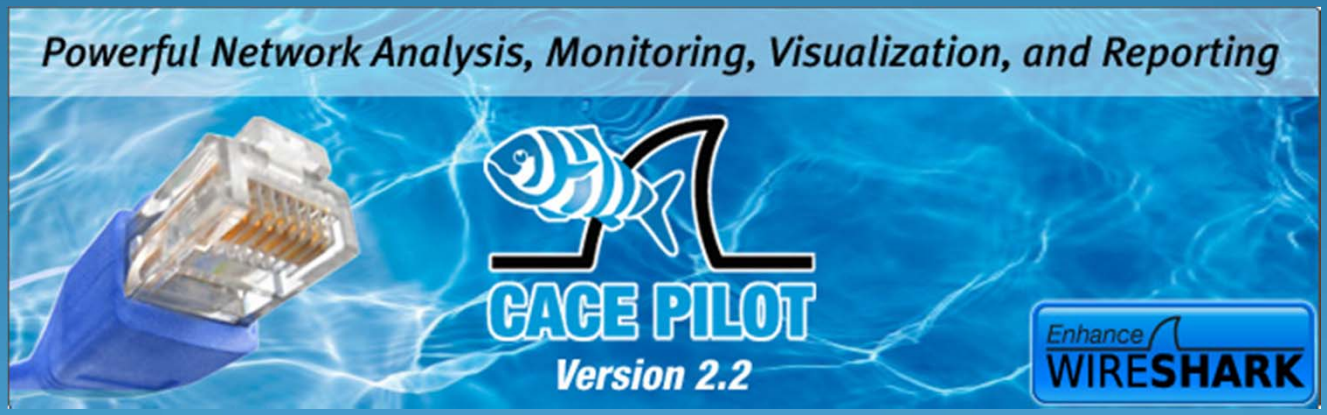
WiresharkとCACE Pilotによるダンプ解析とトレンド分析

(Pilot-1)



いけりり★ネットワークサービス　竹下恵

http://www.ikeriri.ne.jp/

竹下恵(Megumi Takeshita)
いけりり★ネットワークサービス

- 鹿児島県出身　鶴丸高校→上智大学　ベイネットワークス　ノーテルネットワークスを経ていけりり★ネットワークサービスを創設
- パケットキャプチャおよび、情報処理技術者試験に関する自著15冊
- 個人のブログはこちら
  http://www.ikeriri.ne.jp/blog/
- コールサイン JA1UVG
- 年齢や3サイズは禁則事項です！

Agenda:セッションの概要

- オリエンテーション
- 1：パケットキャプチャとダンプ解析・トレンド分析
  - 1－1:キャプチャ前に準備すること
  - 1－2:LANアナライザWiresharkの紹介
  - 1－3:Wiresharkの主要機能(ハンズオン)
  - 1－4:WiresharkのTIPSとテクニック
  - 1－5:Wiresharkによるダンプ解析 (EthernetII/ARP/IP)
  - 1－6:ARP処理とIPフラグメント化
  - 1－7:TCPとUDPの見方
  - 1－8:HTTPの分析
  - 1－9:Wiresharkの統計機能
- 2:CACE Pilotの基本
  - 2－1:CACE Pilotの紹介
  - 2－2:CACE Pilotのインストールと起動
  - 2－3:インタフェース・pcapファイルの設定
  - 2－4:Viewの適用・カスタムViewの作成
  - 2－5:Drill DownとWiresharkとの連携
  - 2－6:Time Controlの設定
  - 2－7:レポートの出力と保存
  - 2－8:Watchの作成と適用
- 3:Wireshark/Pilot応用(フィルタ)
  - 3－1:プロファイルの作成と切替
  - 3－2:Wiresharkの設定ファイル
  - 3－3:キャプチャフィルタの利用
  - 3－4:リモートキャプチャ
  - 3－5:エキスパートモード
  - 3－6:ファイルラベル
  - 3－7:遅延に関するフィルタ
  - 3－8:各プロトコル分析のフィルタ
  - 3－9:セキュリティ調査のフィルタ
- 質疑応答

オリエンテーション

- ようこそ！ Welcome！いけりりセミナーへ！
- 時間は10:00－17:00（お昼休み:12:30－13:00）
  休憩はだいたい90分に1回くらい10分程度とります。
  延長18:00までは考えてください。19:00には片付けます！
- 座席はお好きなところで大丈夫です
- PC（Windows7） ※持ち込みPCを利用されてもOKです。
- 当ビルは全館禁煙となっております。（すみません！）
- 原則飲食物は禁止ですが、飲み物はこぼさないようにして持ち込んでいただいて構いません。
- 気軽にどんどん質問していただいて構いません！ぜひ！
- 御領収書、法人の方へ御請求書などをお渡ししています。
  もし記述に不備や要望がありましたらお教えください。

配布物/環境の紹介

★配布物

- CACE Pilot体験版CD（ライセンスキー付属）1点
- レジュメ（本スライド）1点
- CACE Pilot Reference Manual 1点
- Network Toolkit CD-ROM 1点
- USBメモリ1点
- CACE社　サインペンおよびメモ帳　1点
- いけりりバッグ・マグネット・ストラップ

★実習環境

- Windows7（少し準備が必要です！）
- 有線LAN

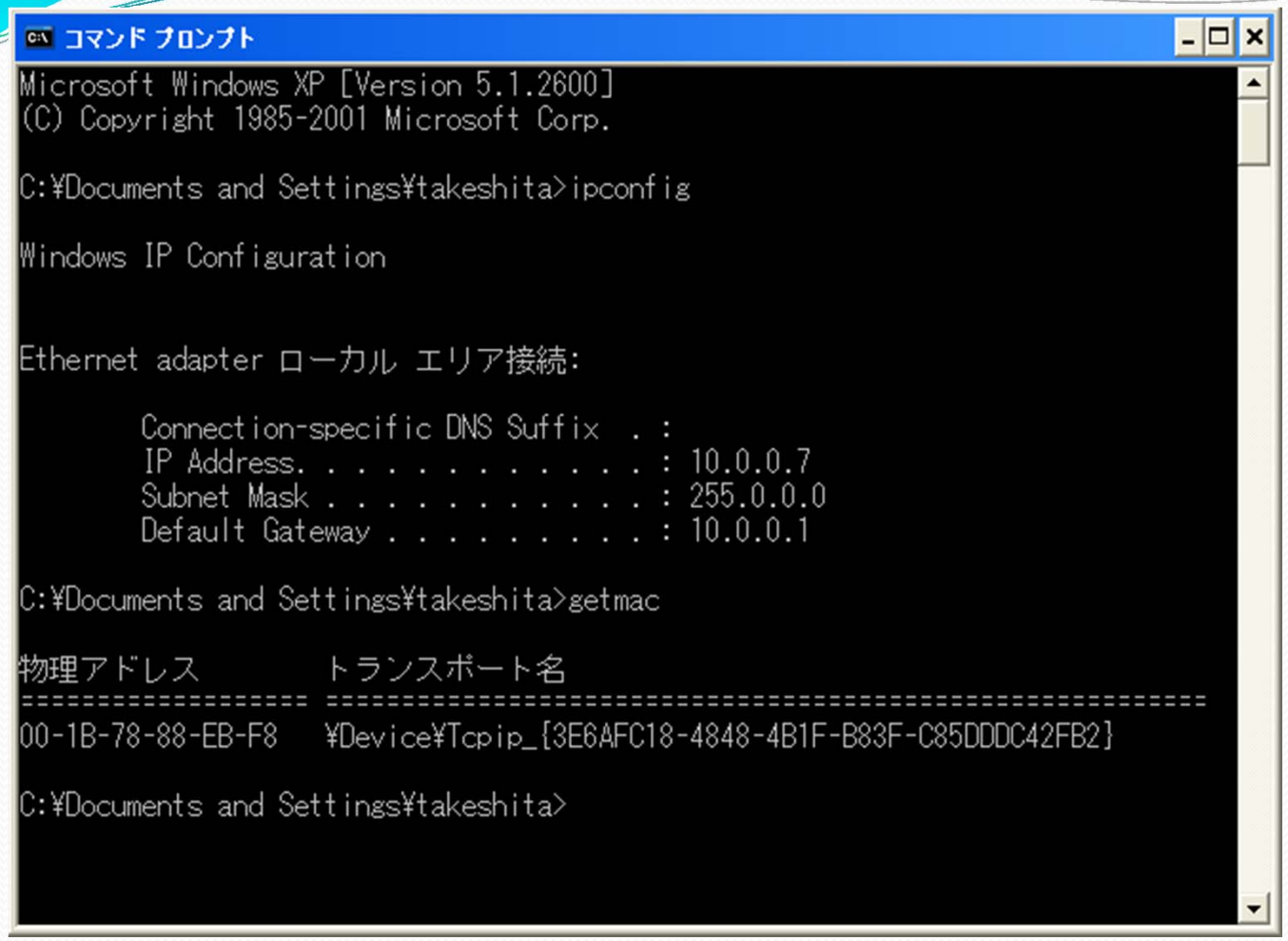
1:パケットキャプチャと分析

トピック
1－1:キャプチャ前に準備すること
1－2:LANアナライザWiresharkの紹介
1－3:Wiresharkの主要機能(ハンズオン)
1－4:WiresharkのTIPSとテクニック
1－5:Wiresharkによるダンプ解析(EthernetII/ARP/IP)
1－6:ARP処理とIPフラグメント化
1－7:TCPとUDPの見方
1－8:HTTPの分析
1－9:Wiresharkの統計機能

キャプチャする前に準備すること

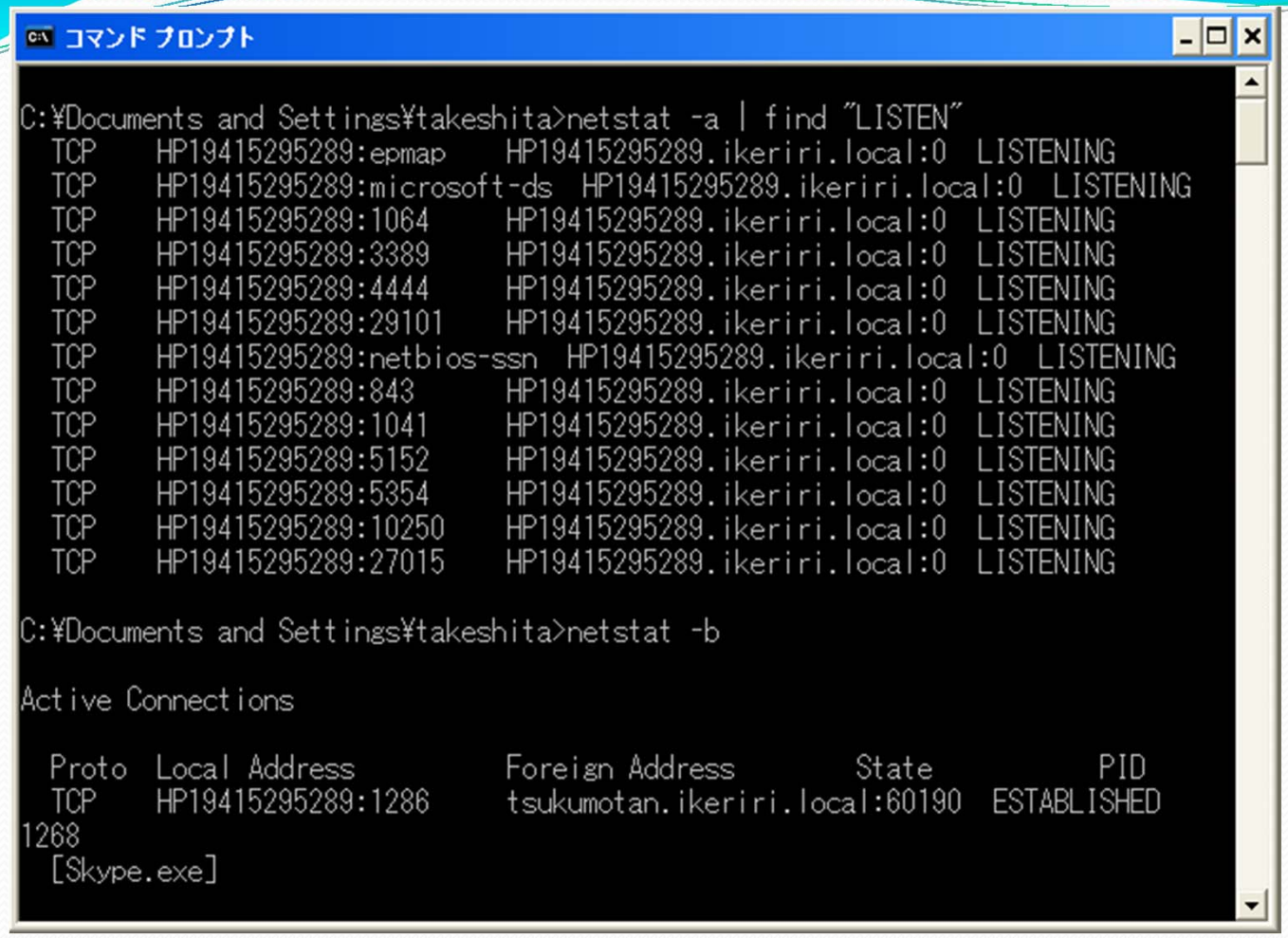
- テキストの方にも記載（入門）P81　（応用）P25あります。
- Webブラウザのキャッシュをクリアします。また、プロキシサーバーの設定をなし（直接接続）にします。、
- ウイルス・スパイウエア対策ソフトの自動検出機能、また、WindowsFirewallや各種パーソナルファイアウォールをオフにしてください。
- 不要な常駐ソフトウエアは可能な限り停止してください。
- 不要なサービスを停止します。
  ※特にパケットを出すものは止めておくと便利です。
  例 VPN関係やUPnP、iTuneやプリンタ等へのアクセス
- 日付、IPアドレス、MACアドレスなどといった情報を残しておくと後で確認する際に便利です。

