SOCKSとは

2.1. SOCKSとは

SOCKS とは何か、という点については Wikipedia などを参照して欲しい。

大抵の Web ブラウザは、Proxy サーバの一つとして、SOCKS サーバを用いることができる。

SOCKS には「version4」「version4a」「version5」の 3 タイプ存在する。

基本的は、
1. SOCKS クライアントがメッセージを送る(接続要求や、認証要求など)。
2. SOCKS サーバが結果を返す。

というやり取りを SOCK クライアント(Web ブラウザ)と SOCKS サーバを通じて、SOCKS クライアントと SOCKS サーバ間で「接続」が確立される。

それぞれの SOCKS バージョンごとの SOCKS クライアントから SOCKS サーバへのリクエスト・メッセージのパケット形式は以下である。

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Ver (0x04)	Cmd (0x01)	PortNo		Forward IP Address				Username							
Username					0x00										

図 2.1-1 : SOCKSv4 の接続要求パケット

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Ver (0x04)	Cmd (0x01)	PortNo		Forward IP Address (0.0.0.X)				Username							
Username					0x00	Hostname									
Hostname								0x00							

図 2.1-2 : SOCKSv4a の接続要求パケット

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Ver (0x05)	AuthTypeCount	AuthType1	AuthType2	…											

図 2.1-3 : SOCKSv5 の Hello パケット

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Ver (0x05)	Cmd (0x01)	0x00	AddrType (0x01)	Forward IP Address				PortNo							

図 2.1-4 : SOCKSv5 の接続要求パケット(転送先が IPv4)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Ver (0x05)	Cmd (0x01)	0x00	AddrType (0x03)	Size	Hostname										
Hostname									PortNo						

図 2.1-5 : SOCKSv5 の接続要求パケット(転送先がホスト名で指定されるアドレス)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Ver (0x05)	Cmd (0x01)	0x00	AddrType (0x04)	Forward IPv6 Address											
Forward IP Address				PortNo											

図 2.1-6 : SOCKSv5 の接続要求パケット(転送先が IPv6)

2.2. SOCKSv4 でのアドレス解決の必須性

図 2.1-1のSOCKSv4 のパケットを見ると分かるが、SOCKSサーバに転送先の実際のサーバのアドレスを伝える手段は、IPv4 アドレスしかないことが分かる。
つまり、ホスト名で指定されるサーバへ SOCKS 経由で接続する際、SOCKSv4 では SOCKS クライアント側で、一度名前解決を行った上で、ホスト名を IP アドレスに変換した上で、SOCKS サーバへ接続要求を出す必要がある。

2.3. SOCKSv4 以外での、ホスト名指定のサーバへの接続

SOCKSv4 以外の場合はどうであろうか。図 2.1-2はSOCKSv4a、図 2.1-4～図 2.1-6は SOCKSv5 のパケット構造であるが、ホスト名の場合も考慮されていることが分かる。

つまり、ホスト名で指定されるサーバへ SOCKS 経由で接続する際、SOCKSv4 以外 (SOCKSv4a と SOCKSv5)は、ホスト名を用いて、SOCKS サーバへ接続要求を出すことができる。そして、ホスト名から IP アドレスへの名前解決を SOCKS サーバが行うことになる。

SOCKSv4a の場合、転送先 IP アドレスを「0.0.0.X」(X は非 0)とすることで、パケット後半部分をホスト名として SOCKS サーバへ渡すことができる。

SOCKSv5 の場合、パケットの先頭から 4 バイト目を「0x03」とすることで、一バイトの長さ情報に続いて、ホスト名を続けることができる。

当然であるが、SOCKS クライアントが SOCKS 通信をする前に名前解決を行い、転送先サーバのアドレスを IP アドレスとして SOCKS サーバへ通知することも可能ではある。

2.4. SOCKSとIPv6

図 2.1-6から、SOCKSv5 はIPv6 に対応しているようだ。

3. 各Webブラウザの SOCKS実装の調査

3.1. 環境

SOCKS サーバとして、Tor(9050/tcp)を使い、Web ブラウザと Tor 間の通信をパケットキャプチャし、Web ブラウザの SOCKS 実装の状況を確認してみる。
通常はローカルホスト上の Tor クライアント(SOCKS サーバ)を使うと思うが、今回は(待ち受けアドレスを「127.0.0.1」から「0.0.0.0」へ変更することで)ネットワーク上の Tor クライアント(SOCKS サーバ)と Web ブラウザを通信させることで、パケットキャプチャを行えるようにした。

また、Web サーバとして、「www.ntt.com」を使用した。

3.2. 調査前の処理

実際に調査を行う前に事前に転送先ホスト「www.ntt.com」のアドレスを調べておく。調査当日は、「www.ntt.com=210.163.219.224=(0xD2, 0xA3, 0xDB, 0xE0)」であることを確認した。

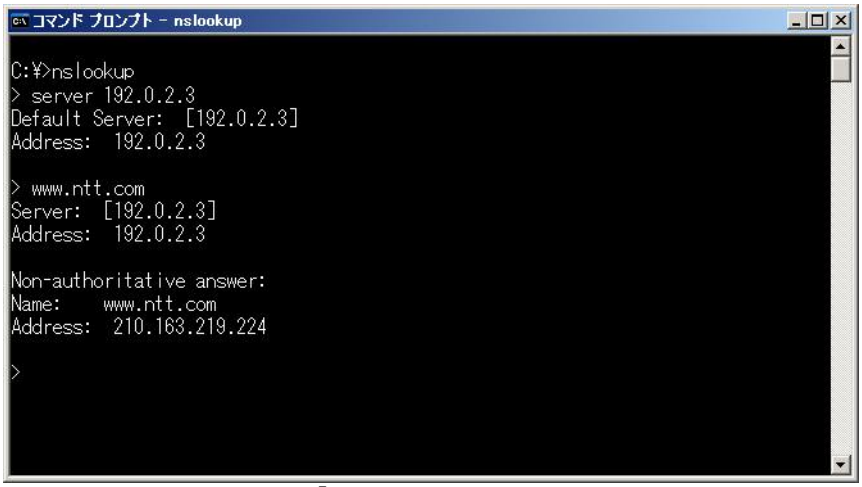

図 3.2-1 : 「www.ntt.com=210.163.219.224」

3.3. MS-IE8.0.6001.18702 SP0 (MS-WinXP SP3 [Win32{patched 2013/02/28}])の場合

IE8 の場合、SOCKS4 で接続しているため、DNS パケットが流出しているのが、確認できる。
また、Windows ログインユーザ名を SOCKS のユーザ名として利用していることも確認できる。

図 3.3-1 : プロキシ設定画面

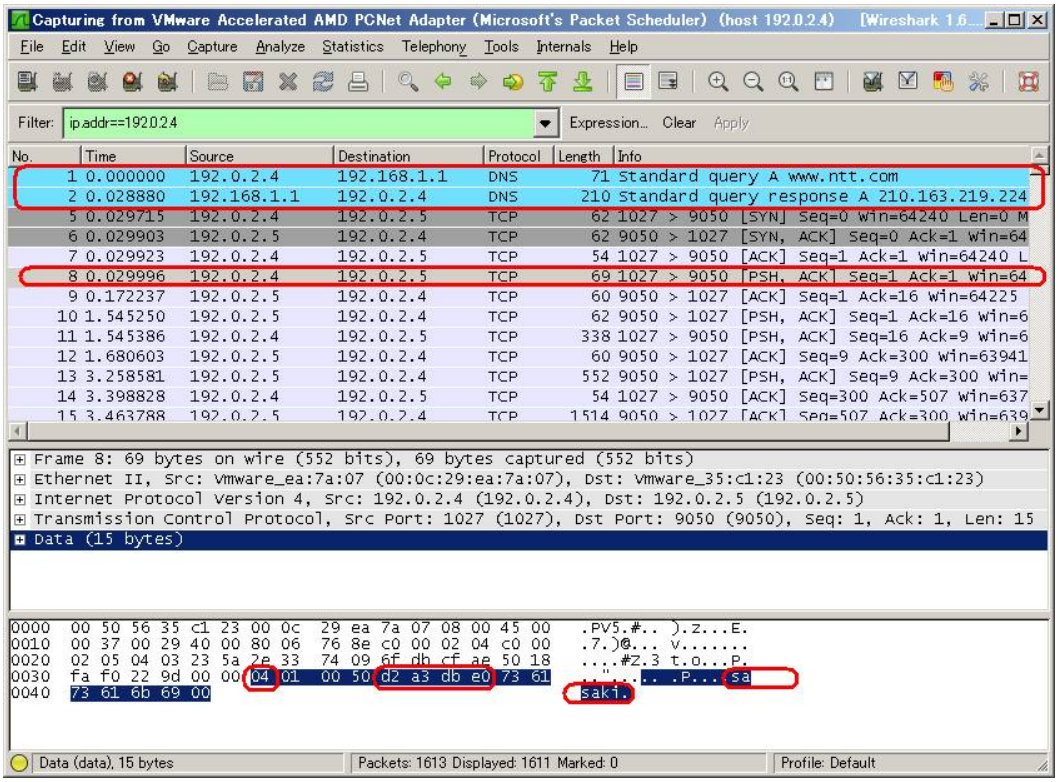

図 3.3-2 : 図 3.3-1の設定で、SOCKSサーバ(192.0.2.5:9050)へ接続した結果

SOCKS接続前にDNSで名前解決を行い、IPアドレスをSOCKSの

接続要求パケットに埋め込んでいるのが確認できる

また、Windowsログインユーザ名も確認できる

3.4. MS-IE9.0.8112.16421 更新バージョン 9.0.13(KB2792100) (MS-Win7 SP1 [Win32{patched 2013/02/28}])の場合

IE9 の場合、SOCKS4 で接続しているため、DNS パケットが流出しているのが、確認できる。
また、Windows ログインユーザ名を SOCKS のユーザ名として利用していることも確認できる。

