Wireshark 入門

インストールと
パケットキャプチャの開始

hebikuzure

推奨図書

- 実践 パケット解析――Wiresharkを使ったトラブルシューティング
  - http://www.oreilly.co.jp/books/9784873113517/
  - ISBN978-4-87311-351-7

- これをネタに話をしようと思っていたのですが.....

インストール

- 公式サイトからダウンロードしてインストールしましょう
- http://www.wireshark.org/

注意事項

- 最新バージョンを利用しましょう
  - セキュリティ修正が含まれます
  - 古いバージョンは攻撃対象になります
- Windows 環境では同梱の WinPcap を利用しましょう

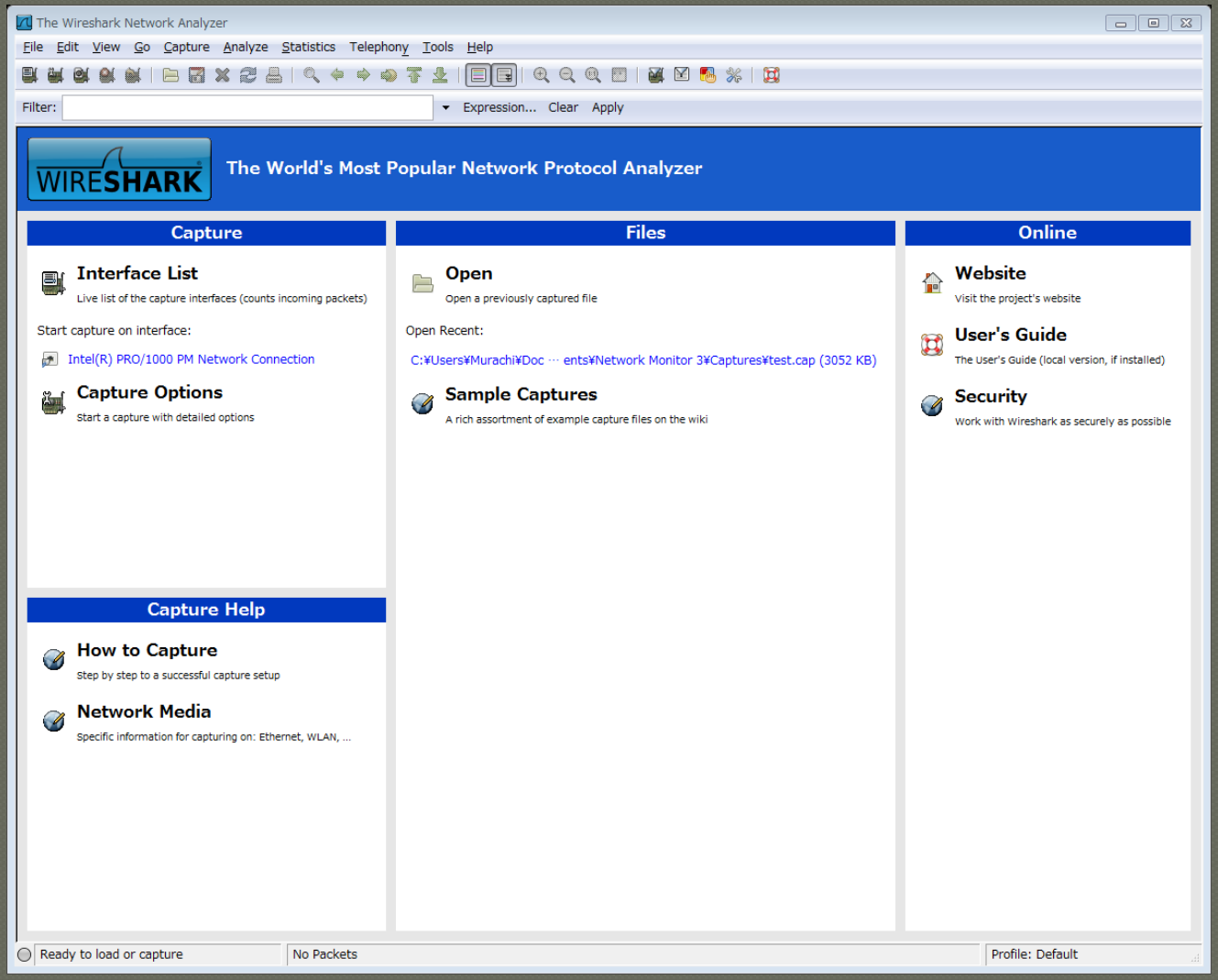
WinPcap の注意事項

- WinPcap 4.1 以降のバージョンでは NPF サービスが自動起動に設定されます
  - [管理者として実行] しなくてもパケット キャプチャができます
  - 自動起動で問題がある場合は、以下のレジストリ キーで設定が変更できます
    HKLM¥SYSTEM¥CurrentControlSet¥services¥NPF¥Start
    - 0x1 : SERVICE_SYSTEM_START
    - 0x2 : SERVICE_AUTO_START
    - 0x3 : SERVICE_DEMAND_START