準備しておくこと便利(1)



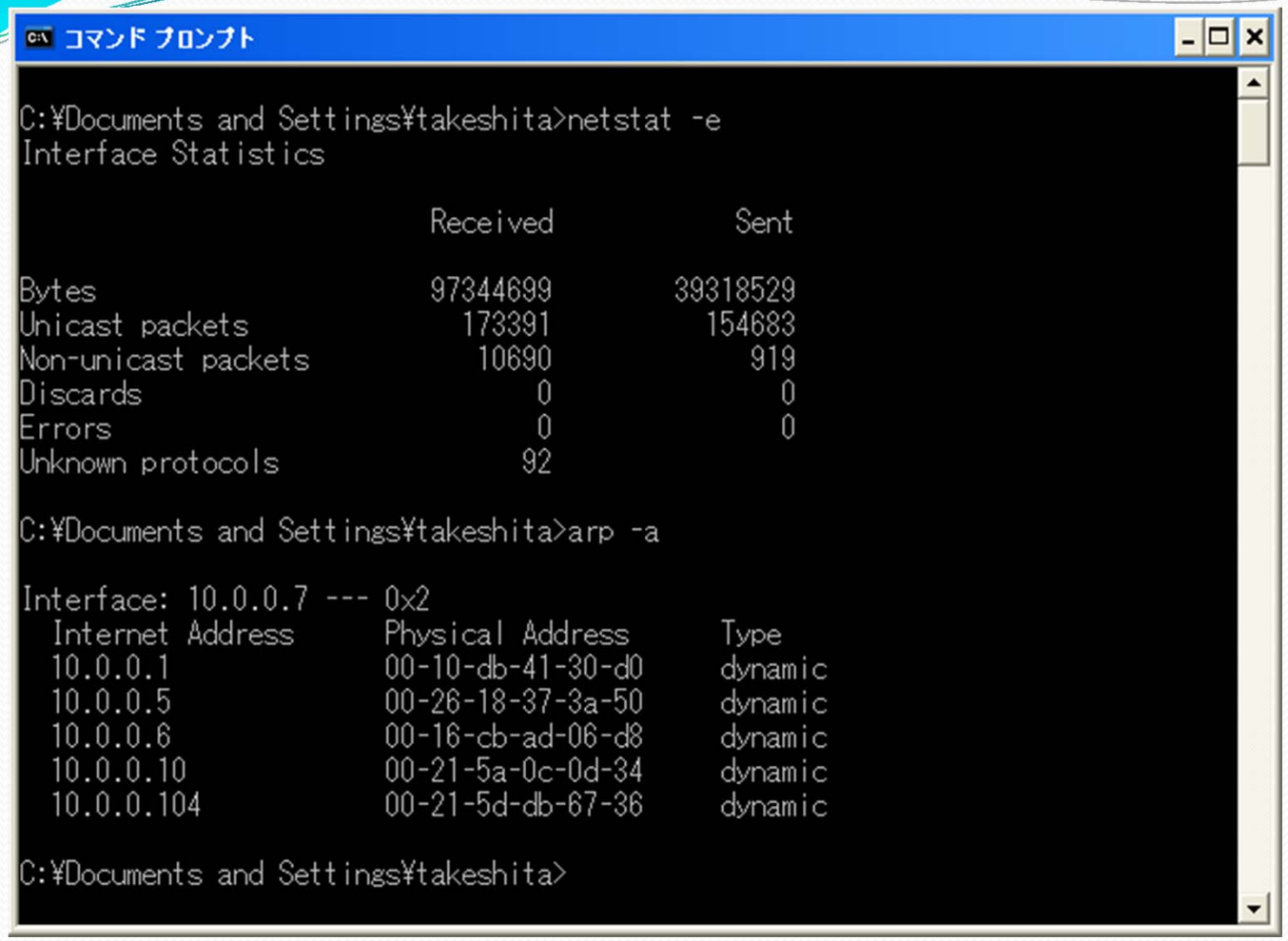
- **Ipconfigとgetmacの内容やついでにdate /tやtime /tの結果もリダイレクトしてテキストファイルに残しておきます。**
  例:ipconfig /all > C:¥junbi.txt

準備しておくこと便利(2)



- TCPやUDPの接続の状態はnetstatで確認できます。これをパイプして特にポートが開いているもの(LISTEN)しているものを確認しておきます。また-bも実施します。

準備しておくこと便利(3)

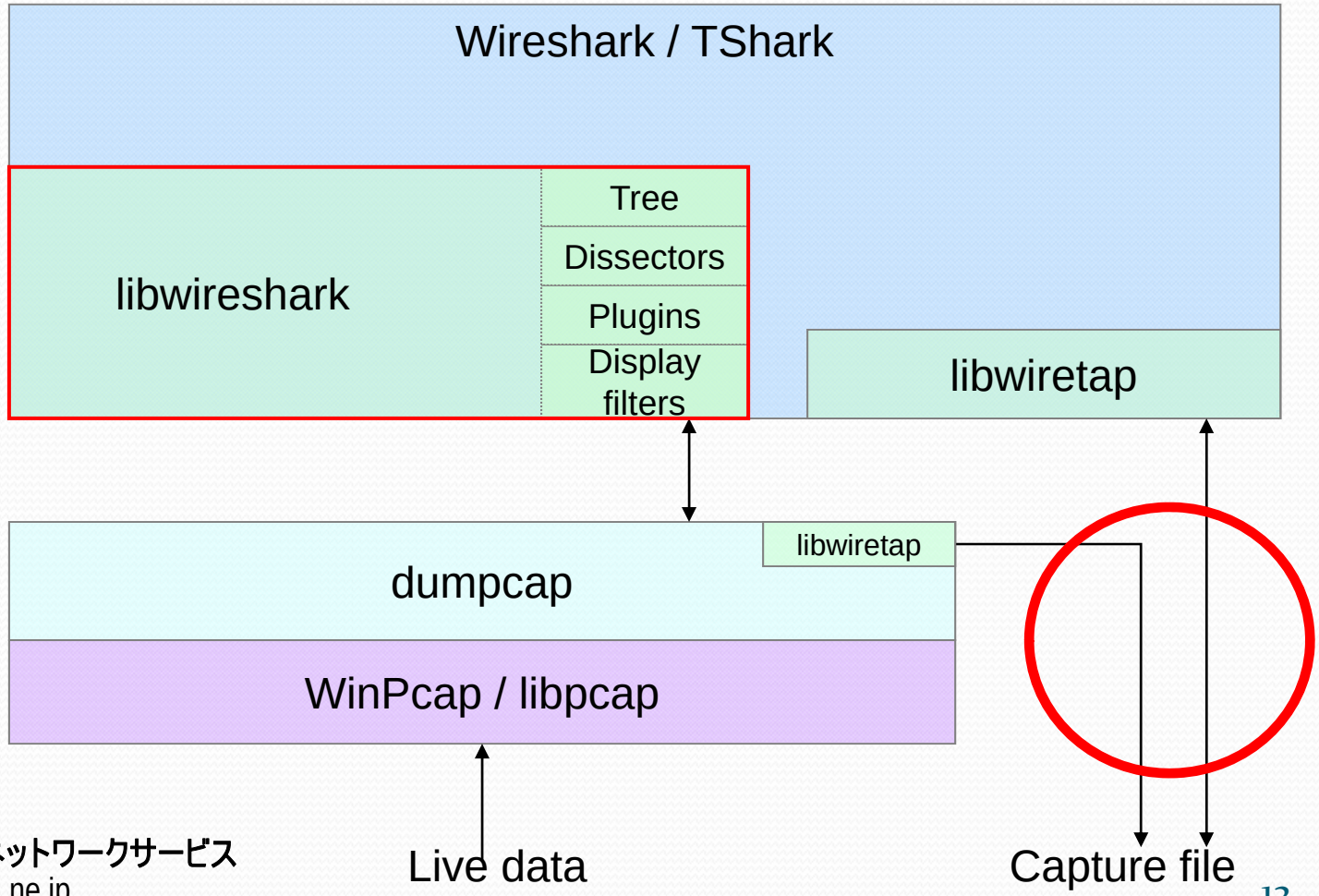


- NICの状態(特にエラーフレーム)がないか確認しておきます。ARPテーブル(IPとMACの対応表)に問題がないかも見ておくとよいです。

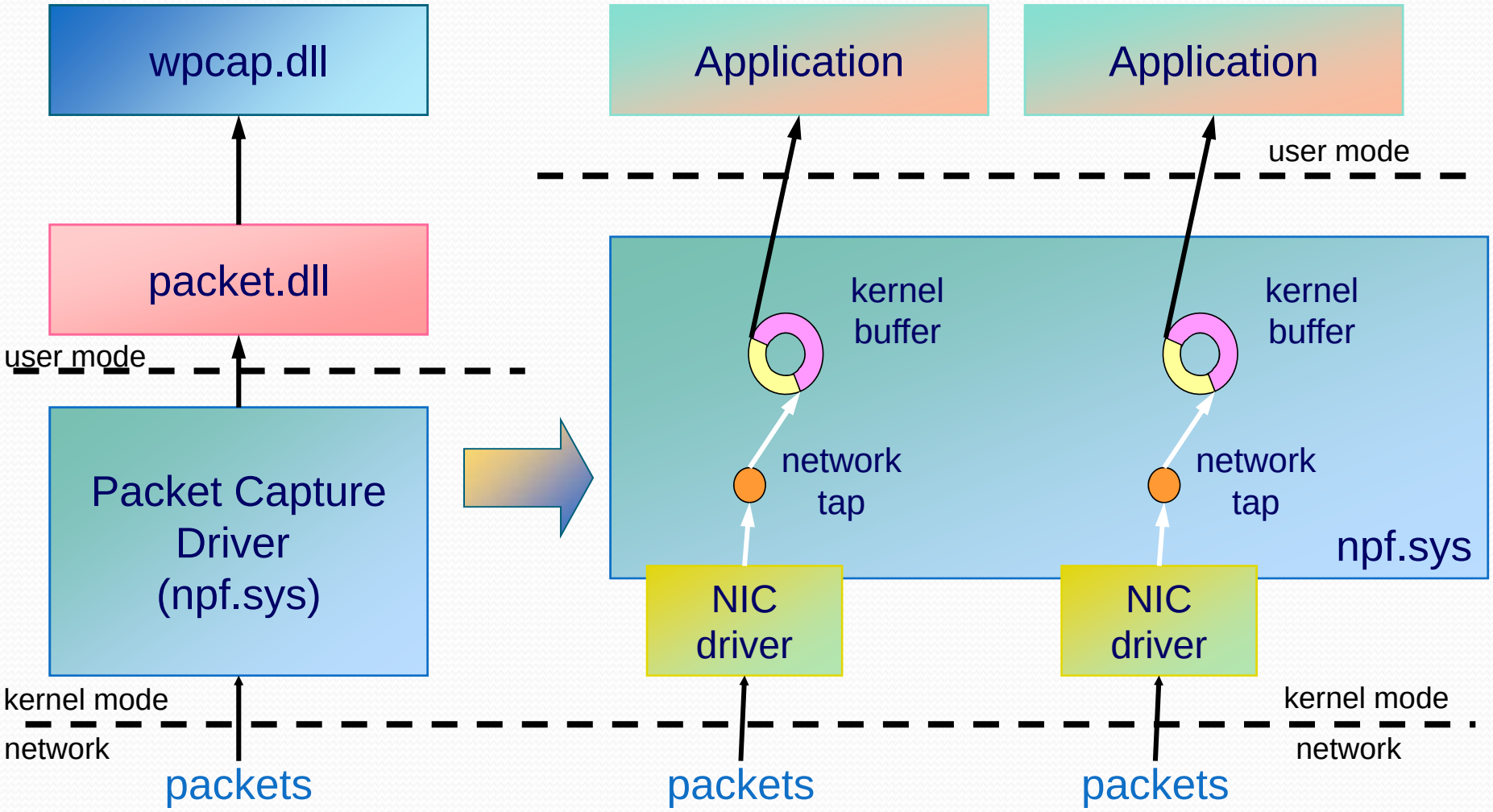
Wiresharkについて

- オープンソース（GPL）のLANアナライザ
  （元Ethereal）デコードできるプロトコルは1000以上
- ソースコードやWindows(32/64/USB版）やOSX・Linux対応
- WikiにあるSampleキャプチャページは必見です
  http://wiki.wireshark.org/SampleCaptures
- 新バージョンでできるようになったこと（主要機能）
  ★TCPやUDPの通信内容を色分けできるようになりました。
  ★グラフ機能とキャプチャフィルタが強化されています。
  ★設定プロファイルが作れるようになりました。
  ★別ウインドウでパケットを開いたりできます。
  ★FWのトラフィックフィルタ対応（途中）
  ★Lua対応（API）Dissectorが書きやすくなりました。
  ★ステータス行など、様々な部分で地味に強化