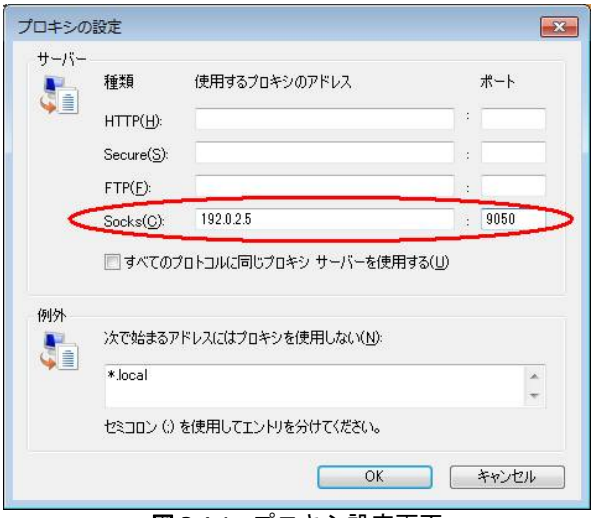

図 3.4-1 : プロキシ設定画面

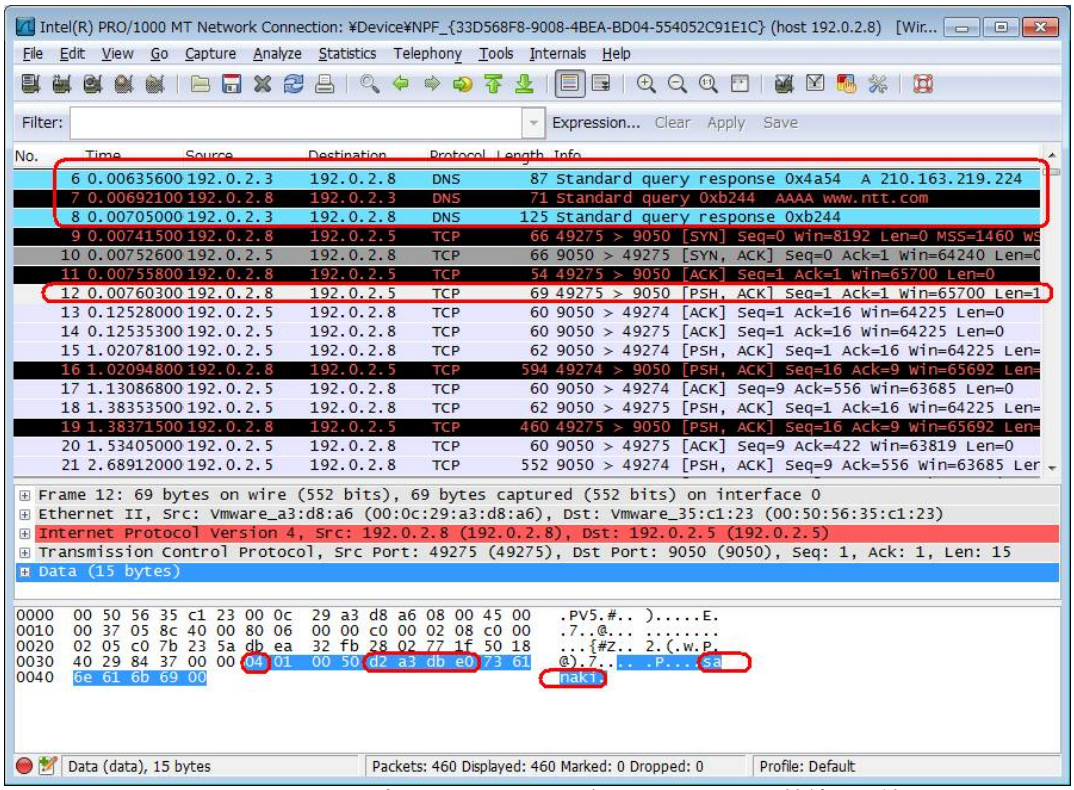

図 3.4-2 : 図 3.4-1の設定で、SOCKSサーバ(192.0.2.5:9050)へ接続した結果

SOCKS接続前にDNSで名前解決を行い、IPアドレスをSOCKSの

接続要求パケットに埋め込んでいるのが確認できる

また、Windowsログインユーザ名も確認できる

3.5. MS-IE10.0.9200.16521 更新バージョン RTM(KB2718695) (MS-Win7 SP1 [Win32{patched 2013/02/28}])の場合

IE10 の場合、SOCKS4 で接続しているため、DNS パケットが流出しているのが、確認できる。
また、Windows ログインユーザ名を SOCKS のユーザ名として利用していることも確認できる。

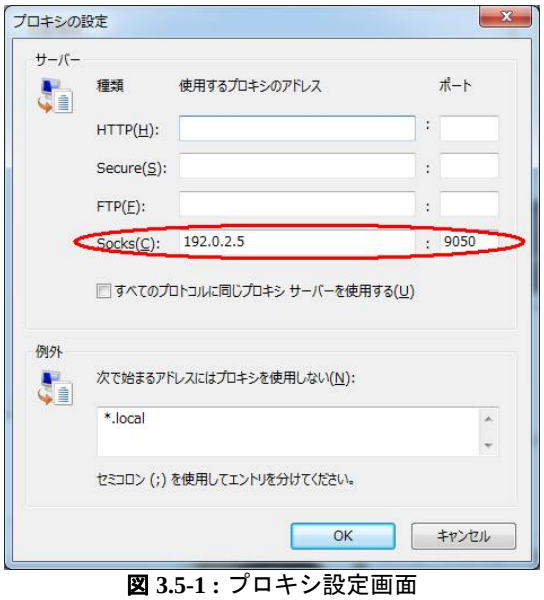

図 3.5-1 : プロキシ設定画面

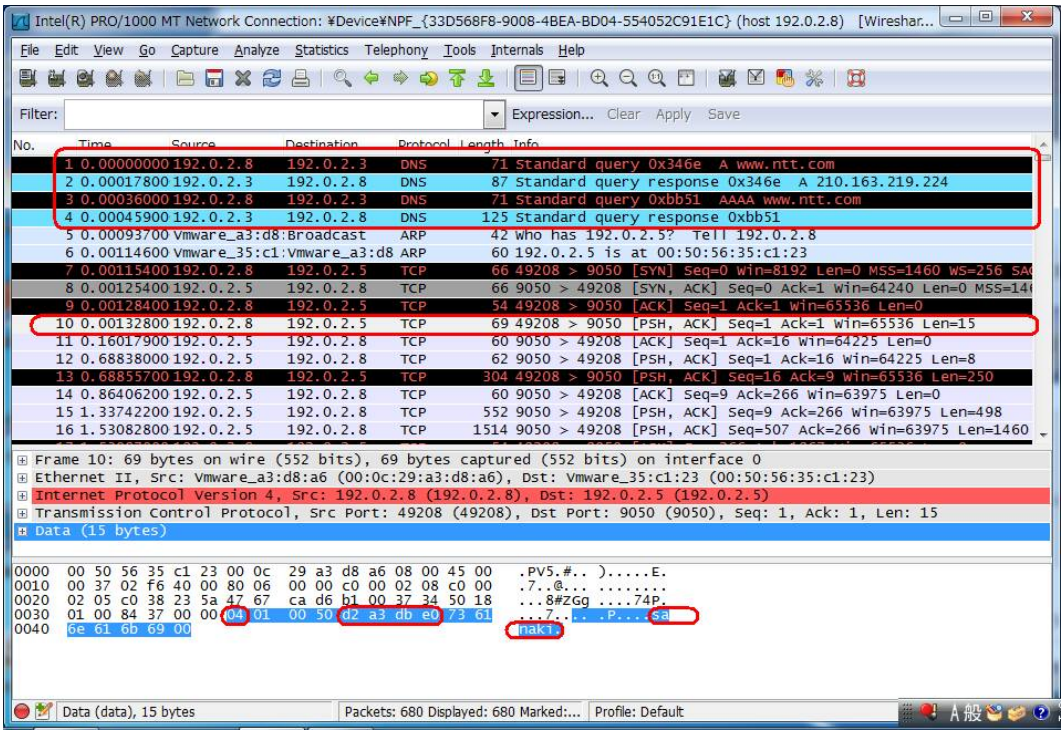

図 3.5-2 : 図 3.5-1の設定で、SOCKSサーバ(192.0.2.5:9050)へ接続した結果

SOCKS接続前にDNSで名前解決を行い、IPアドレスをSOCKSの

接続要求パケットに埋め込んでいるのが確認できる

また、Windowsログインユーザ名も確認できる

3.6. Safari5.0.5(7533.21.1) (MS-Win7 SP1 [Win32{patched 2013/02/28}])の場合

Safari のプロキシ設定は、OS 標準設定を用いる。
Safari の場合、SOCKS5 で接続している。また、ホスト名の名前解決は SOCKS サーバ側に依頼している状況が確認できる。