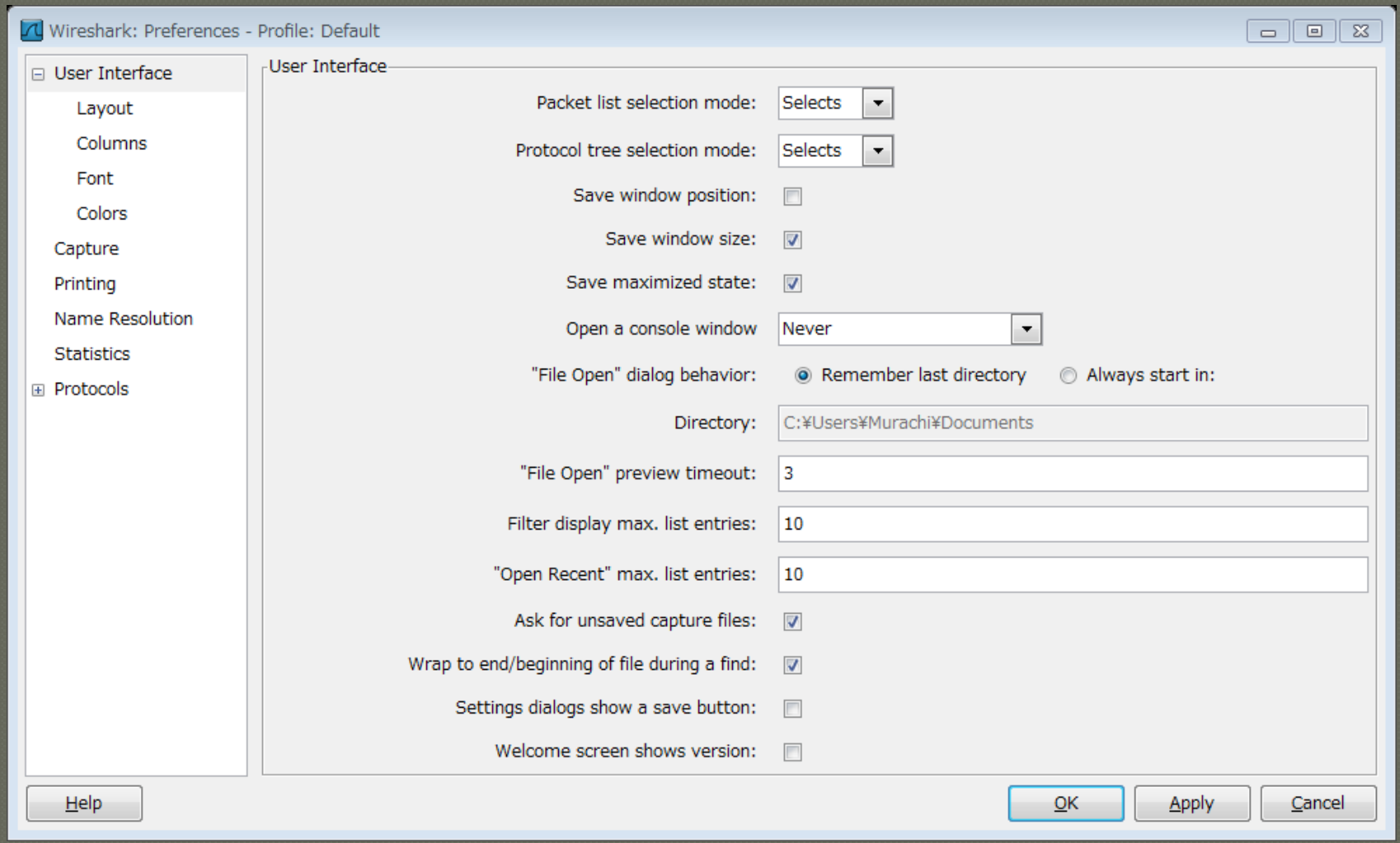
参考情報

- **How To Set Up a Capture**
  http://wiki.wireshark.org/CaptureSetup
- **Security**
  http://wiki.wireshark.org/Security
- **Platform-Specific information about capture privileges**
  http://wiki.wireshark.org/CaptureSetup/CapturePrivileges