Wiresharkのアーキテクチャ

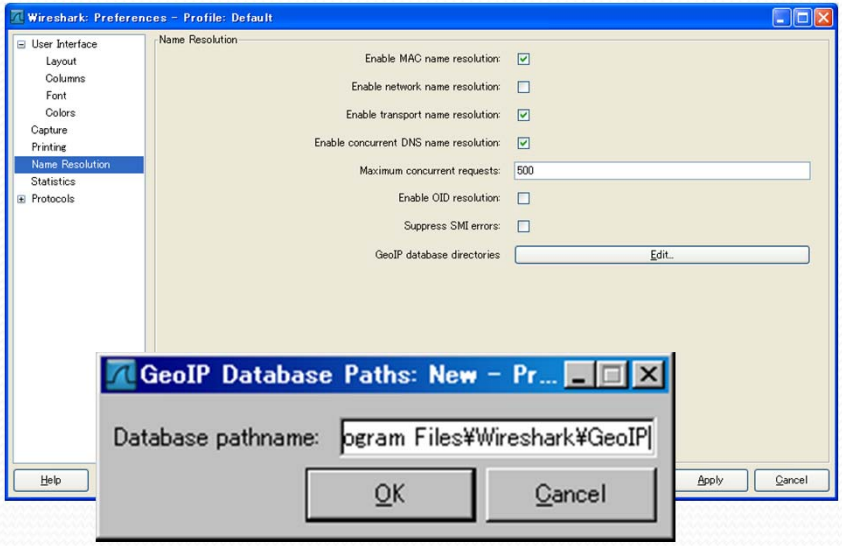


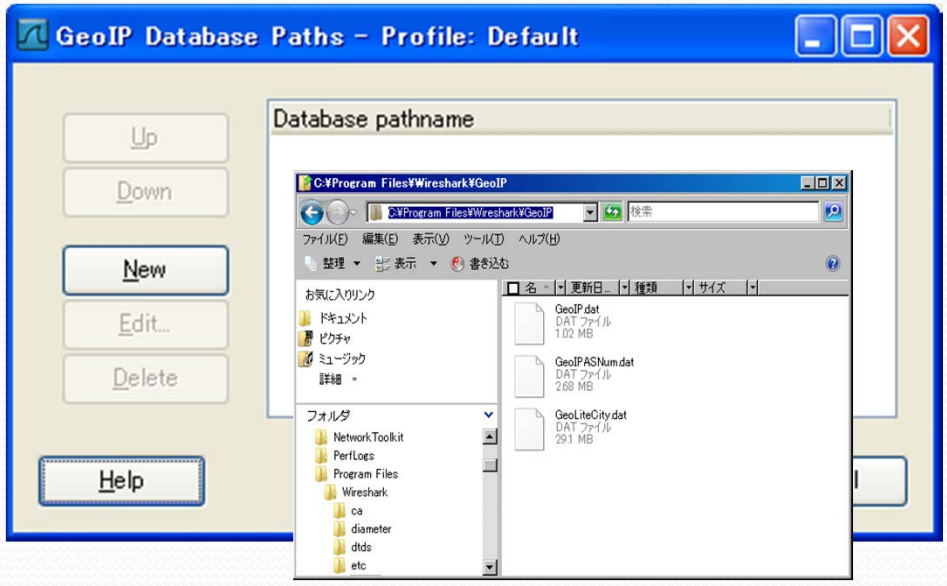
WinPcapのアーキテクチャー



GeoIPデータベースの活用

- GeoIPデータベースを設定すると、IPアドレスから地理情報（緯度や経度）、AS番号などの情報を活用できます。
- C:¥Program Files¥Wireshark¥GeoIP を追加して、MaxMind社のページのデータベースを設定します。





TIPS1：ぜひ覚えたいショートカット

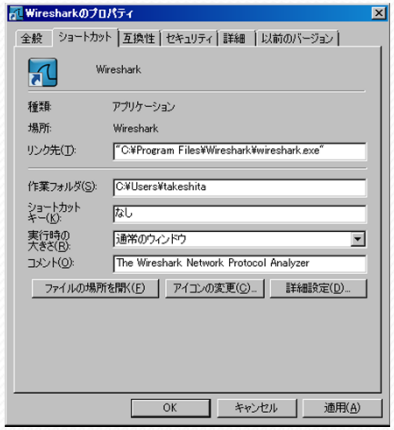
キー操作	内容
Ctrl+↑や↓	パケット一覧画面にフォーカスをあてている状態で、パケット詳細画面のフィールドの上下（↑↓）移動ができます。（超便利）
Ctrl+←や→	パケット一覧画面にフォーカスをあてている状態で、パケット詳細画面のツリーの展開（→）と折りたたみ（←）ができます。
Ctrl+O,Ctrl+W,Ctrl+P, Ctrl+P,Ctrl+S, Ctrl+Shift+S,Ctrl+Q	基本的ですが、パケットキャプチャファイルを開く(Open)、閉じる(Window Close)、印刷(Print)、保存(Save)、名前をつけて保存(Save As)、終了(Quit)
Ctrl+H	パケットのデータ部の任意のバイトを選択して出力できます。１６進数(Hex)で覚えてください。データの復元や取り出しに便利です。
Ctrl+F	パケットの検索（Find）
Ctrl+N,Ctrl+B	次のパケットへ（Next）や前のパケット（Before）への移動
Ctrl+M Shift+Ctrl+N,Shift+Ctrl+B Ctrl+A,Ctrl+D	パケットのマーク（Mark）、多用します！これで印刷、保存へ マークしたら次（Shift+Next）や前（Shift+Before）へ移動 全部マーク（All）やマーク削除（Delete）も使うといいです。
Ctrl+T	参照時間をセット（Time）選択したパケットを基準時間にしたい時
Ctrl+Shift+P, Ctrl+Shift+A	設定（Preference）を確認します。 設定プロファイルはCtrl+Shift+A

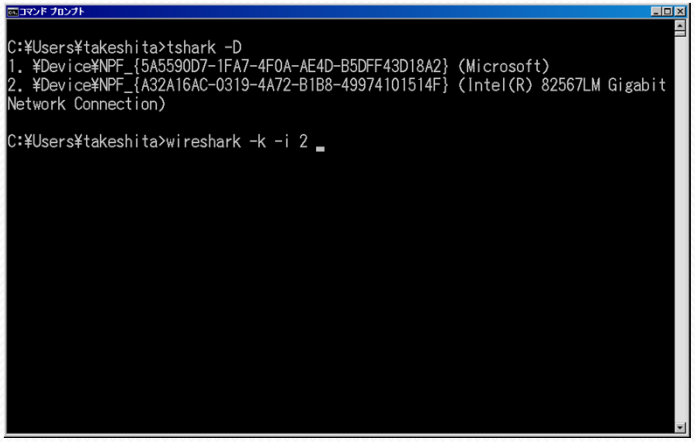
TIPS2：ぜひ覚えたいショートカット

キー操作	内容
Ctrl+[+],Ctrl+[-], Ctrl+[=]	画面のフォントの変更、テンキーが使えるとさらに便利です。拡大は[+]、縮小は[-]、等倍は[=]になります。
Ctrl+Shift+R	列のリサイズ（Resize）拡大、縮小などで表示がずれたときに便利
Ctrl+R	パケットを再読込（Reload）します。表示がくずれたり、おかしくなったときにこれをやると直ります。
Ctrl+[Space]	色分けルール（1-10）を元に戻します。独自の色分けを設定した後、普通に戻したい時などに利用します。
Alt+←や→	Ctrlだとフィールドの展開と縮小でしたが、Altと左右（←→）で過去に選択したパケットの前と後の移動ができます。
Alt+[Home],Alt+[End]	WordやExcelでもおなじみですが、最初のパケットと最後のパケットへ移動できます。
Ctrl+G	任意の番号のパケットへ移動（Go）します。
Ctrl+I	キャプチャインタフェース画面(Interface)を表示します。
Ctrl+K	キャプチャオプション（Kyapucha Option）画面を開きます。。
Ctrl+E（トグル） Ctrl+R（キャプチャ中）	キャプチャの開始や停止を行います（Execute）、キャプチャ中にもういっかい取り直したいときはCtrl+R（Restart）です。
Ctrl＋Shift+E	デコードするプロトコルを有効化（Enabled）します。

TIPS3：起動ショートカット

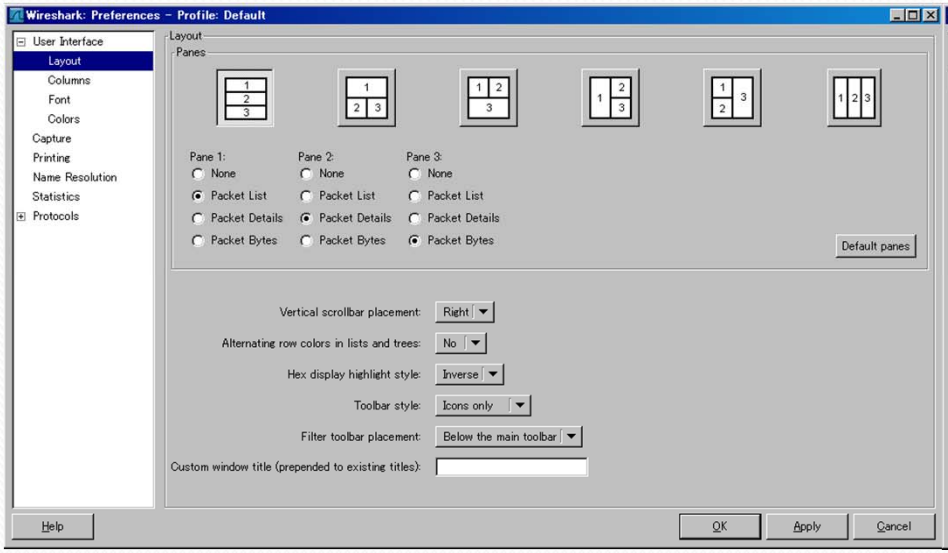
- Wiresharkのコマンドラインマニュアル
  http://www.wireshark.org/docs/man-pages/wireshark.html
- すぐにキャプチャを始めるなら –kオプションを付けます。
  インタフェース指定は-iの後にインタフェース名
  tshark –Dでインタフェースのインデックスも指定できます。
  例：C:¥Users¥takeshita>wireshark -i ¥Device¥NPF_{A32A16AC-0319-4A72-B1B8-49974101514F} –k
- バッチファイルや起動ショートカットにしておきます。
  環境変数のPATHにC:¥Program Files¥Wiresharkも！