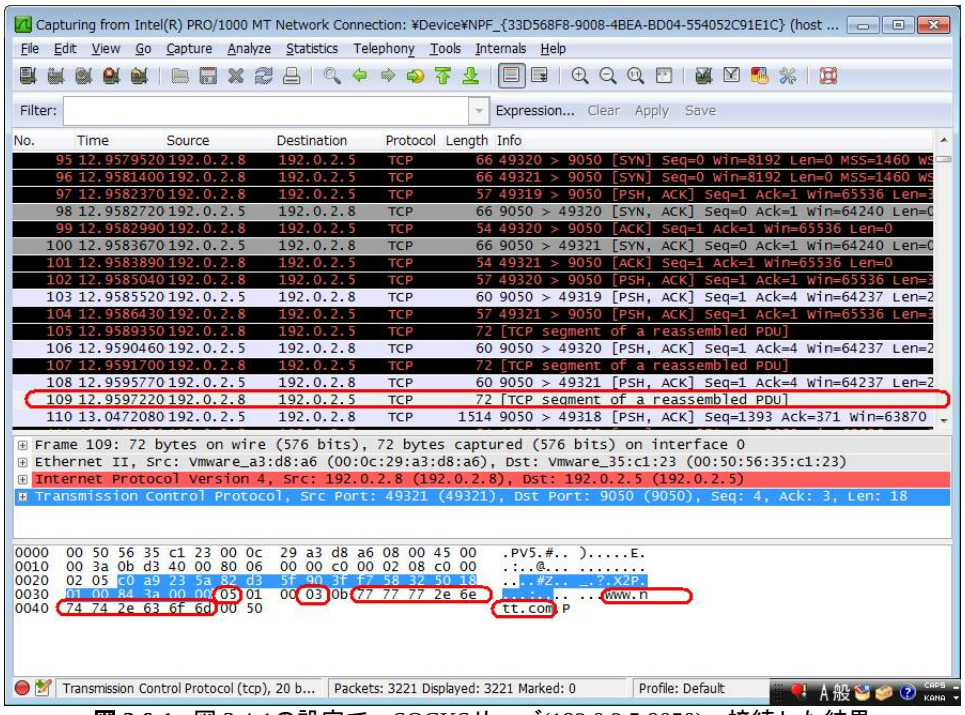

図 3.6-1 : 図 3.4-1の設定で、SOCKSサーバ(192.0.2.5:9050)へ接続した結果

SOCKS5 で接続し、ホスト名の名前解決は行わずSOCKSサーバへ依頼していることが確認できる

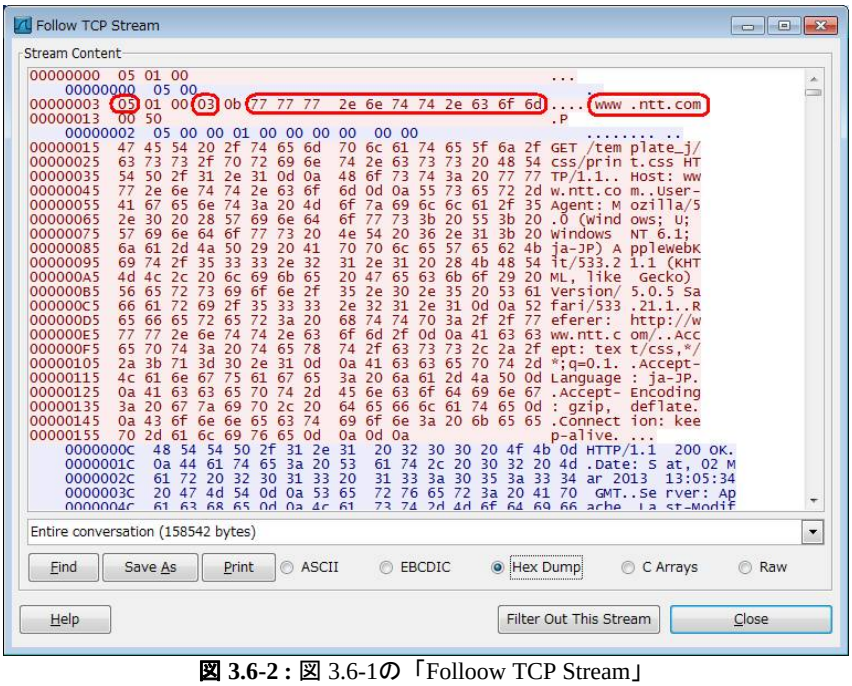

図 3.6-2 : 図 3.6-1の「Folloow TCP Stream」

3.7. Opera12.14 Build 1738 (MS-WinXP SP3 [Win32{patched 2013/02/28}])の場合

Opera は、SOKCS5 を用いているが、わざわざ自らホスト名の名前解決を行い、IP アドレスを SOCKS5 の接続要求パケットに埋め込んでいることが確認できる。

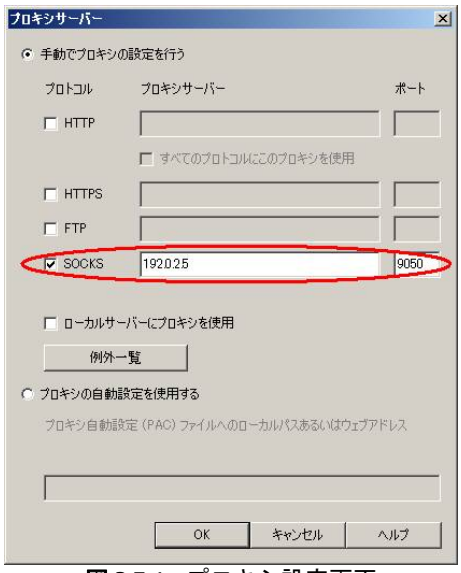

図 3.7-1：プロキシ設定画面

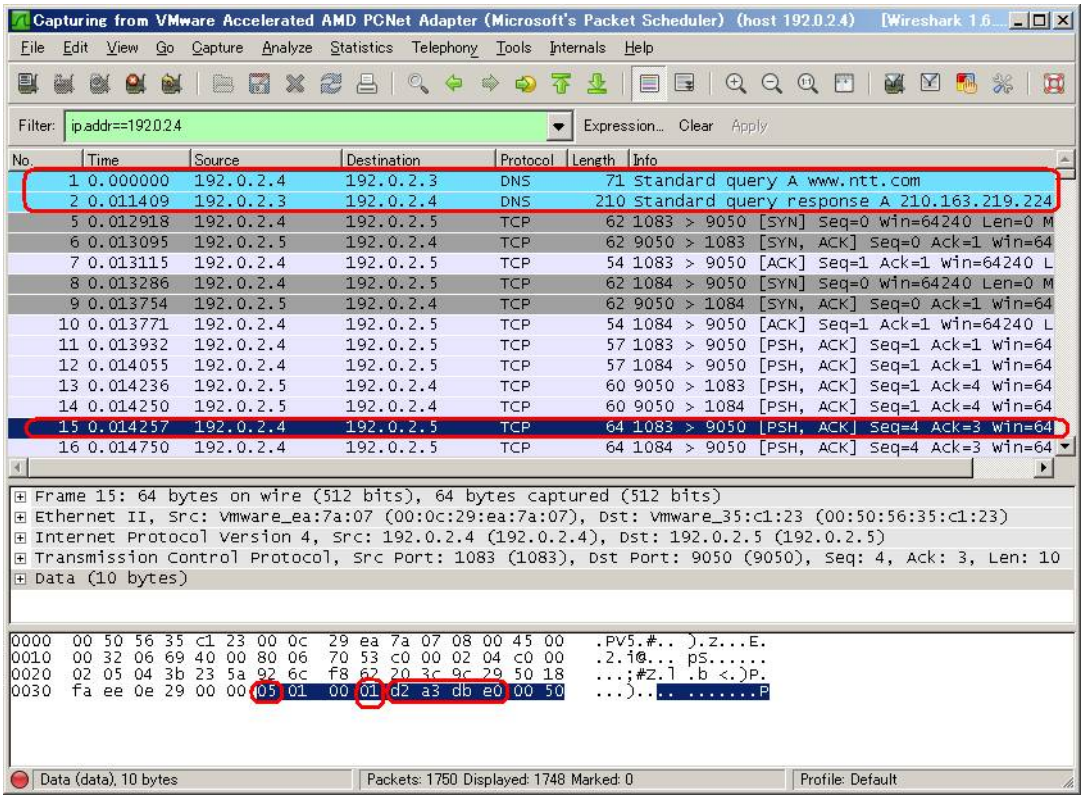

図 3.7-2：図 3.7-1の設定で、SOCKSサーバ(192.0.2.5:9050)へ接続した結果

SOCKS接続前にDNSで名前解決を行い、IPアドレスをSOCKSの

接続要求パケットに埋め込んでいるのが確認できる

3.8. Google-Chrome25.0.1364.97m (2013/02/28 時点) (MS-WinXP SP3 [Win32{patched 2013/02/28}])の場合

Google-Chrome のプロキシ設定は、OS 標準設定を用いる。
Google-Chrome は SOCKS4 で接続しているため、DNS パケットが流出しているのが、確認できる。