Wireshark の起動



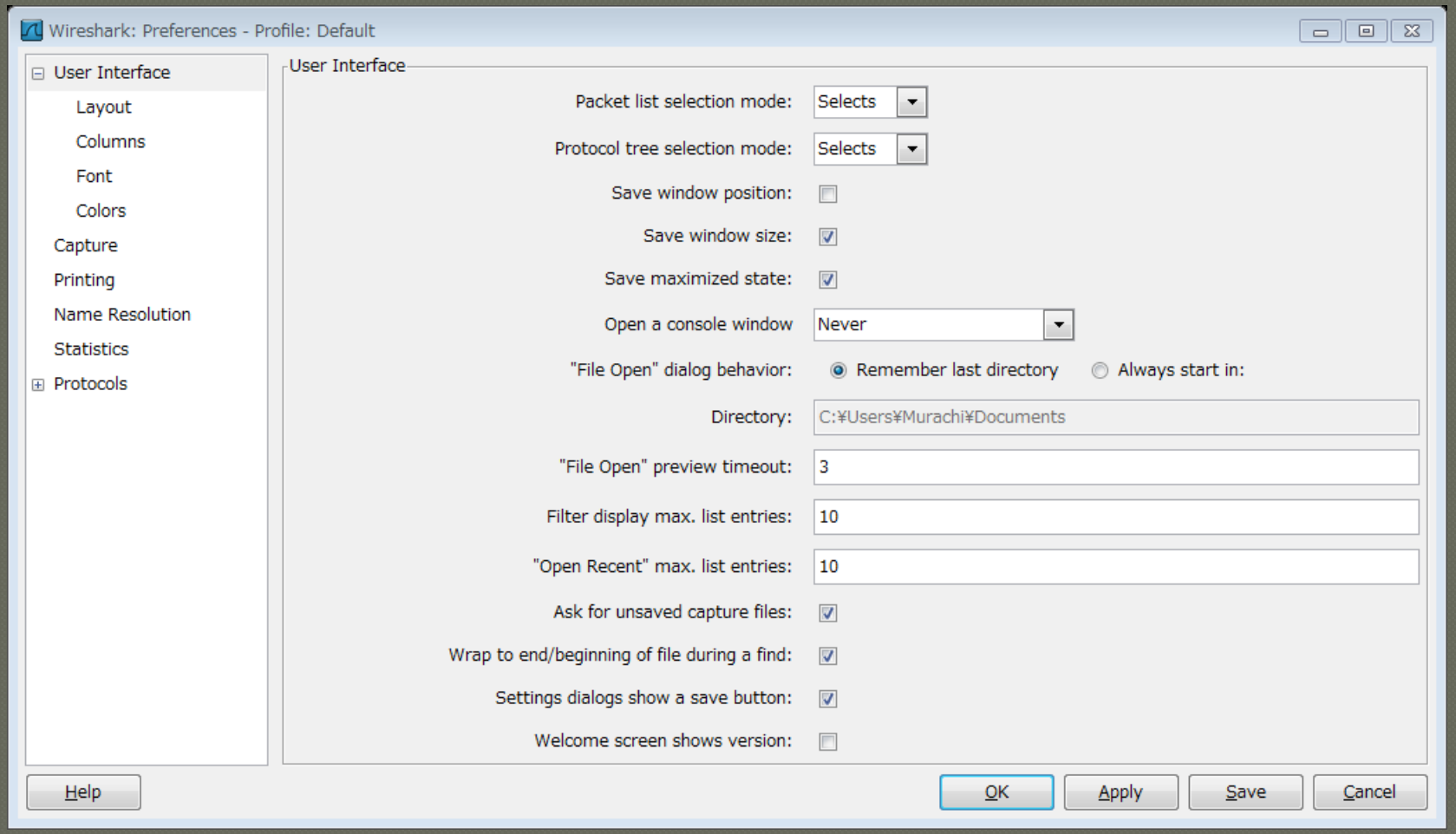
最初の設定


Wireshark: Preferences - Profile: Default
User Interface
Layout
Columns
Font
Colors
Capture
Printing
Name Resolution
Statistics
Protocols
User Interface
Packet list selection mode:
Selects
Protocol tree selection mode:
Selects
Save window position:
Save window size:
Save maximized state:
Open a console window
Never
"File Open" dialog behavior:
Remember last directory
Always start in:
Directory:
C:¥Users¥Murachi¥Documents
"File Open" preview timeout:
3
Filter display max. list entries:
10
"Open Recent" max. list entries:
10
Ask for unsaved capture files:
Wrap to end/beginning of file during a find:
Settings dialogs show a save button:
Welcome screen shows version:
Help
OK
Apply
Cancel

User Interface

- ディスプレイ サイズに応じてフォントやウィンドウの設定をしましょう
- [Setting dialogs shows a save button] を有効にすると、複数の設定をする際に便利です。