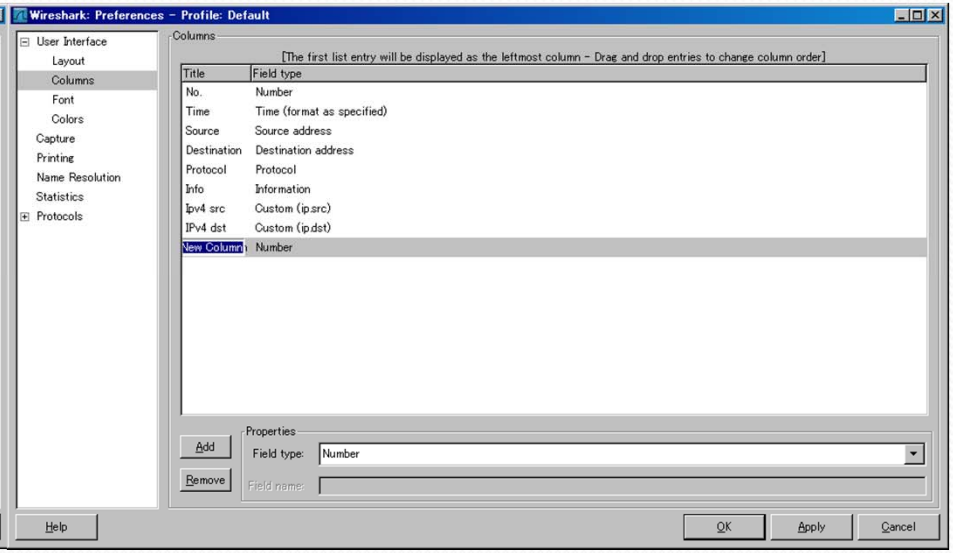




TIPS4：表示の変更と列の追加

- 用途に応じて画面表示スタイルを変更しましょう
  Preference＞Layout　例：ダンプをみたい場合等
- 頻繁に追いかけたいフィールドは列に追加しておきます。
  Preference＞Columns
  TCPのシーケンス番号、確認応答番号
  送信元ポート、宛先ポート等





EthernetII上でのパケットサイズ

ICMP

EthernetII (14)	IP (20)	ICMP (8)	メッセージサイズ MTU=1500なら1472まで

- ping 相手IP –l メッセージサイズ
  ※-fを付加することでフラグメント禁止

TCP

EthernetII (14)	IP (20)	TCP (20)	セグメントサイズ MSS＝1460

UDP

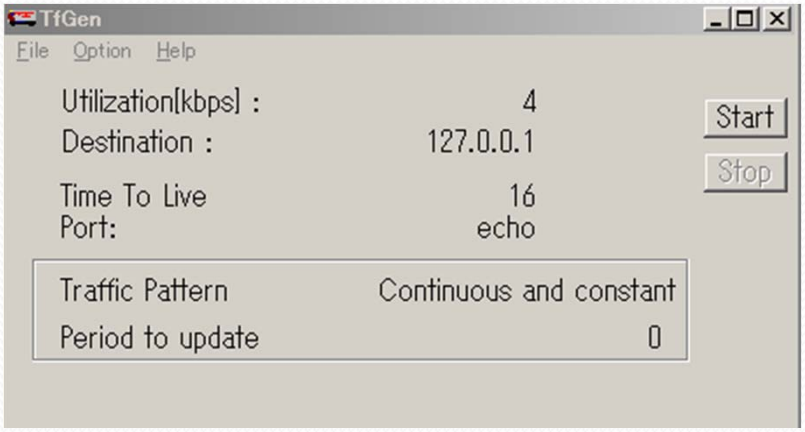
EthernetII (14)	IP (20)	UDP (8)	データグラムサイズ MTU=1500なら1472まで

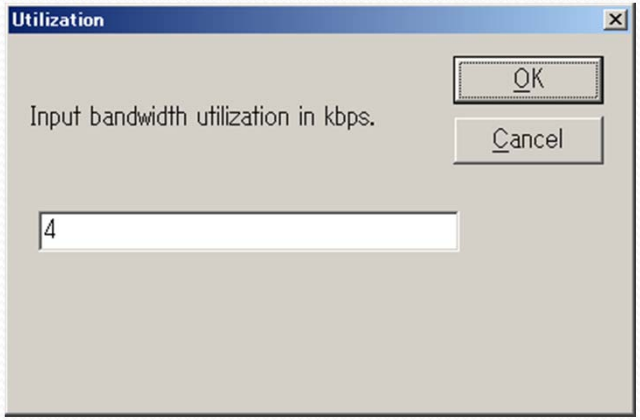
PPPoEヘッダーと各種MTUサイズ

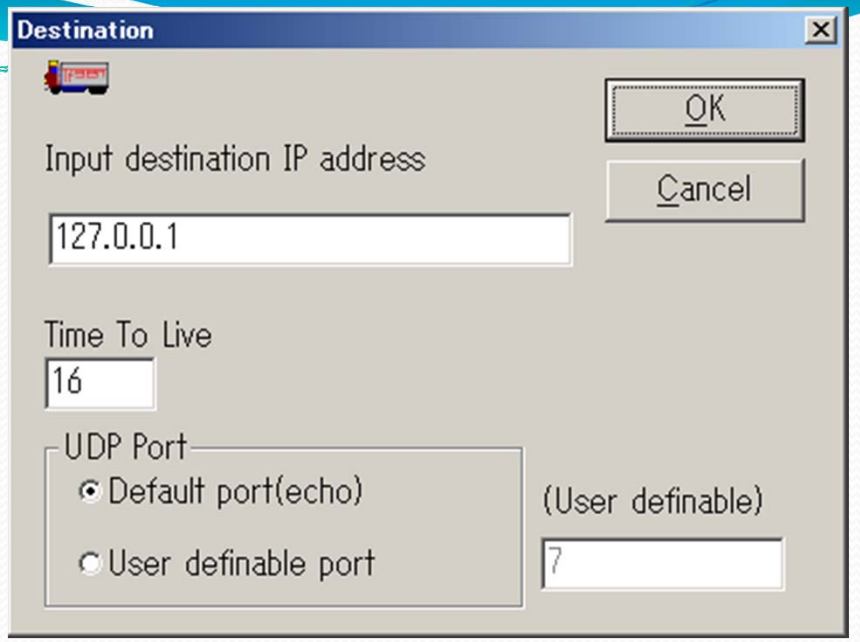
- NTT東日本フレッツ網
  MTUを1454Byte以下（MSSを1414Byte以下）
- 西日本フレッツ光プレミアム
  MTUを1438Byte以下（ MSSを1398Byte以下）
- GRE + IPsec (転送モード)1440 バイト
- GRE + IPsec (トンネルモード)1420バイト
- UDP(NAT Traversal）はIP(20)UDP(8)および
  PPPoE、PPPヘッダなどをさらに減じます。

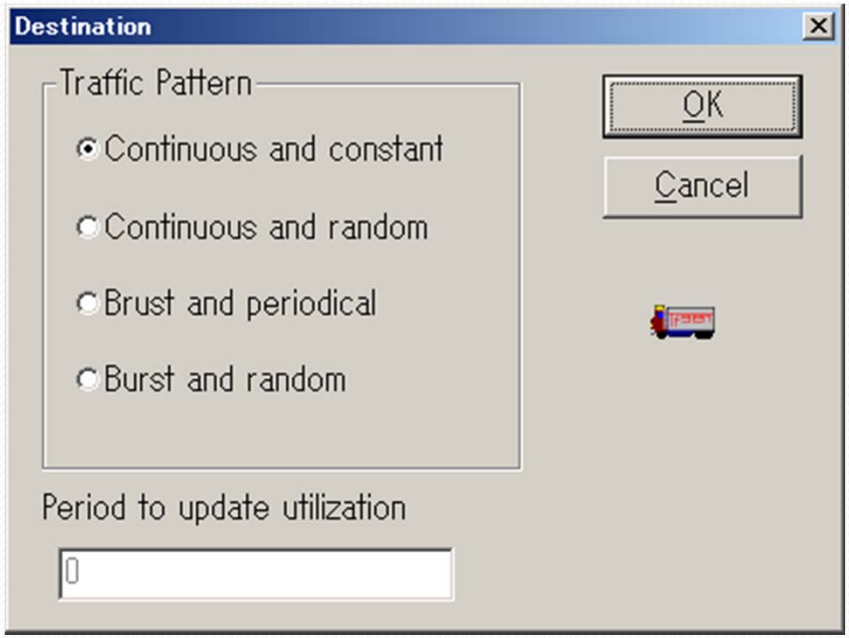
tfgen

- Tfgenはフリーのトラフィック送信テストツールです



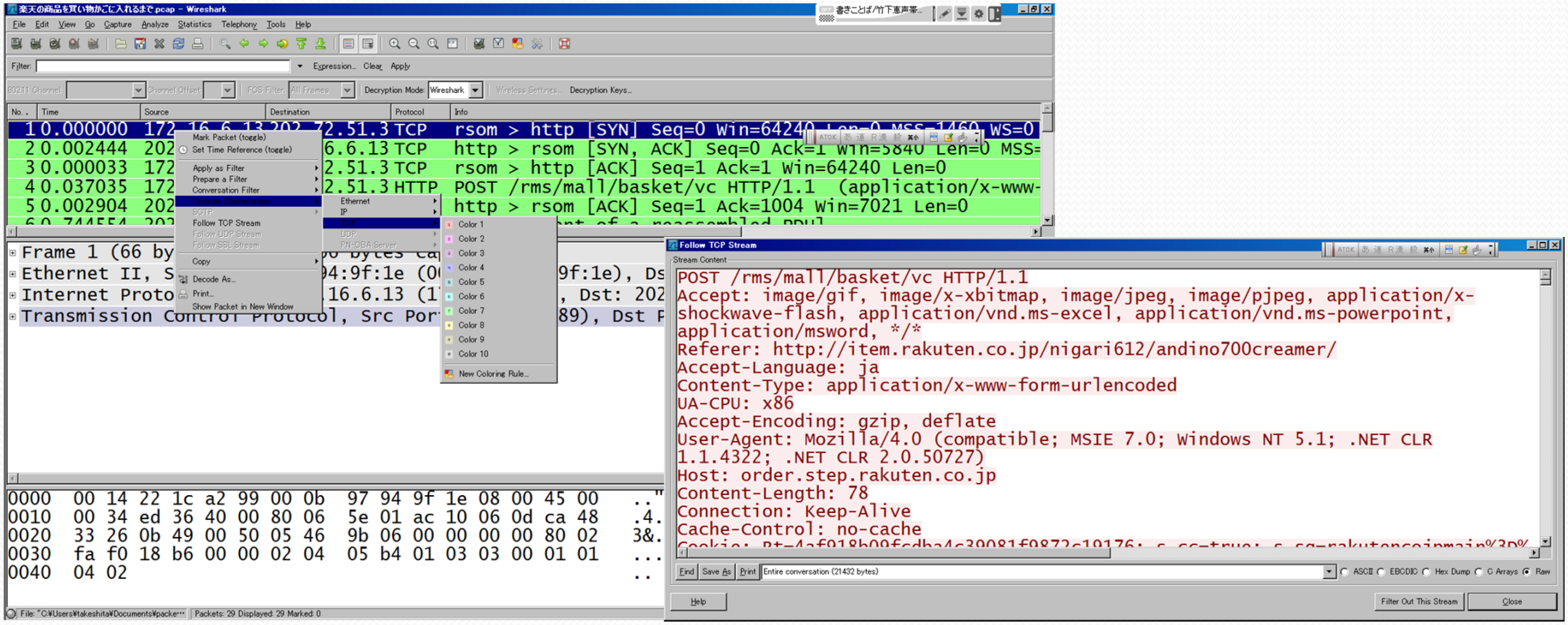






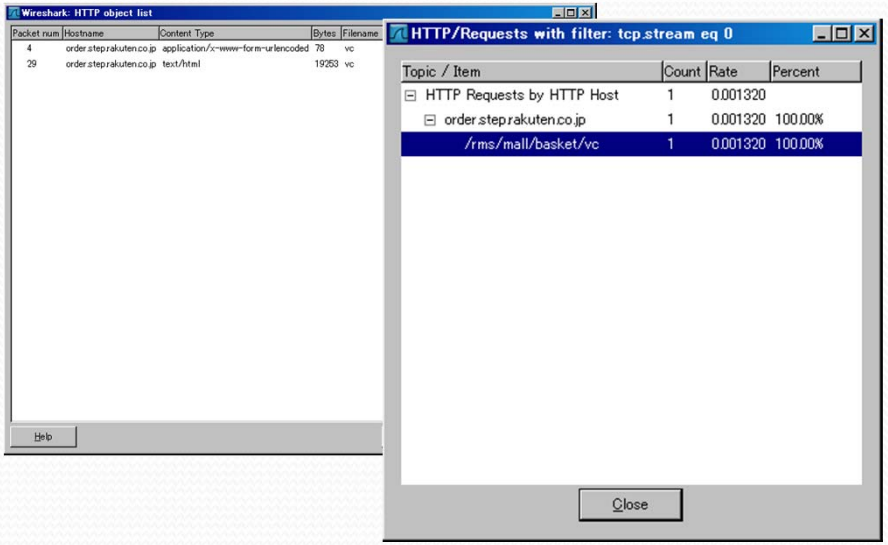
TCPとUDPはストリームで見ます

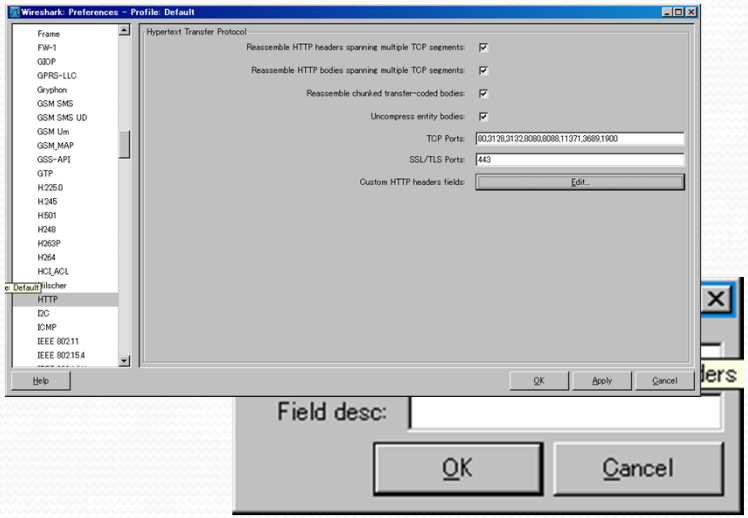
- TCPの通信を見たら、その通信を色分けします。
- Follow TCP Streamでバイトの内容を抽出します。
- UDPもFollow UDP Streamで確認してください。