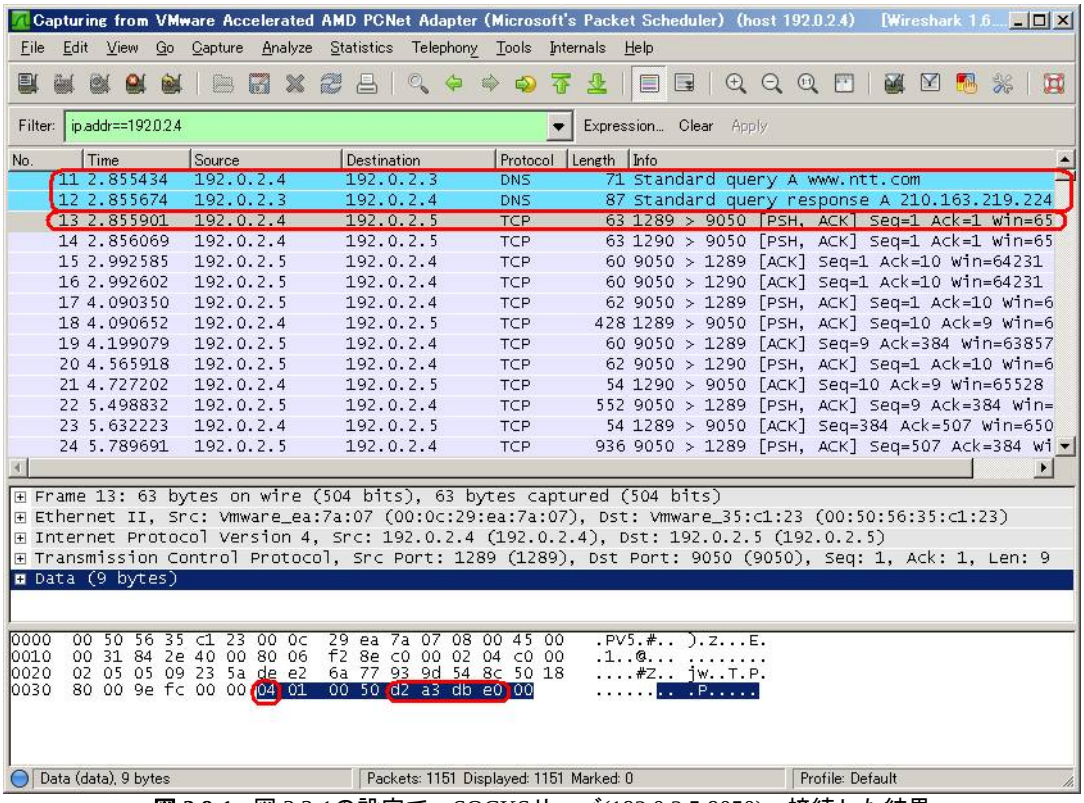

図 3.8-1 : 図 3.3-1の設定で、SOCKSサーバ(192.0.2.5:9050)へ接続した結果

SOCKS接続前にDNSで名前解決を行い、IPアドレスをSOCKSの

接続要求パケットに埋め込んでいるのが確認できる

3.9. Firefox19.0 (MS-WinXP SP3 [Win32{patched 2013/02/28}])の場合

Firefoxには、SOCKSのプロトコルバージョンを選択できるようになっている。既定では、「ver5」が選択されている。既定の状態では、SOKCS5 を用いているが、わざわざ自らホスト名の名前解決を行い、IPアドレスをSOCKS5 の接続要求パケットに埋め込んでいることが確認できる(図 3.9-1～図 3.9-2)。
また、「ver4」を選択しても同様に、わざわざ自らホスト名の名前解決を行い、IPアドレスをSOCKS4 の接続要求パケットに埋め込んでいることを確認した(図 3.9-3～図 3.9-4)。
さらに、詳細設定を行う「about:config」にて「network.proxy.socks_remote_dns=true」という設定を行った場合の挙動も確認した(図 3.9-5)。
この設定によって、自ら名前解決することなく、SOCKSサーバ側に名前解決は依頼するようになったことが確認できる(SOCKS5 = 図 3.9-6～図 3.9-8) (SOCKS4a = 図 3.9-9～図 3.9-10)。