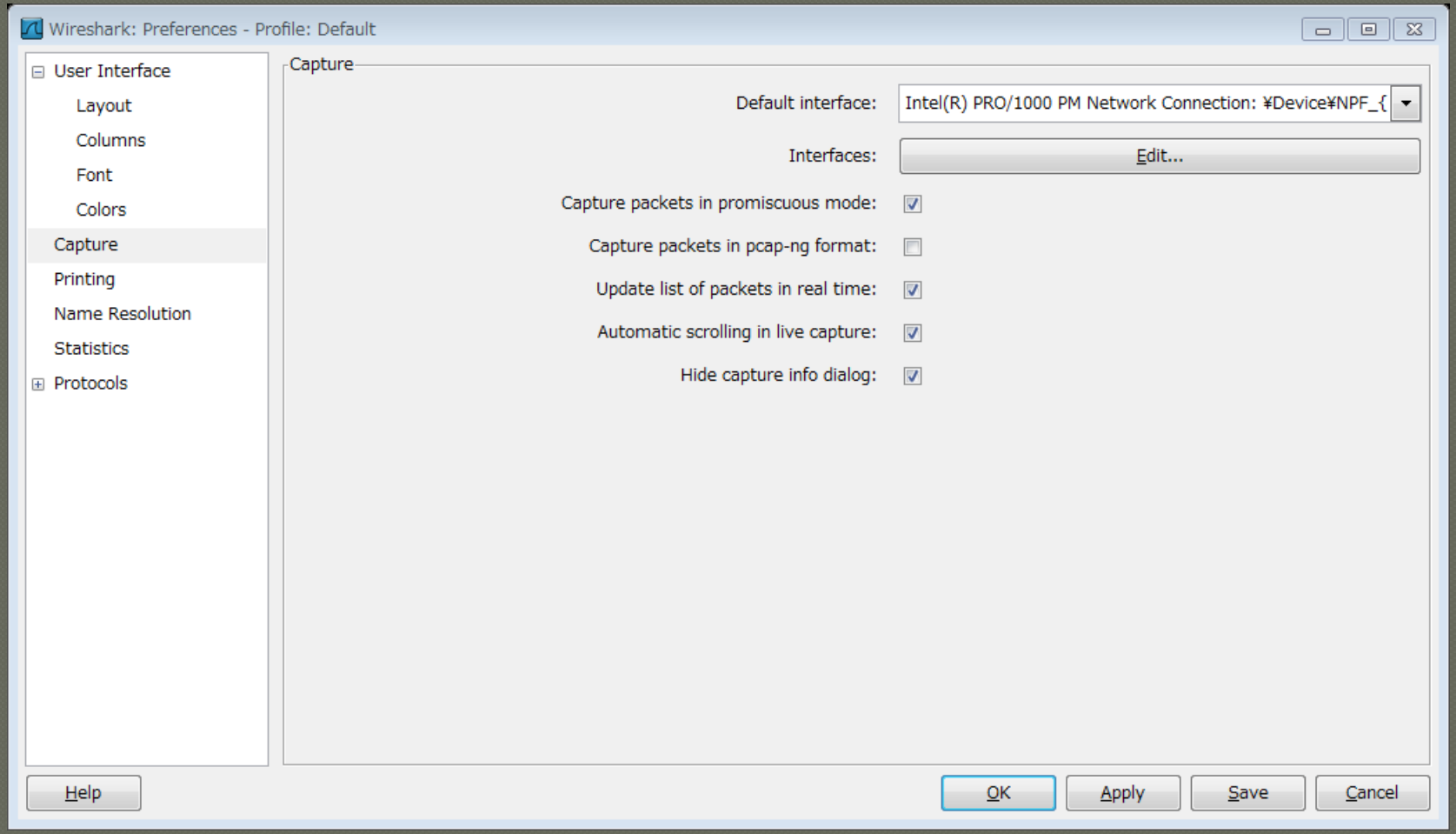
User Interface



Capture

- 既定でキャプチャするネットワーク インターフェイスを設定しましょう
- プロミスキャス モードを有効にするか設定しましょう
- スクロールの設定をしましょう
  （非力なマシンでキャプチャする場合は “Update list of packets in real time” と Automatic scrolling in live capture” をオフにしましょう）