HTTPのExport機能を活用しましょう

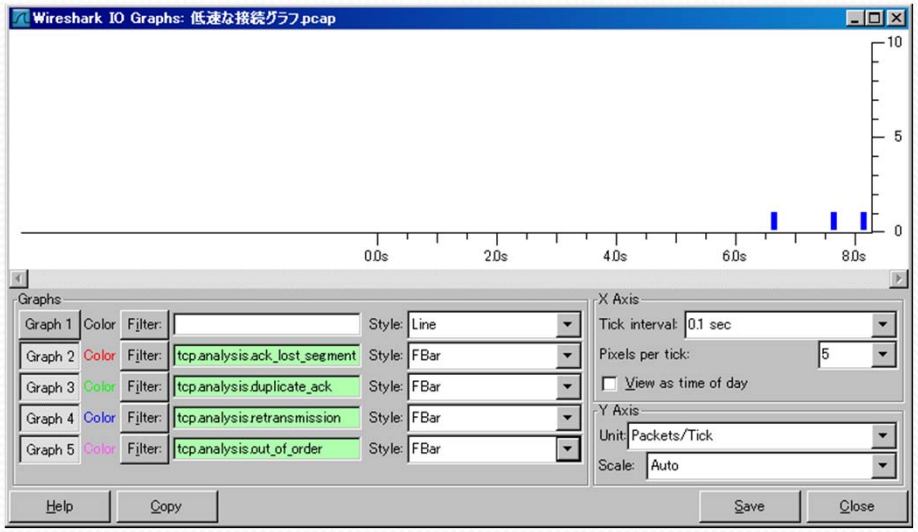
- Webの通信内容は日本語も含めて復元できます。
  File>Export>Object>HTTP （画像等もOK）
- HTTP特有の統計もあります。
  Statistics>HTTP以下
- カスタムヘッダーの追加もできます。
  Preference>Protocol＞HTTP以下

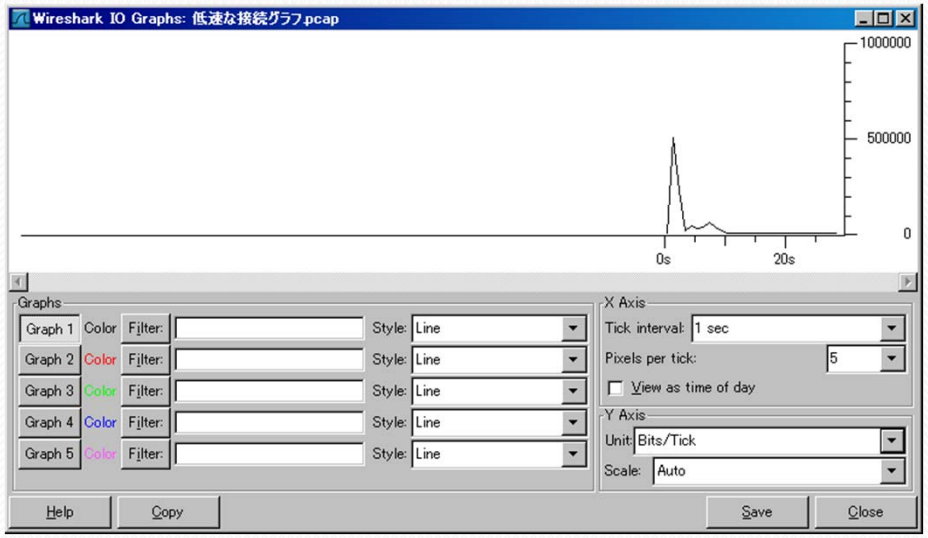




IOグラフは頻度と通信量の2面から

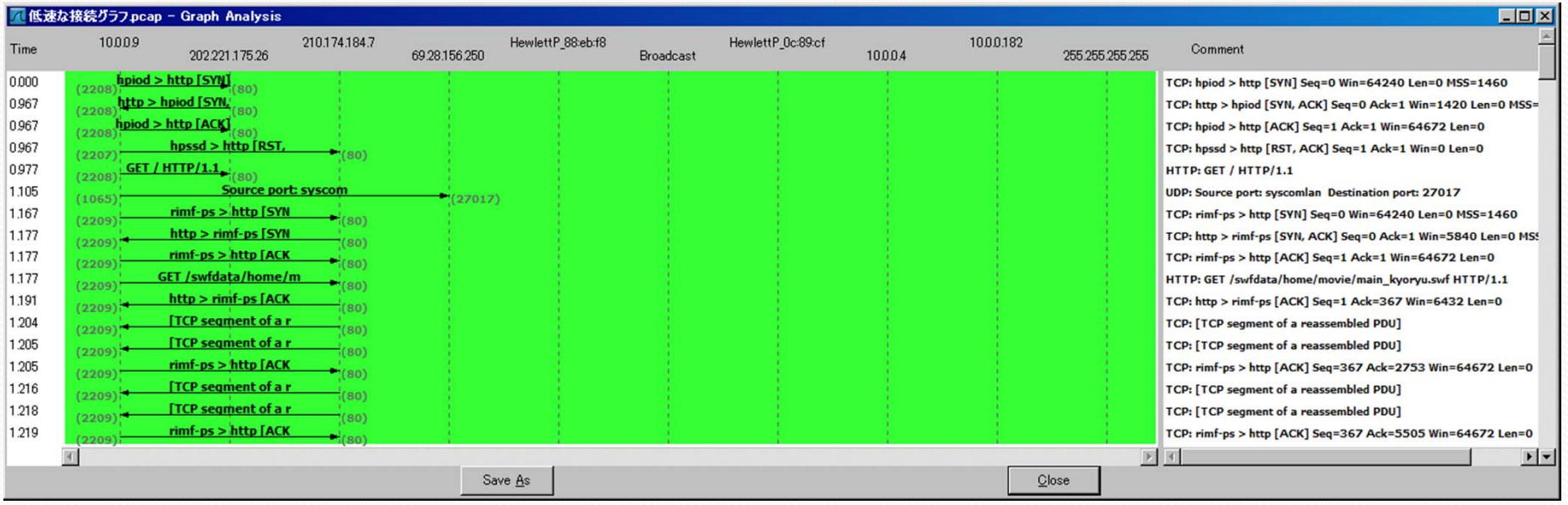
- エラーや再送などはパケット数をY軸にして頻度グラフを作ります。（ヒストグラム形式がおすすめ）
- 通信量はビット数をY軸にX軸を秒にしてbpsグラフを作ります。（線グラフなどがおすすめ）





シーケンスを追いかけるにはFlowGraphを

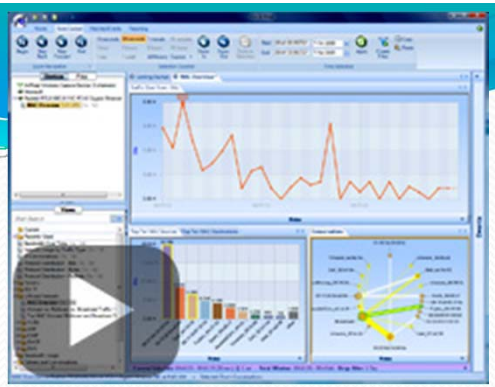
- 通信のやりとりを追いかけるにはStatistics>FlowGraph
- 横にのばすと通信の相手がよく分かります。
- TCPのフラグに注視する場合にはTCP Graphを選択



2：CACE Pilotによる分析・調査

トピック
2－1：CACE Pilotの紹介
2－2：CACE PilotのFAQ
2－3：CACE Pilotのインストールと起動
2－4：インタフェース・pcapファイルの設定
2－5：Viewの適用・カスタムViewの作成
2－6：Drill DownとWiresharkとの連携
2－7：Time Controlの設定
2－8：レポートの出力と保存
2－9：Watchの作成と適用

CACE Pilotとは



- **Wiresharkからわかりやすい図版やレポートを！**

  CACE Pilotは非常に可視化された強力な有線、無線ネットワークのアナライザです。CACE PilotはWiresharkの利用を革命的に変えて、Wiresharkだけでは分からなかった可能性を提供します。CACE PilotはWiresharkと完全統合しており、既存のWiresharkでの分析を革命的に変えて、ネットワークの問題を調べたり、セキュリティの問題を明らかにする際に非常に効果的に活用できます。たとえば、左のビデオのように、数ギガバイトのパケットキャプチャファイルから、Webサーバーの遅延の原因を特定することができます。

- **CACE Pilotでできること**
  - 数ギガバイトのパケットキャプチャファイルを素早く開けて分析できます。
  - Viewという概念を用いて、大量のトラフィックから、目的のトラフィックを簡単に抽出して図表を簡単に作成できます。
  - 現在取得中のキャプチャであっても、取得済みのパケットキャプチャファイルであっても、時間を表すタイムラインをドラッグすることで、大量のデータからその時間の特定のトラフィックを数クリックで簡単に抽出できます。
  - ベースラインに応じて、Watchという概念を用いて、トリガによる警告を作成して長時間のトラフィックをモニターできます。
  - 独自のViewを作成することで、セキュリティのコントロールやネットワークの調査で使える図表を作成することができます。
  - Wiresharkのパケットキャプチャフィルタや表示フィルタを生かしてCACE Pilotを用いてより深い分析を行うことができます。

CACE Pilotの機能（1）

- Wiresharkと一緒に使う
  CACE PilotはWiresharkとともに用いるWiresharkと完全統合された唯一の分析ツールです。Wiresharkでは、とっても大きなファイルを開いて必要な情報を収集するのはとても大変です。でも、CACE Pilotに最適化された分析エンジンを用いることで、必要なトラフィックをすぐに抽出して、図表を作成することができます。
- ビュー（View）機能：柔軟性のある分析と可視化の機能
  CACE Pilotは、トラブルシューティングの要望にこたえる対話型のビュー（ビューとはキャプチャファイルから図表を作る概念です）を多数用意しています。ビューの一例には、以下のようなものがあります。
  - ・IEEE802.11無線LAN用のView。無線APの探知、帯域、チャンネルの利用状況、再送、信号やノイズなど。
  - ・LANやネットワークのトラブルシューティング用のView。MACアドレスやVLAN、ARP、ICMP、DHCPやDNSなど。
  - ・帯域の利用状況のView。MicroBurstsやIP、TCP、HTTP（詳細）、VoIPなど。
  - ・パケットの送受信状況や送受信の相手のマトリクス的View。IPやサブネット、国、TCP、WebおよびVoIPなど。
  - ・パフォーマンスとエラーのView。IPやTCP、WebやVoIPなど。
  - ・利用者の活動状況のView。WebやVoIPなど。
- 図表（Charts）機能：ダイナミックに表示が変更されます。
  CACE Pilotは棒グラフ、パイチャート、ヒストグラム、リング状の対話状況（マトリクス）、とぎれたグラフ、そして、表形式のチャートを自由に作成して、表示、保存、印刷することができます。これらの図表は動的に取得したパケットやタイムラインの変更に応じて動的に変更されます。
- ドリルダウン（Drill-Down）機能：革新的な詳細の分析ができます。
  Drill-Downは、CACE Pilot独自の強力な機能のひとつです。Drill-Down機能によって、ビューをみて、問題があれば、その時刻を動的に絞ったり、そのプロトコルやアドレスやポートなどを絞ったり、任意のフィルターを作成して絞ったりできます。これらは最終的にWiresharkを表示して1つ1つのパケットのダンプまで確認することができます。この強力なDrill-Down機能により、問題解決。が容易になります。巨大なパケットキャプチャファイルを分析する際においても、Drill-Down機能をもちいて、速やかに問題のあるネットワークの動きを見つけて詳細化することができます。