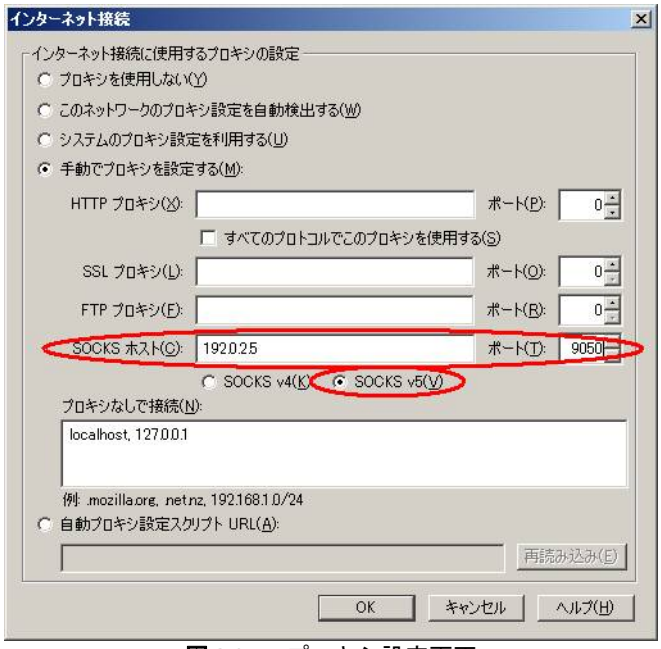

図 3.9-1：プロキシ設定画面

既定では「SOCKS5」が選択されている

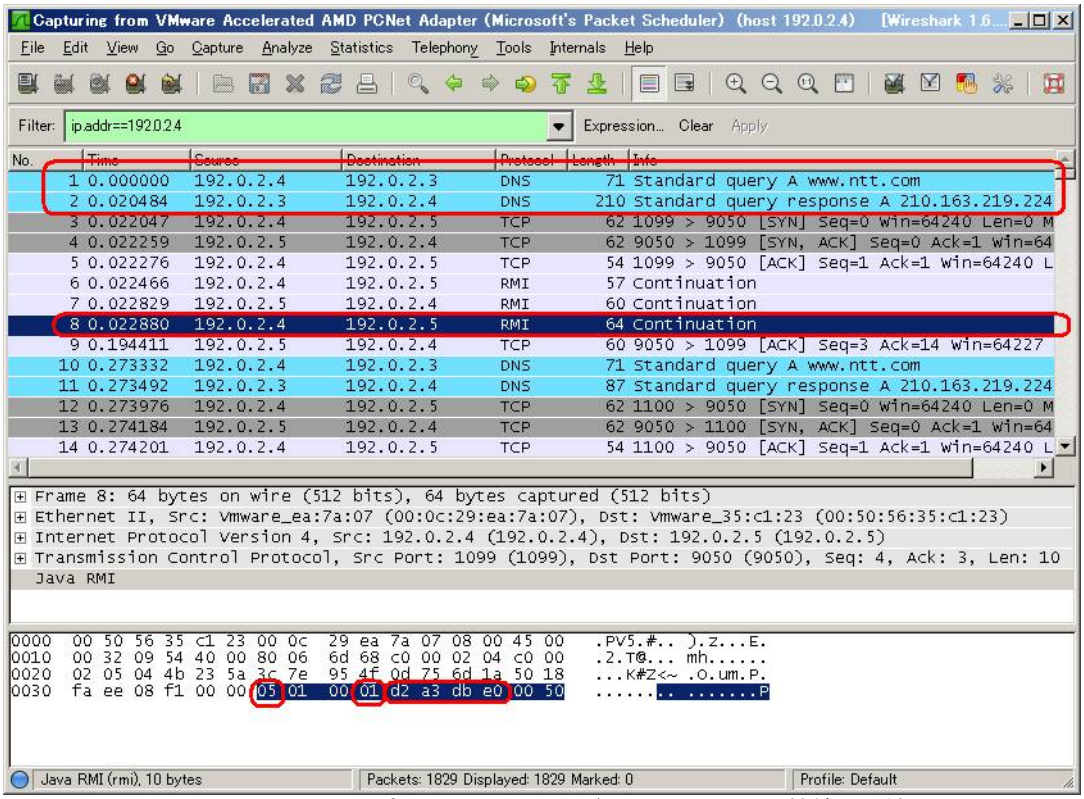

図 3.9-2：図 3.9-1の設定で、SOCKSサーバ(192.0.2.5:9050)へ接続した結果

SOCKS接続前にDNSで名前解決を行い、IPアドレスをSOCKSの

接続要求パケットに埋め込んでいるのが確認できる

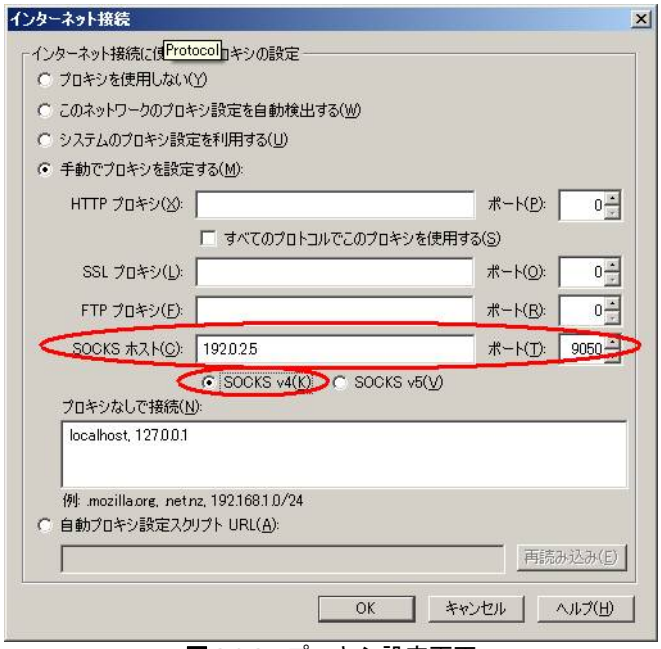

図 3.9-3 : プロキシ設定画面

「SOCKS4」を選択した

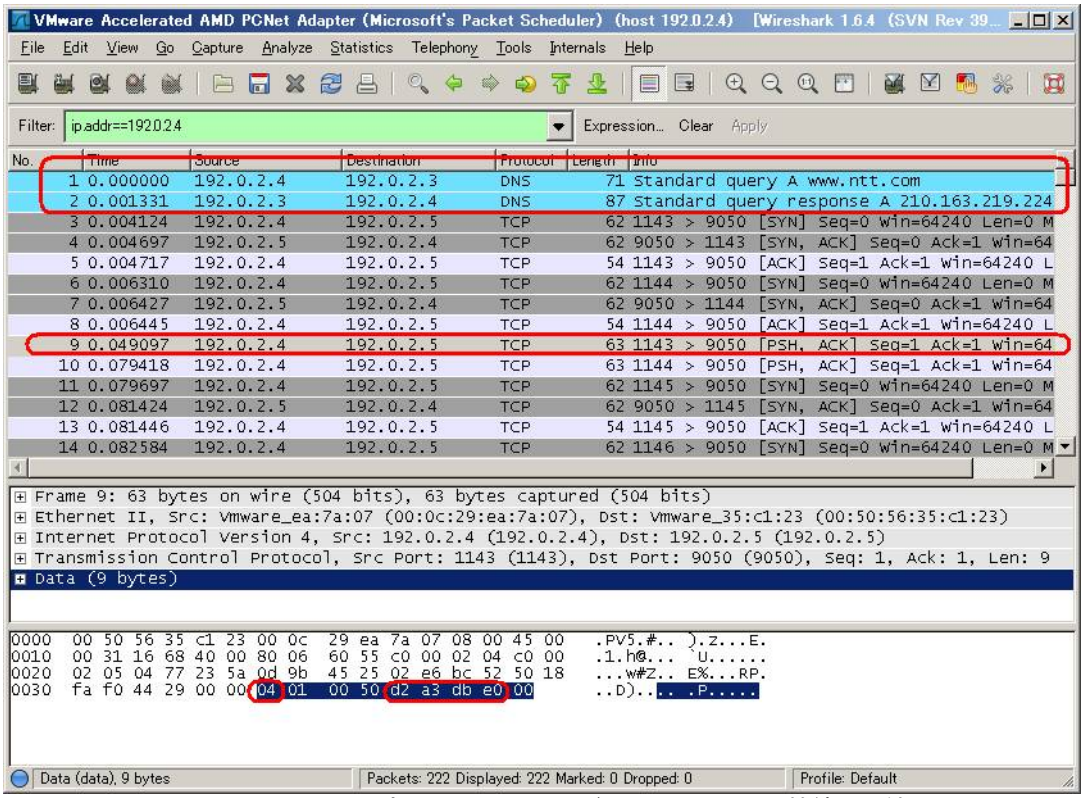

図 3.9-4 : 図 3.9-3の設定で、SOCKSサーバ(192.0.2.5:9050)へ接続した結果

SOCKS接続前にDNSで名前解決を行い、IPアドレスをSOCKSの

接続要求パケットに埋め込んでいるのが確認できる

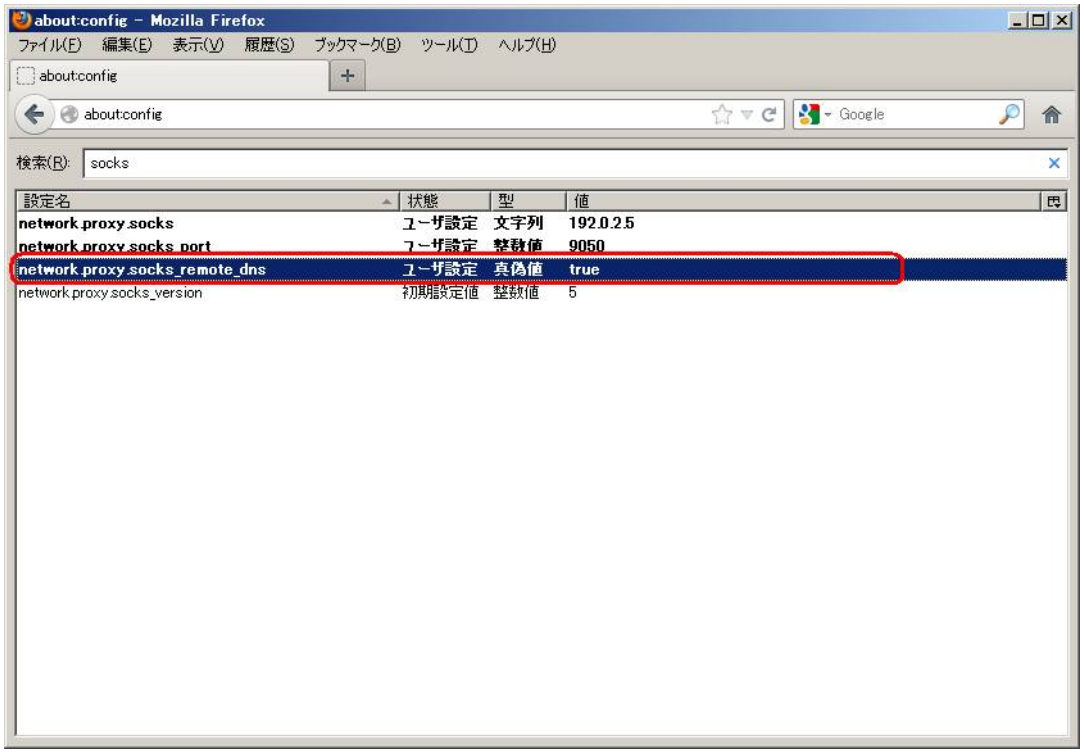