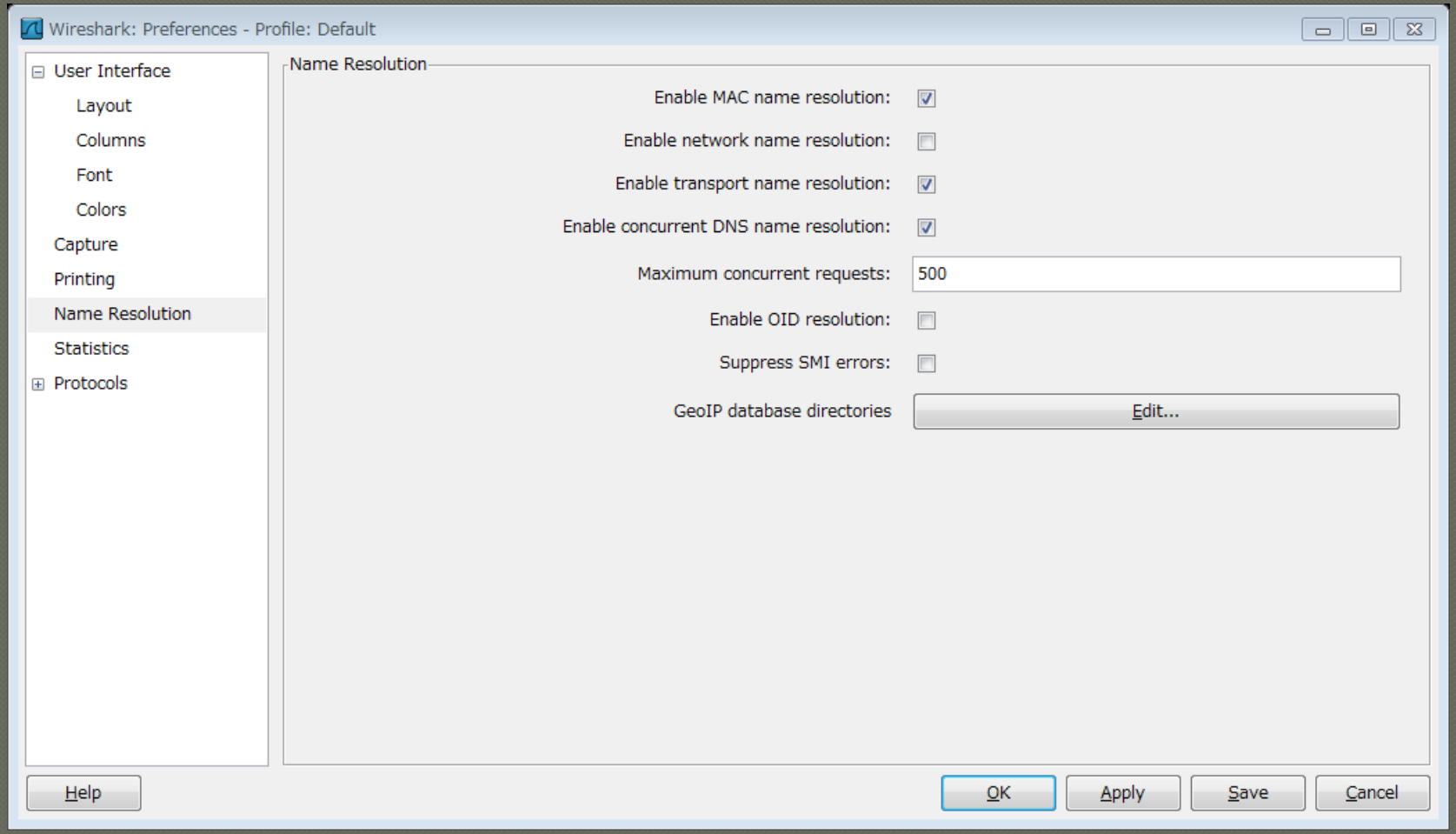
Capture


Wireshark: Preferences - Profile: Default
User Interface
Layout
Columns
Font
Colors
Capture
Printing
Name Resolution
Statistics
Protocols
Capture
Default interface:
Intel(R) PRO/1000 PM Network Connection: ¥Device¥NPF_{
Interfaces:
Edit...
Capture packets in promiscuous mode:
Capture packets in pcap-ng format:
Update list of packets in real time:
Automatic scrolling in live capture:
Hide capture info dialog:
Help
OK
Apply
Save
Cancel

Name Resolution

- MAC（ネットワークアダプタ）、コンピュータ（サーバー）名、サービス名の名前解決をして表示するか、設定しましょう。
  - ネットワーク名は DNS を参照するので負荷が大きくなります
  - サービス名はポートで判断するので、クライアント側のサービス名は当てになりません