CACE Pilotの機能（2）

- **時間調節（Time Control）機能：巨大なPcapの時間をさっと抽出**
  丸一日分や数週間分、ましてや数ヶ月ものパケットキャプチャファイルでトラフィックを調べるのはかなり大変ですよね。でも、CACE Pilotの時間を戻ったり、進めたりする機能を使えば、簡単に、特定の期間のパケットをすぐに見ることができます。時間調整機能は、選択した期間に基づいて、パケットキャプチャファイルのサンプルをとり、データを集約、最適化して、すぐに統計や図表を作成することができます。時間を戻る機能は、過去のpcapファイルだけでなく、現在取得しているパケットに対しても実行することができます。
- **ウォッチトリガー（Watches）機能：**Wiresharkでトリガーができます。
  CACE Pilotは「Watch」と呼ばれる洗練されたトリガーおよびアラート技術をもっています。パケットキャプチャを長時間どんどん過去のものを捨てながらキャプチャをしていて、問題が発生したときに、管理者にメールを送ったり、パケットキャプチャを開始したいことがありますよね。Watch機能では、何か特定の問題が発生した際に、パケットキャプチャファイルから自由に作成したトリガー条件をもとに、アラートを行えます。たとえば、高い帯域利用率や、遅いサーバーの応答時間や、長いTCPの往復遅延時間などでアラートを作成できます。
  Watch機能によって、トリガー条件が一致すると、指定した動作を実行できます。動作としては、ログをとったり、メールを送ったり、キャプチャを行うなどがあります。
- **レポート（Reporting）機能：優れた報告書を作成できます。**
  CACE Pilotは、作成したViewをもとに、図表を含めた分かりやすい報告書を作成することができます。業務や監査に利用できるレベルの報告書を作成して、PDFやMS-Word、Excel形式などにエクスポートして活用できます。
- AirPcap対応：無線LANネットワークも調査できます。
  CACE PilotはAirPcapシリーズといっしょに使うこともできます。CACE Pilotには、802.11用のViewも用意されているので、直接無線LANネットワークとの比較や調査を行うことができます。
  CACE社のAirPcapシリーズと完全に統合されているので、Pilotを使えば業務において、ノートPCを使って現場で全チャンネルのパケットキャプチャをとったり、トラブルシューティングを行ったり、WPA/WPA2（事前共有鍵）の暗号解除を行ったりできます！

価格とライセンス形態

- CACE Pilot はもともと1年のソフトウエア更新および保守契約が付帯しておりますが、新しいバージョンの利用やViewの追加をはじめ、2年目以降の保守契約をおすすめしております。

- CACE Pilot + 12 カ月のソフトウエア保守付属 $1295 USD
- CACE Pilot + AirPcap Ex Adapter + 12 カ月のソフトウエア保守 $1743 USD
- CACE Pilot + AirPcap Ex 3-Pack + 12 カ月のソフトウエア保守 $2640 USD
- CACE Pilot + AirPcap Nx Adapter + 12 カ月のソフトウエア保守 $1923 USD
- CACE Pilot + AirPcap Nx 3-Pack + 12 カ月のソフトウエア保守　$3180 USD
- ソフトウエアの更新契約　CACE Pilot 1年間のソフトウエア更新　$300 USD

- 日本国内においては、いけりり★ネットワークサービス(株)におまかせください！

CACE PilotのFAQ（1）

- CACE Pilotって何？
  グラフィカルな操作で、Wiresharkと統合されたネットワークの分析・調査・統計・報告ツールです。特にWiresharkの苦手とするような統計・分析・報告を簡単に行うことができます。
- CACE Pilotのシステム要件は？
  OS: Windows XP, Windows Vista, and Windows 7 (32 and 64 bit)
  CPU：dual-core 2.0 GHz以上　メモリ：2 GB RAM
  ※.NetFrameworkiで描画しているので、とにかくCPUが早いと快適です。
  HDD：300MB 以上
  ※レポートファイルは小さいですが、特にパケットキャプチャファイルの容量に気をつけてください。実際には、キャプチャを保存する数10－数百ギガのディスクが必須と思います。
  画面解像度：1024 x 768以上
  ※たくさんのViewなどを快適に操作するためにも、こちらも大きいサイズをおすすめします。
- CACE Pilotを別のマシンにインストールしてライセンスを移動するには？
  プログラムの追加と削除から行うことで、アクティベーションが解除され、プロダクトキーを別のマシンに適用できるようになります。
  ※ハードウエア構成を大きく変える（HDD等）でも別インストールと見なされることがあります。その場合はいったん削除して再インストールすればOKです。それでもだめならUSにお願いして、強制的にアクティベーションを解除してもらい、再度インストールになります。
- CACE PilotはWindows7に対応している？
  はい。バージョン2．4で32ビットおよび64ビット版に対応しており、日本語OSで実績あります。

CACE PilotのFAQ（2）

- CACE Pilotは一般の無線LANカードに対応していますか？
  AirPcapでないと、他のチャンネルのパケットの取得（モニターモード）ができないため、一般的な無線LANカードは使うことができません。
- マシンがクラッシュして、Pilotを再インストールする際には？
  CACE社のサポートページにフォームがあり、こちらからプロダクトキーに対して、追加のアクティベーション（通常は2個）を行うことができます。
- Wiresharkで開けるSnifferのファイルがCACE Pilotで開けないのは何故？
  CACE Pilotでは、現在pcapファイルのみ開けます。そのため、一度Wiresharkでそのファイルを開いてPcap形式（libpcap）で保存するか、“¥Program Files¥Wireshark¥”以下にある、editcapなどのコマンドで変換する必要があります。
- レポートの表紙を変更するにはどうするの？
  レポートリボンより、セッティングタブの中で、レポートの題名や顧客名、その他情報を追加できます。
- CACE Pilotのレポートで独自のスタイルシートを利用できますか？
  現在、CACE Pilotには5つのスタイルシートが準備されていますが、もし、自社のスタイルシートやデザインがあれば、「 C:¥Program Files¥CACE Technologies¥CACE Pilot 」以下に、Pilot.Client.configというXMLファイルがあり、こちらのファイルの「styles」を編集して対処できます。
- CACE Pilotのレポートに注釈をつけることができますか？
  レポートを作成した際に、チャートの下をクリックして、テキストを入力して注記を行えます。

CACE PilotのFAQ（3）

- たくさんのネットワークの保守に1ライセンスのCACE Pilotを用いて調査できますか？
  （マシンを必要なときに、つなぎ替えたり、Wiresharkのpcapファイルを読ませるなど）
  CACE Pilotは1購入あたり、シングルシートライセンスとなっており、インストールしたマシンで動作させることができます。そのため、このような使い方も大丈夫です。
  ※複数ポートのNICを用いたり、VLANごとのパケットをWiresharkでとって、分析マシンにCACE Pilotをインストールするとよいです。もちろん、現場のノートPCにインストールしているととても便利です。
  さらに、現在、PilotコンソールとSMDSという構成を用いて、クライアントサーバー型（Webブラウザ等）でPilotを利用する製品もあります。
- Linux/UNIXマシンの発見にCACE Pilotを用いることはできますか？
  CACE Pilotは端末の検出ツールではありませんが、LANアナライザのように用いて通信している端末を見つけることができます。
- ビデオや音声の分析をCACE Pilotで行うことができますか？
  現在、CACE PilotはIPの通信状況の分析が中心ですが、VoIPのタブやViewを用いて、分析や調査を行うことができます。
- カスタマイズではなく、独自のViewを作成してCACE Pilotに実装できますか？
  現在は不可能ですが、もし、特定のViewを作成したいのでしたら、要望をお教えください。開発の際に考慮いたします。

CACE PilotのFAQ（4）

- 特定のプロトコルやアプリケーションのデータごとに、2値以上の項目でCACE Pilotの分析を行うことができますか？
  「Data Bandwidth over Time」のViewでは、TCPとUDPを2つに分けてそれぞれでチャートを作成できます。「Bandwidth over Time」では、1－4つのプロトコルに分けて分析できます。
- CACE Pilotでアプリケーションのフレームをみるにはどうしたらよいですか？
  アプリケーションを特定するフィルタを作成して、1つのViewを適用します。（例：「Bandwidth over Time」等
- 右クリックして、コンテキストメニューを出そうとすると、Wiresharkで以下のようなエラーが発生します。
  1：「Unexpected error from select: No error 」 2：Wiresharkに何もパケットがない。
  3：コマンドプロンプトが開いて、以下のエラーメッセージを繰り返します。
  “(wireshark.exe:2560): Gtk-CRITICAL **gtk_widget_hide: assertion ‘GTK_IS_WIDGET (widget)’ failed… ”
  CACE Pilotでドラッグしたり、右クリックしたりして、フィルタを適用する際には、2種類のフィルタが存在します。
  1： BPF (キャプチャドライバでフィルタします)：高速ですが、詳細な抽出ができません。例：“net 10.20.172.0 mask 255.255.255.0”;
  2：Wiresharkの表示フィルタ：低速ですが、多彩な機能があります。（これが動作する際には、Wiresharkのエンジンが一度起動する必要があります。） 例：“ip.addr == 10.20.172.0/24”
  この場合には、1のBPFを用いてください。

CACE PilotのFAQ（5）

- Pilotの更新時間を1秒以下に変更できますか？すべてのViewの表示はミリ秒やマイクロ秒などWireshark同様にTimeDisplayFormatで指定しますが、データの更新間隔は1秒です。
  現在では、CACE Pilotの最小の更新時間は1秒です。これ以上小さくするとCPUのリフレッシュ時間がきわめて高いため、現在のバージョンでは制限しています。
- CACE Pilotで1秒以上の更新タイミングを計測して計算できますか？平均はどのようにして計算されますか？
  Viewに依存しますが、通常は更新間隔の平均になります。
- CACE Pilotで信号ノイズ比のViewを作成できますか？
  はい。「802.11 Over Time」のView以下を参照ください。
- サブネットのフィルタを作成するにはどうしたらよいですか？
  1：Viewを適用している際にCtrlを押して、フィルタパネルを出します。
  2：「New」をクリックして、新規にフィルタを作成します。
  3：“Wireshark Capture Filter (BPF)”を選択します。
  4：“net 192.168.1.0 mask 255.255.255.0”（複数あるのなら、“(net 192.168.1.0 mask 255.255.255.0) or (net 192.168.2.0 mask 255.255.255.0)”）のように入力します。
- カスタムViewより、新規にフィルタを作成できますか？
  Viewを適用したら、Ctrlを押して、もしくは右クリックして、「apply with filter」のコンテキストメニューより、フィルタパネルを出します。そして、1つの定義済みフィルタを選ぶか、Wiresharkの表示フィルタやキャプチャフィルタを適用してください。

CACE PilotのFAQ（6）

- 独自のグラフィカルな概要画面を作って、特定のフィルタに結びつけられますか。もしくは少なくとも、定義済みのグラフィカルな概要画面がありますか？
  フィルタを「Overview」のViewにAttachしてください。
- CACE Pilotは仮想環境をサポートしていますか？
  はい、VMWareの仮想環境で動作している実績があります。
- WiresharkとCACE PilotをT1回線の分析に用いたいと思います。MGCPとSIPのトラフィックをチャネル化されていないT1回線で使っていますが、T1回線のキャプチャはどうしたらいいですか？
  Endace社のDAG Ca4rdを用いるか、GL社のUSBのキャプチャボックスを用いてください。
  http://www.endace.com/our-products/dag-network-monitoring-cards/pdh-tdm
  http://www.gl.com/laptopt1.html
  もし、Ciswcoの機器のIPトラフィックのみなら、Cisco IP Traffic Exportも利用できます。
  http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_rawip.html
- 無線LANカードの送信速度やRSSIの値でグラフを作れますか？
  はい。802.11のViewで対応可能です。
- CACE Pilotでは、WiresharkのすべてのDissectorsに対応していますか？また、Viewそのものをカスタマイズできますか？
  WiresharkのDissectorについては、表示フィルタできるものに関しては、すべてサポートしています。また、順次追加されるDissectorについても、新しいバージョンで対応を行っていきます。
- チャンネルごとにWifi機器の適用しているデータ速度をできる限りパケットを失わずに調べたいと思います。CACE Pilotでは、再送の回数を全体に対する%で表示できますか？
  RetransmissionのViewで対応できます。