図 3.9-5 : 詳細設定「about:config」にて

「network.proxy.socks_remote_dns=true」の設定を行う

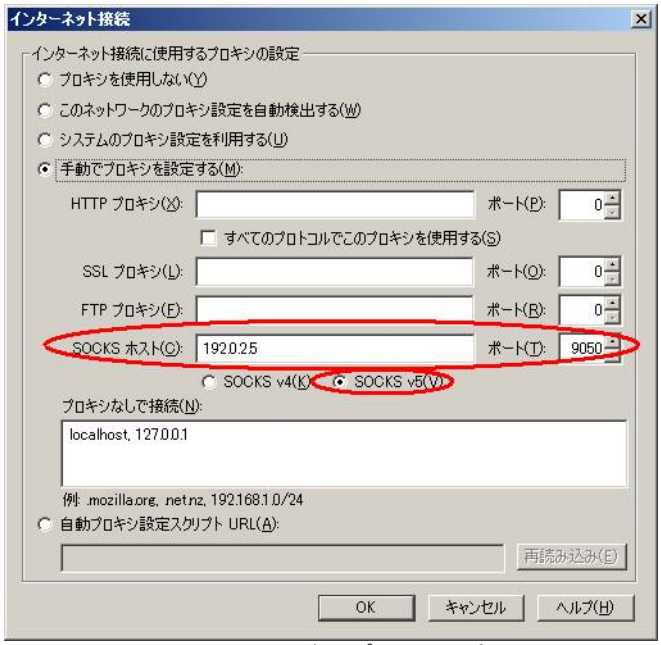

図 3.9-6 : 図 3.9-5後のプロキシ設定画面

既定では「SOCKS5」が選択されている

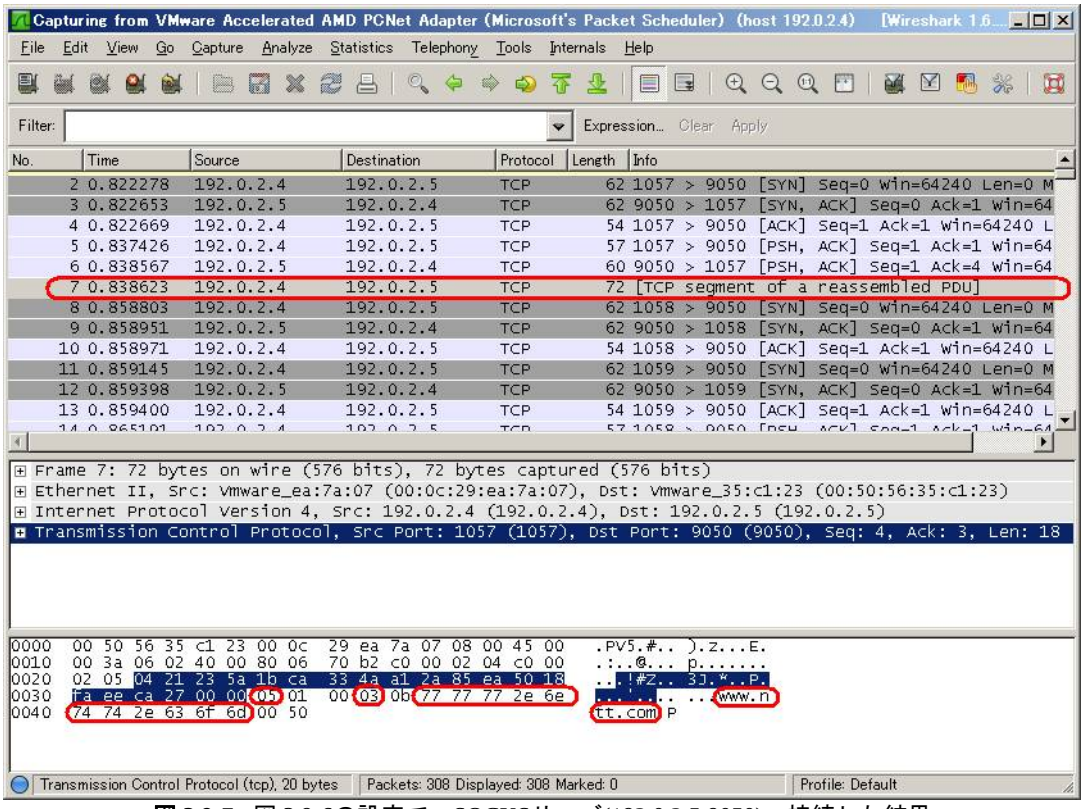

図 3.9-7 : 図 3.9-6の設定で、SOCKSサーバ(192.0.2.5:9050)へ接続した結果

SOCKS5 で接続し、ホスト名の名前解決は行わずSOCKSサーバへ依頼していることが確認できる

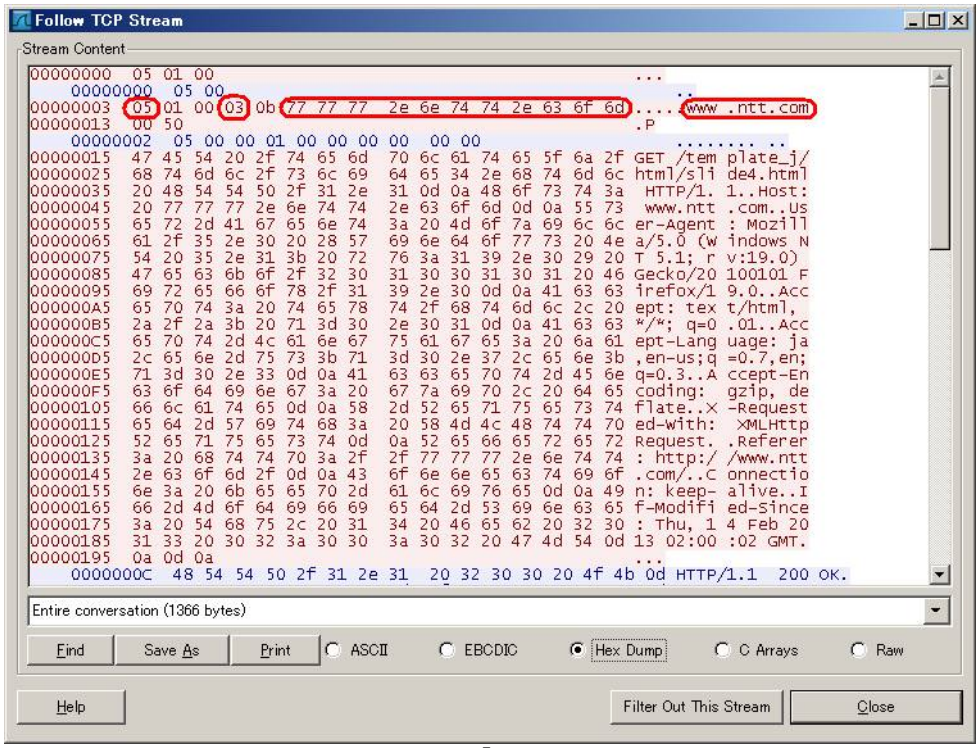

図 3.9-8 : 図 3.9-7の「Follow TCP STream」

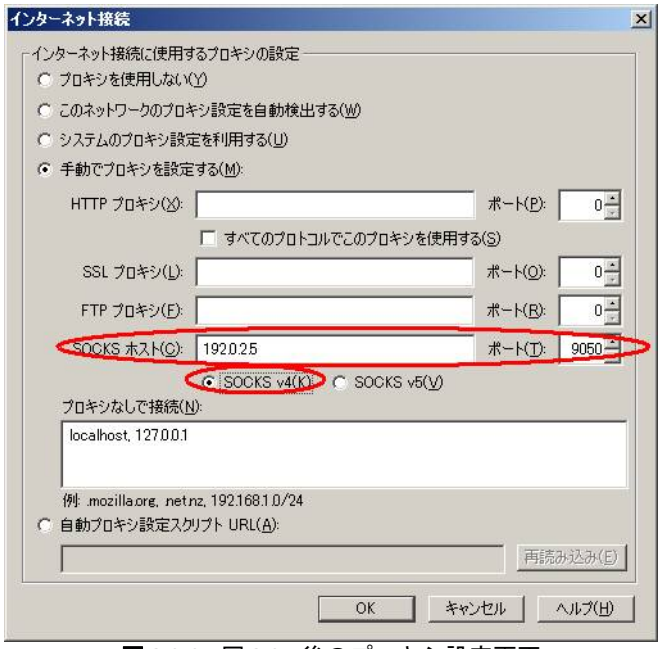

図 3.9-9 : 図 3.9-5後のプロキシ設定画面

「SOCKS4」を選択した

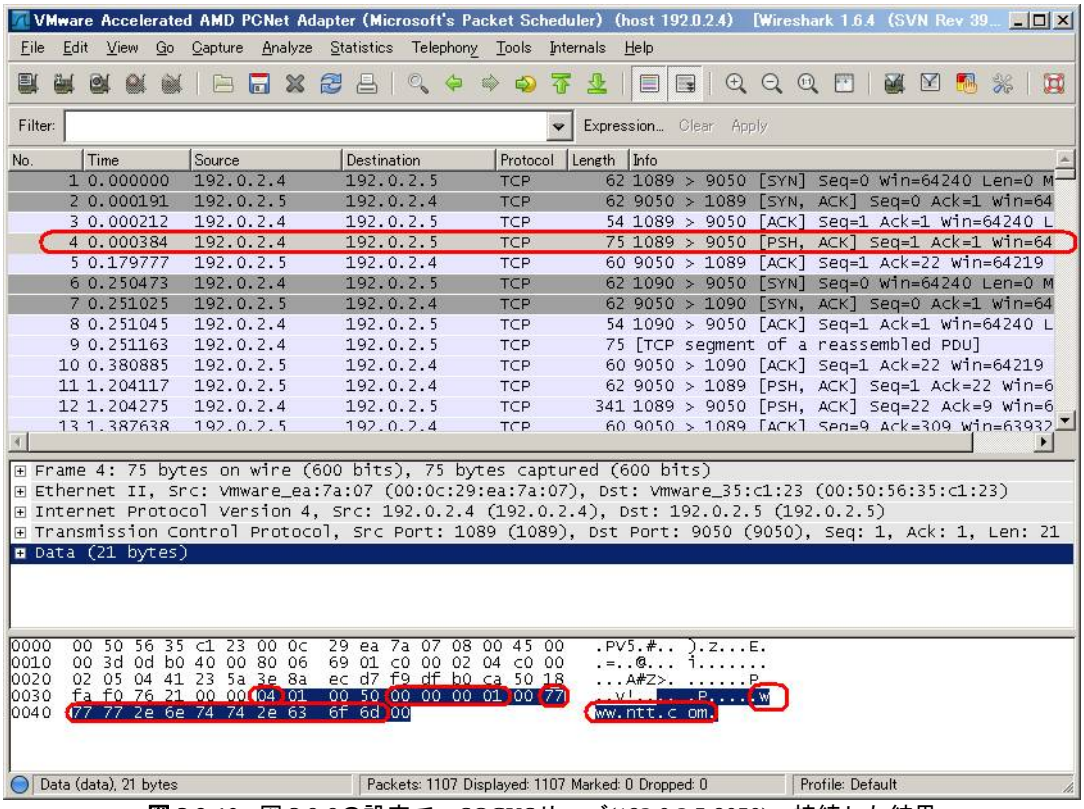