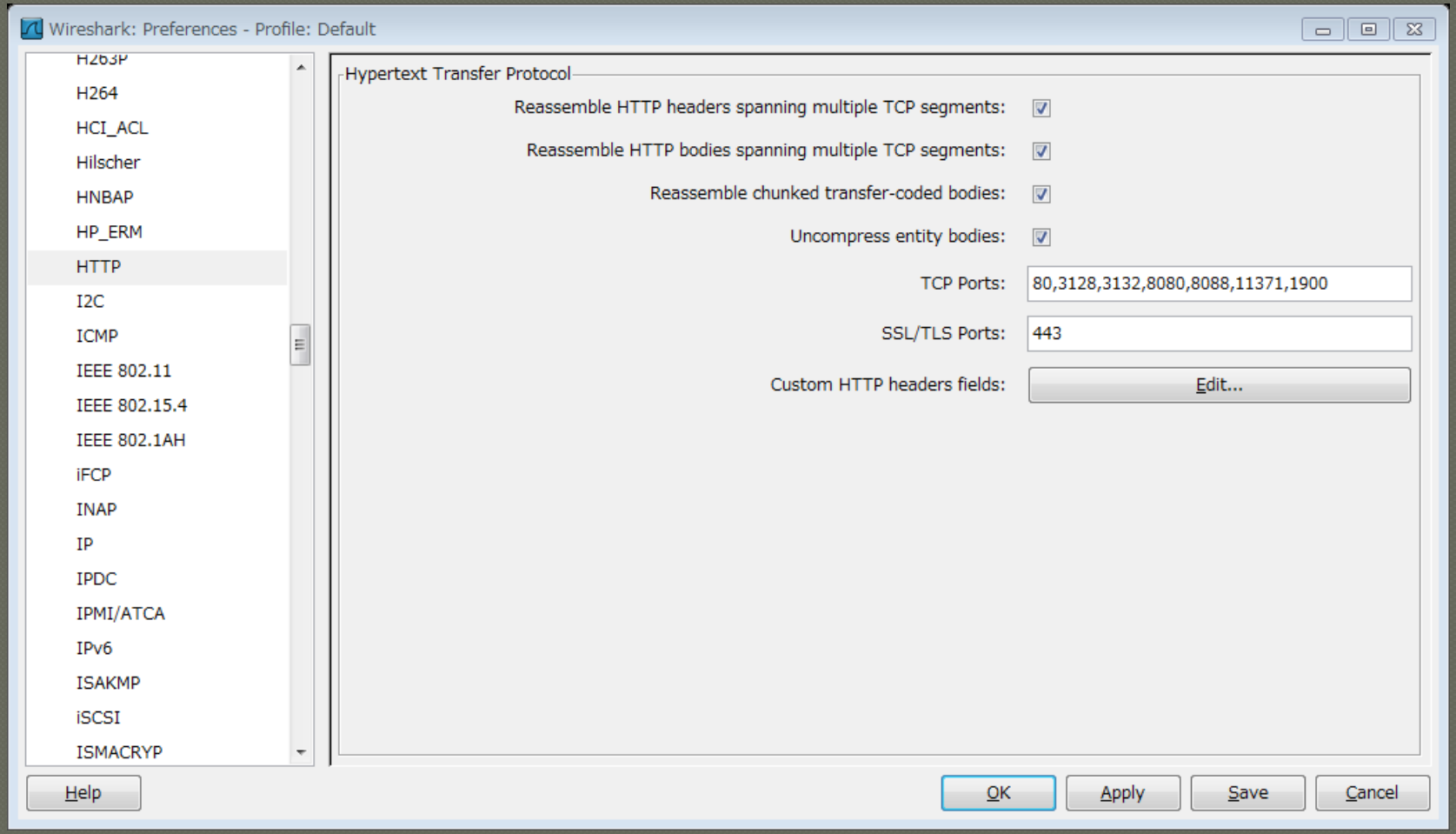
Name Resolution



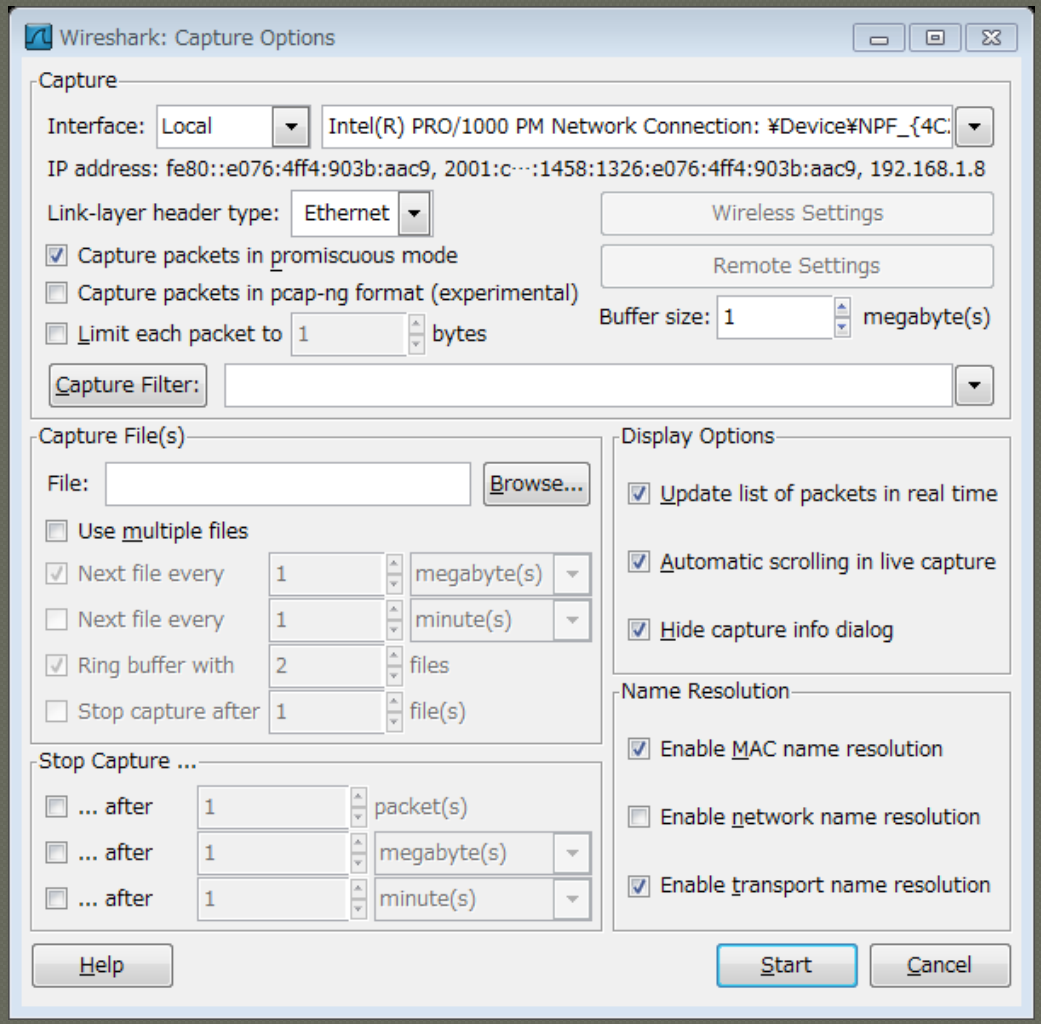
Protocols- HTTP

- “Reassemble HTTP bodies spanning multiple TCP segments” には要注意
- 有効にしていると、HTTP の Body を受信完了したフレームにヘッダー情報も表示されます