CACE PilotのFAQ（7）

- 「TCP Retransmission Timeout Over Time」のViewで、再送の回数でなくて、再送がミリ秒で表示されるのはなぜですか？
  図表では、平均的な再送タイムアウト時間を表示しています。具体的には、1つのセグメントが再送される前に、TCPの再送がどれだけおくれたかを示す時刻の値になります。もし、再送の回数を求めるのなら、「 Transport¥TCP¥Wireshark TCP Metrics 」のViewを用いてください。こちらでは、「 Suspected TCP Retransmissions 」Viewを選択できます。また、「 Bandwidth over Time 」Viewにドリルダウンできます。端末ごとなら「IP Conversations」Viewを用いることができます。
- 「TCP Round Trip Time over Time」 Viewをもちいると、2件しかありませんでした。そして、Y軸を小さな値にすると、何も表示されなくなりました。どうしてですか？
  時間毎のRTOのViewでは、TCPセグメントに対して、対応するACKが帰ったときの時点をもとに、グラフを作成します。そのため、参照点が少ない場合には、件数が減ります。また、特定の値が大きいとグラフの形状は変わります。この場合には、Ctrlキーと、マウスの車輪を使ってズームを調整してください。
- 同一のポートをHTTPとして用いて、たくさんの通信が発生している場合に区別はできますか？
  パケット分析を行う際、CACE Pilotでは、IPやポートで通信を識別します。この際、Youtubeやビデオストリームやファイル転送や、チャットやIMをしているような場合、アプリケーション毎に分類するのは少し困難です。特定の表示フィルタなどを適用できる場合もありますが、DPI（Deep Packet Inspection）を必要とする場合もあります。今後、HTTPのアプリケーション毎の統計を計画しています。

CACE PilotのFAQ（8）

- Linuxでインタフェースに「any」を指定しているpcapファイルをうまく開けません。
  Libpcapにおいて、Linuxでanyを指定すると、PPI（per packet information）に日得るDLT情報を含んだSLLヘッダーをパケットごとにつける場合があります。SLLは、wiki.wireshark.org/SLL.に説明があり、libpcapの“sll.h”が利用されますが、CACE Pilotでは、現在SLLのパケットをサポートしてません。この場合には、editcapなどのツールで通常のpcapファイルに変換してください。
  例：editcap -T ether sll.pcap ether.pcap
- Pcapファイルを取得しようとすると「Microsoft Visual C++ Runtime Library] This application has requested the Runtime to terminate it in an unusual way. Please contact the application‘s support team for more information.」のようなエラーが出ます。
  Wiresharkを使わずに、dupcapやwindumpを使ってパケットをとってみてください。
- VOIPなどでのMOSを計算するViewはありますか？
  話者毎のRTPストリームのMOS値は「Performance and Errors¥VoIP¥Call Quality MOS¥VoIP Call Summary – MOS」のViewで計算できます。
- CACE PilotとWiresharkは何番ポートで通信を行いますか？
  CACE PilotはTCPの61898／61899番ポートでWiresharkと通信を行います。クライアントは任意のポートを用います。

CACE PilotのFAQ（9）

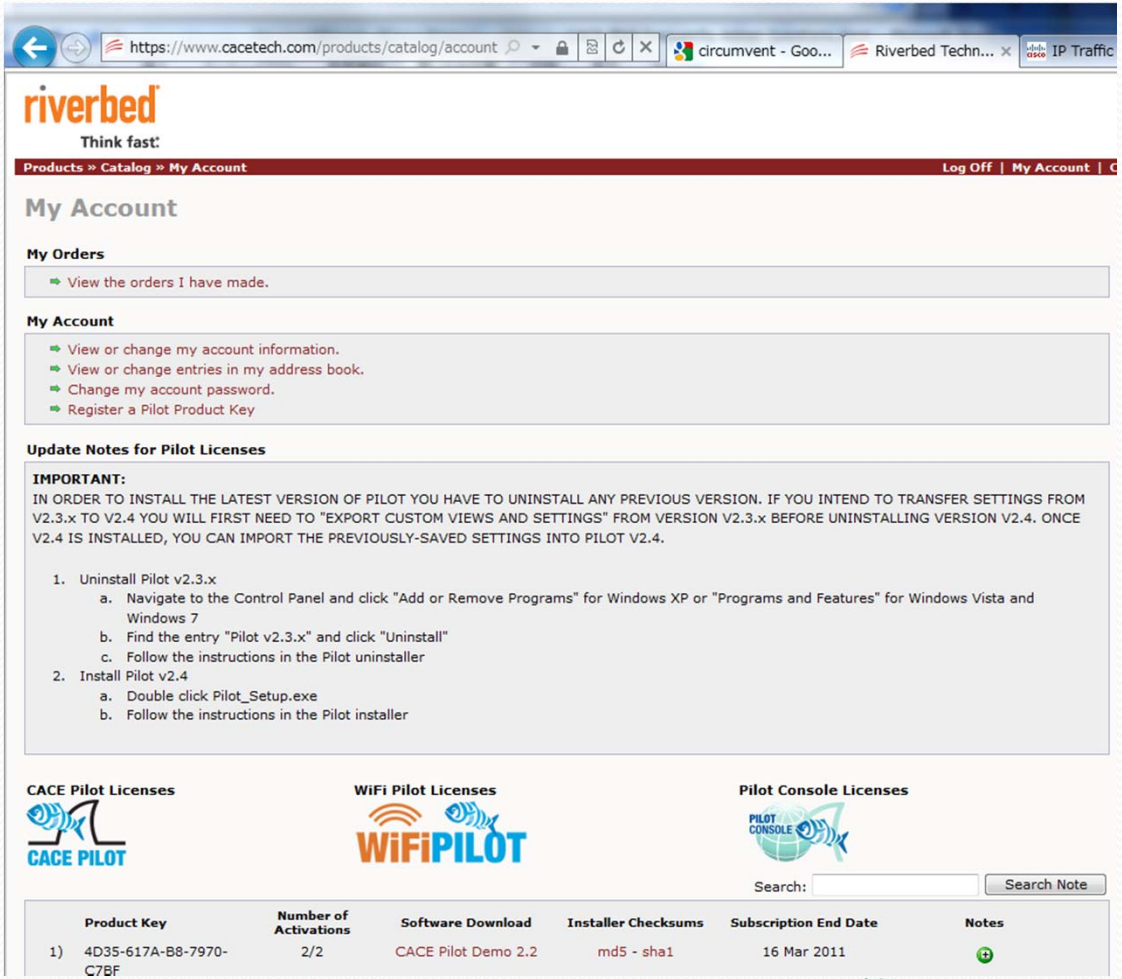
- 任意の80番ポート以外をHTTPとして解析するにはどうしたらよいですか？Wiresharkでは、サブメニューの「Decode As」を用いて、イントラネットの特定のポートをHTTPとして解析できます。同様のことをPilotでも行うことができますか？
  “[Pilotをインストールしたフォルダ以下]¥server¥configuration”にある、proto-groupsファイルを編集してください。
  # Web
  Web 80/tcp HTTP
  Web 8080/tcp HTTP
  Web 443/tcp HTTPS
  たとえば、HTTPを8050でもデコードしたい場合には以下の部分を追加します。
  Web 8050/tcp CustomHTTP
- CACE Pilotでレイヤ2の分析を行うことができますか？
  「LAN and Network」フォルダ以下のViewにたくさんのサンプルが用意されています。
- CACE Pilotでpcapファイルをインポートする際に、「Unsupported link type (raw 802.11)」と表示されます。
  現在、CACE PilotはFCSを含んでいるかどうか知る必要があるためRaw 802.11パケットをサポートすることができません。（※Wiresharkエンジンでデコードするための問題と思われます。）PilotはRadiotapヘッダ（AirPcapシリーズほか）やPPIリンクヘッダー（AirPcapNX等）の物理層情報のついたパケットをサポートしています。これらの情報にはFCSを含んでいるかの情報が含まれます。

CACE PilotのFAQ（10）

- 「All Requested Web Objects」や「Web Conversations」のようなViewを表示しようとすると、「Too many rows! Only 1000 loaded. Data is not complete!」のような警告が表示されます。
  Viewに対して、「Grid Control」を用いるViewでは、エントリ数の限界があります。そのため、「 Bandwidth Over Time」のようなViewを用いてください。
- CACE Pilotをプロミスキャスモードで動作させず、パケットを取得しないようにして、純粋にpcapファイルの分析だけをしたいと思います。WinPcapを削除するとPilotも動かなくなります。
  以下のファイルを手動で削除することで対処できます。
  c:¥Program Files¥CACE Technologies¥CACE Pilot¥server¥plugins¥inputs¥InputPcapAdapter.dll
- Endace DAG Capture file (extensible record format or ERF) がうまく動きません。
  CACE Pilotにおいて、ERFファイルは一部のみサポートされています。
- 別の時刻帯のパケットを受け取った場合はどうなりますか？
  Pilotはインストールした機器の時刻を表示します。また、Wiresharkのコマンドラインツールでpcapファイルの時刻情報を変更して対応できます。
- Windows Server 2008でCACE Pilotは動作しますか？
  ビデオカードに依存します。
- CACE Pilotをダブルクリックしても、なにも起きません。
  CACE Pilot2.3以前は、「Microsoft‘s .NET Framework 4」がインストールされていると問題があります。この場合には、.Net Frameworkの 2.x or 3.xのみインストールしてください。そうしないと、砂時計のアイコンが出て、しばらくして消える問題が発生します。
  対策としては、Pilot2.3.1以上を用いるか、.Net Framework 4をアンインストールします。

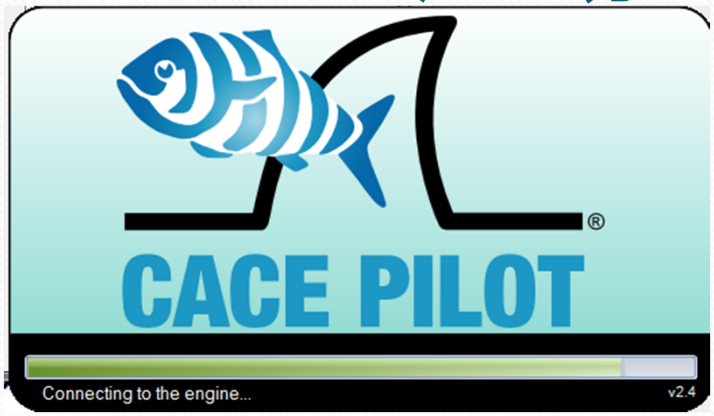
ダウンロードと登録

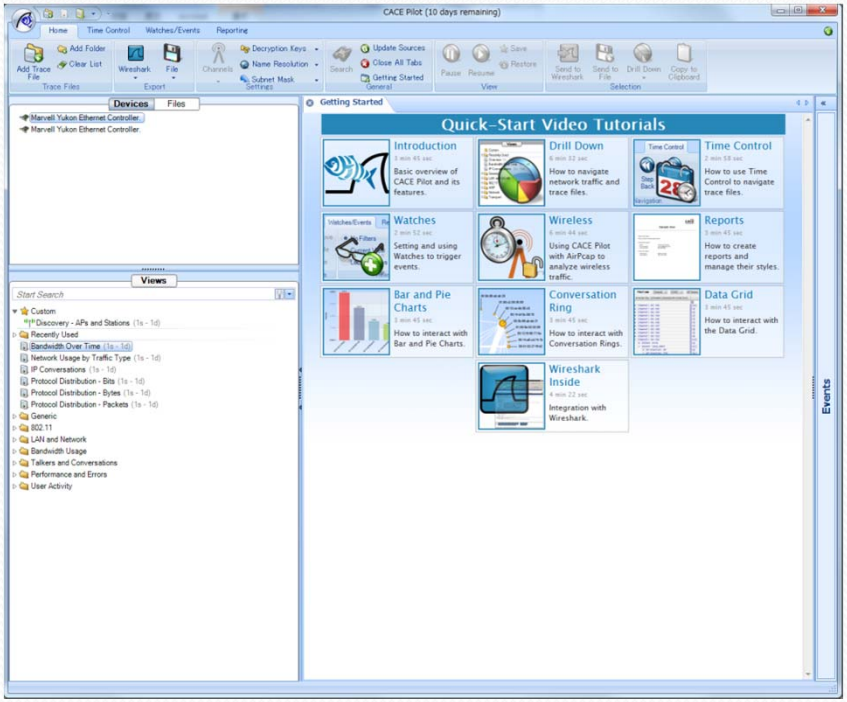
- CACE（Riverbed）社のMyAccountページより、ダウンロード、インストール、アカウント情報の更新ができます。また、Pilotのプロダクトキーの登録を行うことができます。
  https://www.cacetech.com/products/catalog/account.php?