図 3.9-10 : 図 3.9-9の設定で、SOCKSサーバ(192.0.2.5:9050)へ接続した結果

SOCKS4aで接続し、ホスト名の名前解決は行わずSOCKSサーバへ依頼していることが確認できる

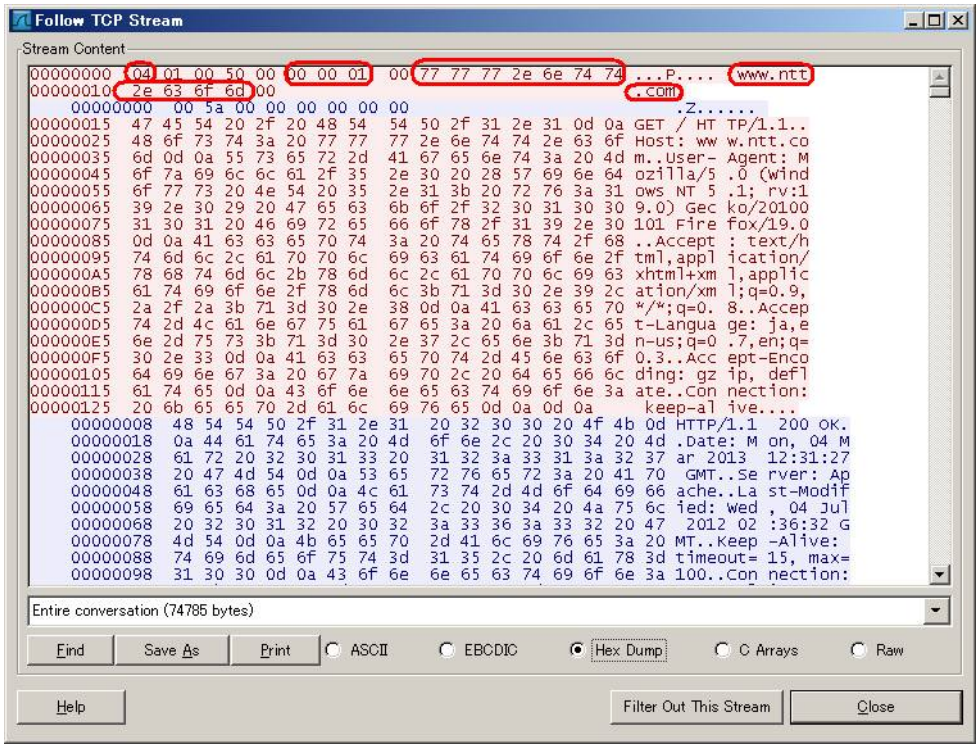

図 3.9-11 : 図 3.9-10の「Follow TCP STream」

3.10. polipo 1.0.4.1 の場合

TorProject から配布されている Vidalia には、polipo というローカル・HTTP・プロキシ・サーバが同梱されていた(以前は、Provoxy であった)。これを中継させた場合も調査した。
結果として、設定ファイル(polipo.conf)に socks5 と記述することで、名前解決を SOCKS サーバに依頼していることを確認した。

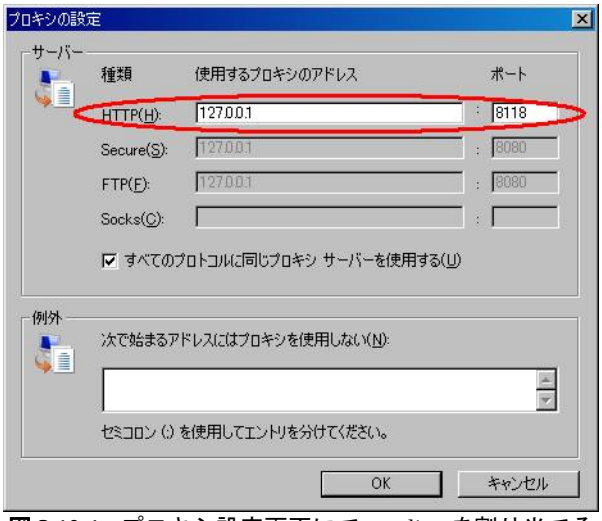

図 3.10-1 : プロキシ設定画面にて、polipo を割り当てる

(polipo は HTTP Proxy で 8118/tcp である)