- 実際のサーバー応答が行われたフレームを確認したい場合は、無効にした方が分かりやすいです

Protocols- HTTP



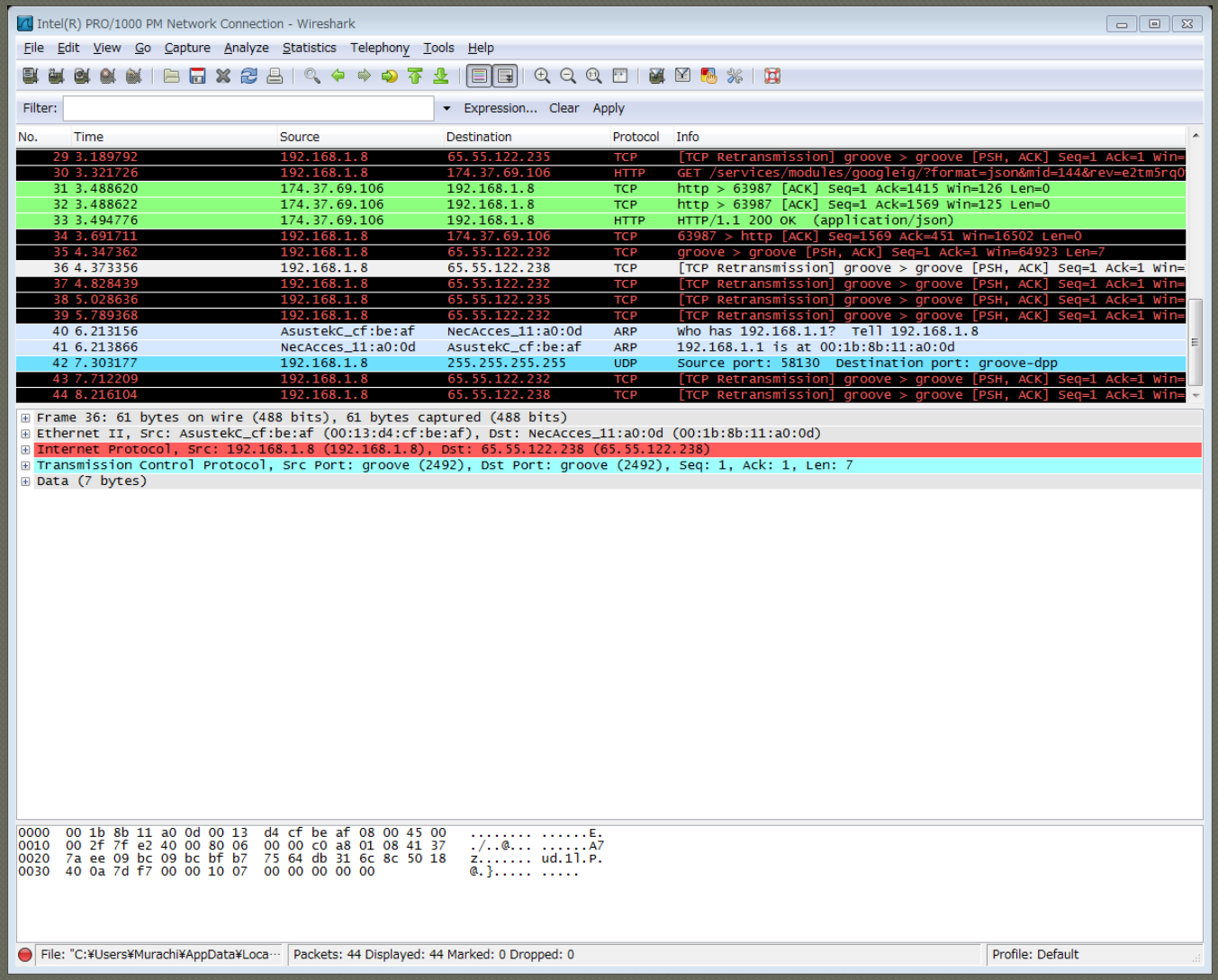
Capture Options



Capture Options

- 開始するキャプチャ セッションだけに有効な設定を行います
- キャプチャ フィルタが設定できます
  - できればフィルタなしでの採取がお勧め
- キャプチャを直接ファイルに保存する設定ができます
- キャプチャの自動停止の設定ができます

キャプチャの開始


Intel(R) PRO/1000 PM Network Connection - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
29 3.189792 192.168.1.8 65.55.122.235 TCP [TCP Retransmission] groove > groove [PSH, ACK] Seq=1 Ack=1 Win=
30 3.321726 192.168.1.8 174.37.69.106 HTTP GET /services/modules/googleig/?format=json&mid=144&rev=e2tm5rq0
31 3.488620 174.37.69.106 192.168.1.8 TCP http > 63987 [ACK] Seq=1 Ack=1415 Win=126 Len=0
32 3.488622 174.37.69.106 192.168.1.8 TCP http > 63987 [ACK] Seq=1 Ack=1569 Win=125 Len=0
33 3.494776 174.37.69.106 192.168.1.8 HTTP HTTP/1.1 200 OK (application/json)
34 3.691711 192.168.1.8 174.37.69.106 TCP 63987 > http [ACK] Seq=1569 Ack=451 Win=16502 Len=0
35 4.347362 192.168.1.8 65.55.122.232 TCP groove > groove [PSH, ACK] Seq=1 Ack=1 Win=64923 Len=7
36 4.373356 192.168.1.8 65.55.122.238 TCP [TCP Retransmission] groove > groove [PSH, ACK] Seq=1 Ack=1 Win=
37 4.828439 192.168.1.8 65.55.122.232 TCP [TCP Retransmission] groove > groove [PSH, ACK] Seq=1 Ack=1 Win=
38 5.028636 192.168.1.8 65.55.122.235 TCP [TCP Retransmission] groove > groove [PSH, ACK] Seq=1 Ack=1 Win=
39 5.789368 192.168.1.8 65.55.122.232 TCP [TCP Retransmission] groove > groove [PSH, ACK] Seq=1 Ack=1 Win=
40 6.213156 AsustekC_cf:be:af NecAcces_11:a0:0d ARP Who has 192.168.1.1? Tell 192.168.1.8
41 6.213866 NecAcces_11:a0:0d AsustekC_cf:be:af ARP 192.168.1.1 is at 00:1b:8b:11:a0:0d
42 7.303177 192.168.1.8 255.255.255.255 UDP Source port: 58130 Destination port: groove-dpp
43 7.712209 192.168.1.8 65.55.122.232 TCP [TCP Retransmission] groove > groove [PSH, ACK] Seq=1 Ack=1 Win=
44 8.216104 192.168.1.8 65.55.122.238 TCP [TCP Retransmission] groove > groove [PSH, ACK] Seq=1 Ack=1 Win=
Frame 36: 61 bytes on wire (488 bits), 61 bytes captured (488 bits)
Ethernet II, Src: AsustekC_cf:be:af (00:13:d4:cf:be:af), Dst: NecAcces_11:a0:0d (00:1b:8b:11:a0:0d)
Internet Protocol, Src: 192.168.1.8 (192.168.1.8), Dst: 65.55.122.238 (65.55.122.238)
Transmission Control Protocol, Src Port: groove (2492), Dst Port: groove (2492), Seq: 1, Ack: 1, Len: 7
Data (7 bytes)
0000 00 1b 8b 11 a0 0d 00 13 d4 cf be af 08 00 45 00 ....E.
0010 00 2f 7f e2 40 00 80 06 00 00 c0 a8 01 08 41 37 ./..@... .....A7
0020 7a ee 09 bc 09 bc bf b7 75 64 db 31 6c 8c 50 18 z..... ud.1l.P.
0030 40 0a 7d f7 00 00 10 07 00 00 00 00 00 @.}..... .....
File: "C:¥Users¥Murachi¥AppData¥Loca··· Packets: 44 Displayed: 44 Marked: 0 Dropped: 0 Profile: Default

非力なマシンでのキャプチャ

- 非力なマシン上で高負荷のトラフィックをキャプチャすると、取りこぼしが起きる場合もあります

回避策

- コマンドライン版を使う（tshark）
- dumpcap や tcpdump、WinDump 使う

DEMO

参考資料

- **Wireshark User's Guide**
  http://www.wireshark.org/docs/wsug_html_chunked/
- **Wireshark Wiki**
  http://wiki.wireshark.org/FrontPage
- **Wireshark University**
  http://www.wiresharktraining.com/