polipo は SOCKS5 で SOCKS サーバへ接続するように pilopo.conf で設定した

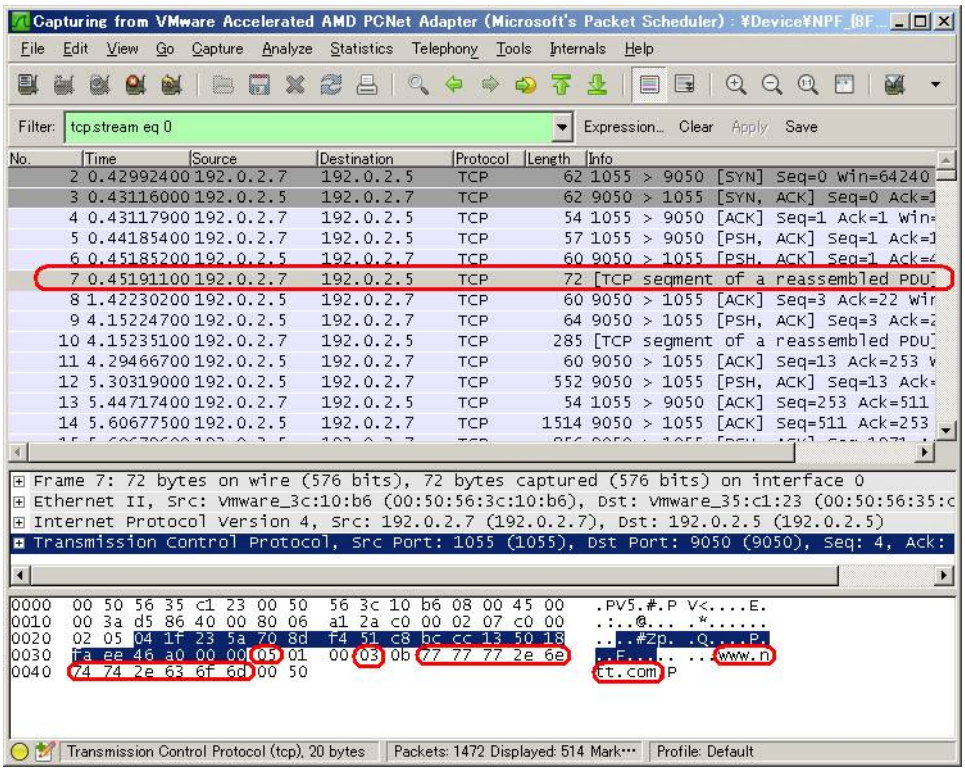

図 3.10-2 : 図 3.10-1の設定で、polipo→SOCKSサーバ(192.0.2.5:9050)へ接続した結果

SOCKS5 で接続し、ホスト名の名前解決は行わずSOCKSサーバへ依頼していることが確認できる

3.11. DropBox 1.6.17 for Win32 の場合

DropBox クライアントについても調査した。
結果として、名前解決を SOCKS サーバに依頼していることを確認した。

図 3.11-1 : プロキシ設定画面

既定では「SOCKS4」を選択した

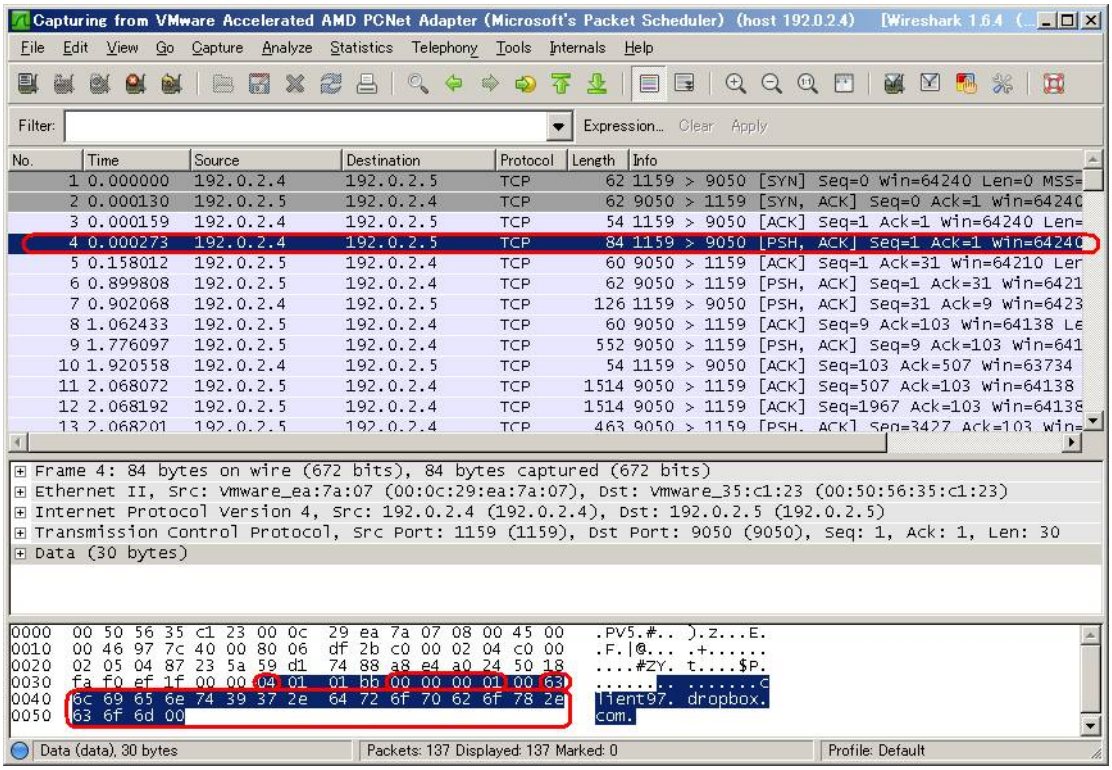

図 3.11-2 : 図 3.11-1の設定で、SOCKSサーバ(192.0.2.5:9050)へ接続した結果

SOCKS4aで接続し、ホスト名の名前解決は行わずSOCKSサーバへ依頼していることが確認できる

図 3.11-3 : プロキシ設定画面

「SOCKS5」を選択した

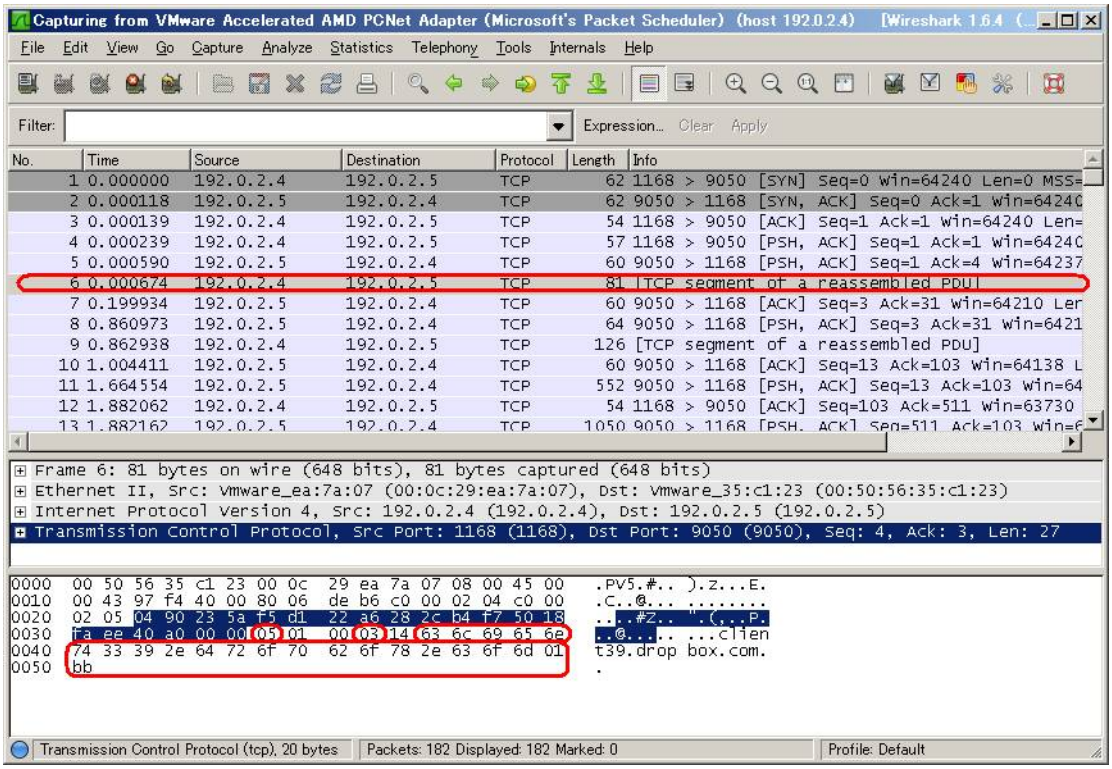

図 3.11-4 : 図 3.11-3の設定で、SOCKSサーバ(192.0.2.5:9050)へ接続した結果

SOCKS5 で接続し、ホスト名の名前解決は行わずSOCKSサーバへ依頼していることが確認できる

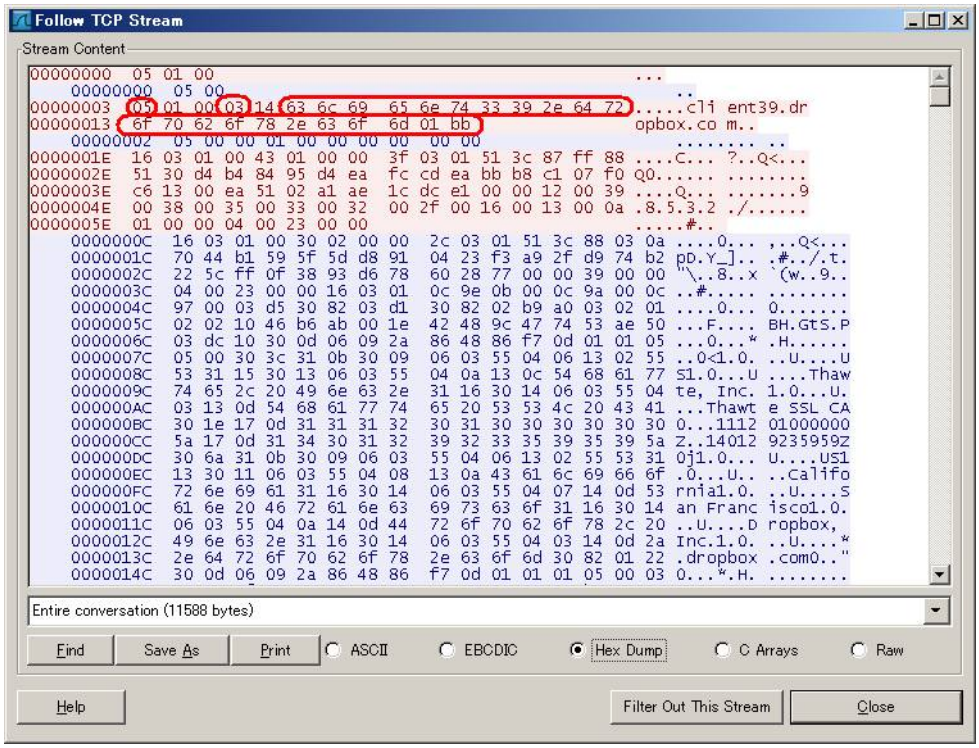

図 3.11-5 : 図 3.11-4の「Follow TCP STream」

3.12. まとめ

以上の結果をまとめると以下のようになる。

Web ブラウザ名	状況	DNS Leakage	備考
MS-IE8	SOCKSv4	○	ログインユーザの SOCKS サーバへの提示
MS-IE9	SOCKSv4	○	ログインユーザの SOCKS サーバへの提示
MS-IE10	SOCKSv4	○	ログインユーザの SOCKS サーバへの提示
Safari5.0.5	SOCKSv5	×	
Opera12.14	SOCKSv5(DNS)	○	
Google-Chrome 25.0.1364.97m	SOCKSv4	○	
Firefox19.0 (socks5)	SOCKSv5(DNS)	○	
Firefox19.0 (socks4)	SOCKSv4	○	
Firefox19.0 (socks5)	SOCKSv5	×	socks_remote_dns=true
Firefox19.0 (socks4)	SOCKSv4a	×	socks_remote_dns=true
polipo1.0.4.1	SOCKSv5	×	(参考)
DropBox1.6.17(socks4)	SOCKSv4a	×	(参考)
DropBox1.6.17(socks5)	SOCKSv5	×	(参考)

(※)SOCKSv5(DNS)：SOCKSv5 でありながら、自ら名前解決を行うタイプ

4. 検証作業者

NTT コミュニケーションズ株式会社
経営企画部マネージドセキュリティサービス推進室
セキュリティオペレーション担当
　佐名木 智貴

5. 履歴

- 2013 年 03 月 11 日 ：ver1.0 最初の公開

6. 最新版の公開URL

http://www.ntt.com/icto/security/data/soc.html

7. 参考

- SOCKS
  http://ja.wikipedia.org/wiki/SOCKS
- SOCKS: A protocol for TCP proxy across firewalls
  http://ftp.icm.edu.pl/packages/socks/socks4/SOCKS4.protocol
- RFC1928
  http://tools.ietf.org/html/rfc1928
- RFC1929
  http://tools.ietf.org/html/rfc1929
- RFC1961
  http://tools.ietf.org/html/rfc1961
- Tor Project
  https://www.torproject.org/

8. 本レポートに関する問合せ先

NTT コミュニケーションズ株式会社
経営企画部
マネージドセキュリティサービス推進室
セキュリティオペレーション担当

e-mail: scan@ntt.com

以 上