CACE Pilotのインストールと起動

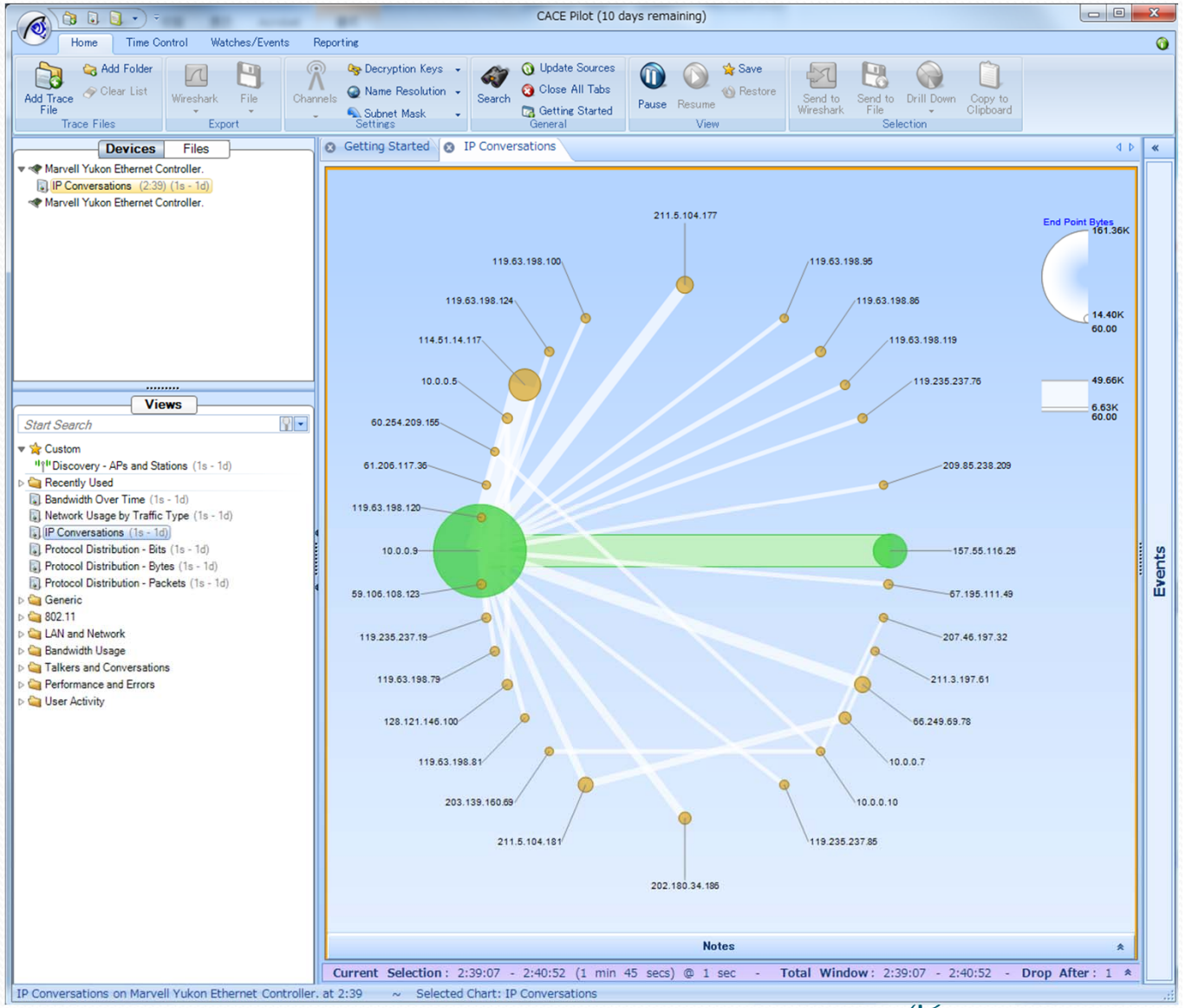
- 削除する際は必ずプログラムの追加と削除から行ってください。
- 各プロダクトキーに対して2つアクティベーションできます。
- 起動しない理由として、.net framework4を旧版では注意してください。（2.3.1以上は問題なし。）
- Wiresharkは対応するバージョンを使います。（同時インストールされます）





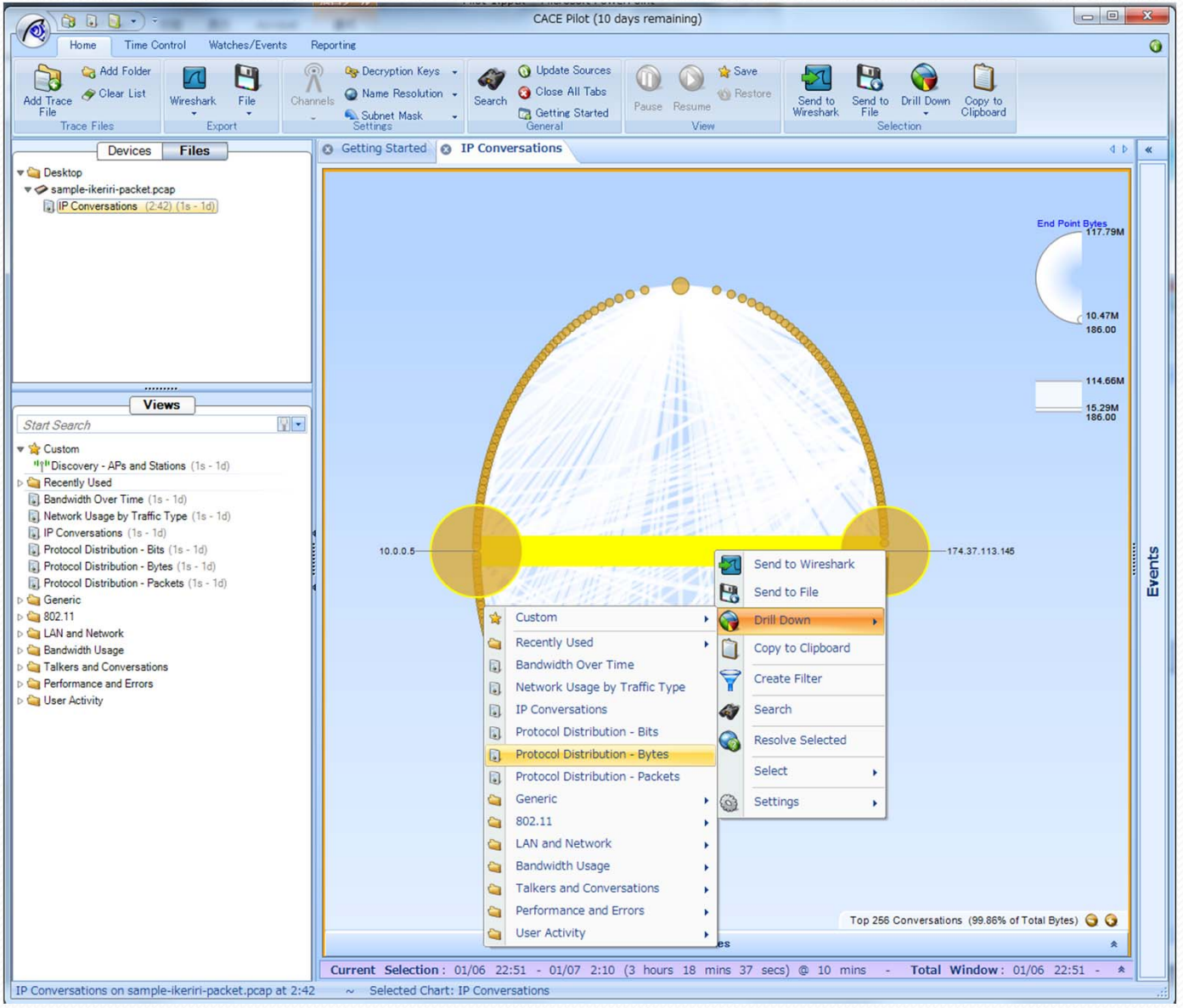
インタフェース・pcapファイルの設定

- Deviceを
  クリックしてから
  Viewにひも付け
  を行います。
- Filesでも同様に
  pcapファイルに
  Viewをひも付け
  していきます。



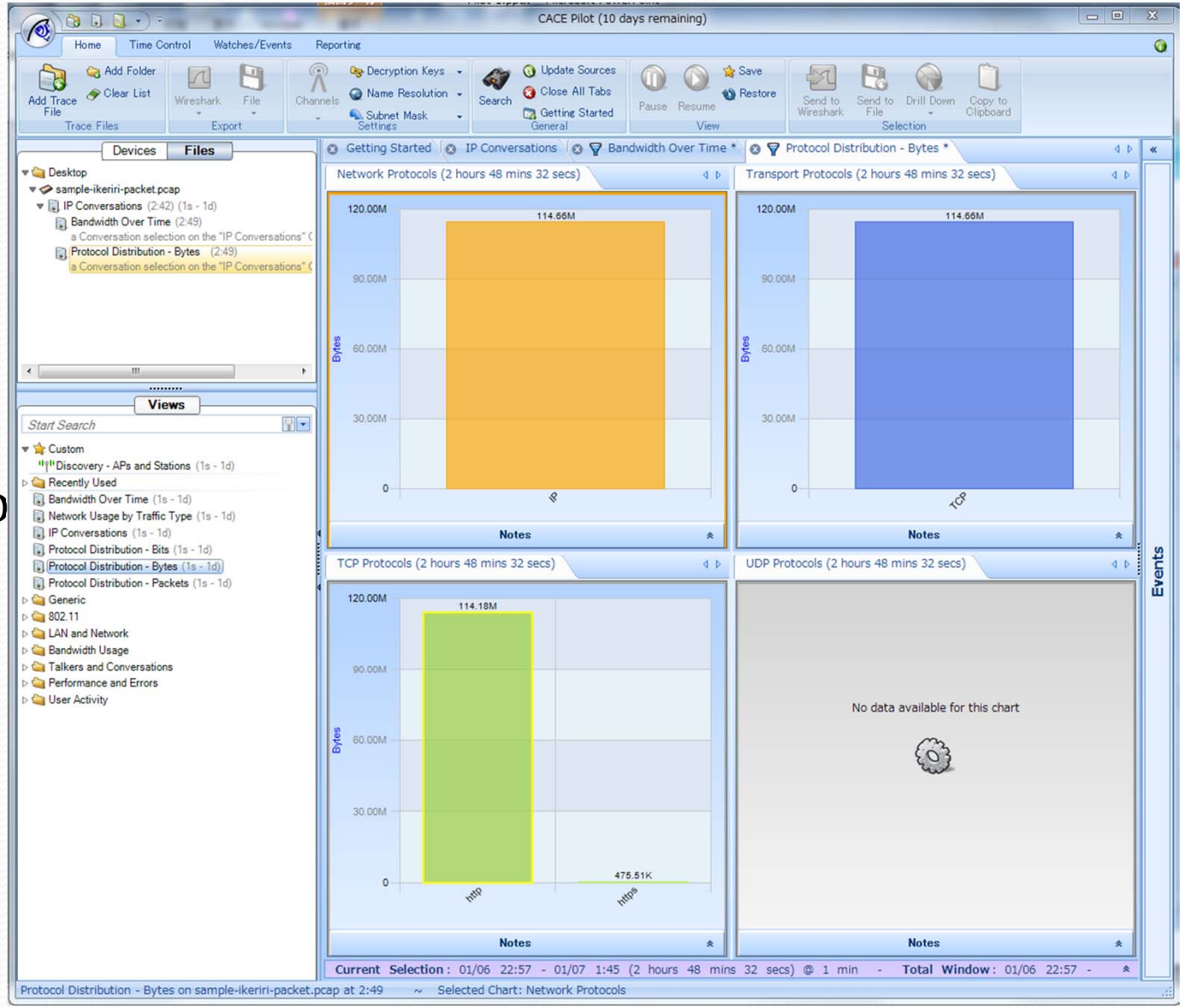
Viewの適用・カスタムViewの作成

- View内部で該当するトラフィックを選択してさらに右クリックして、カスタムViewを作成して分析できます。
※Ctrlでフィルタの適用が行えます。



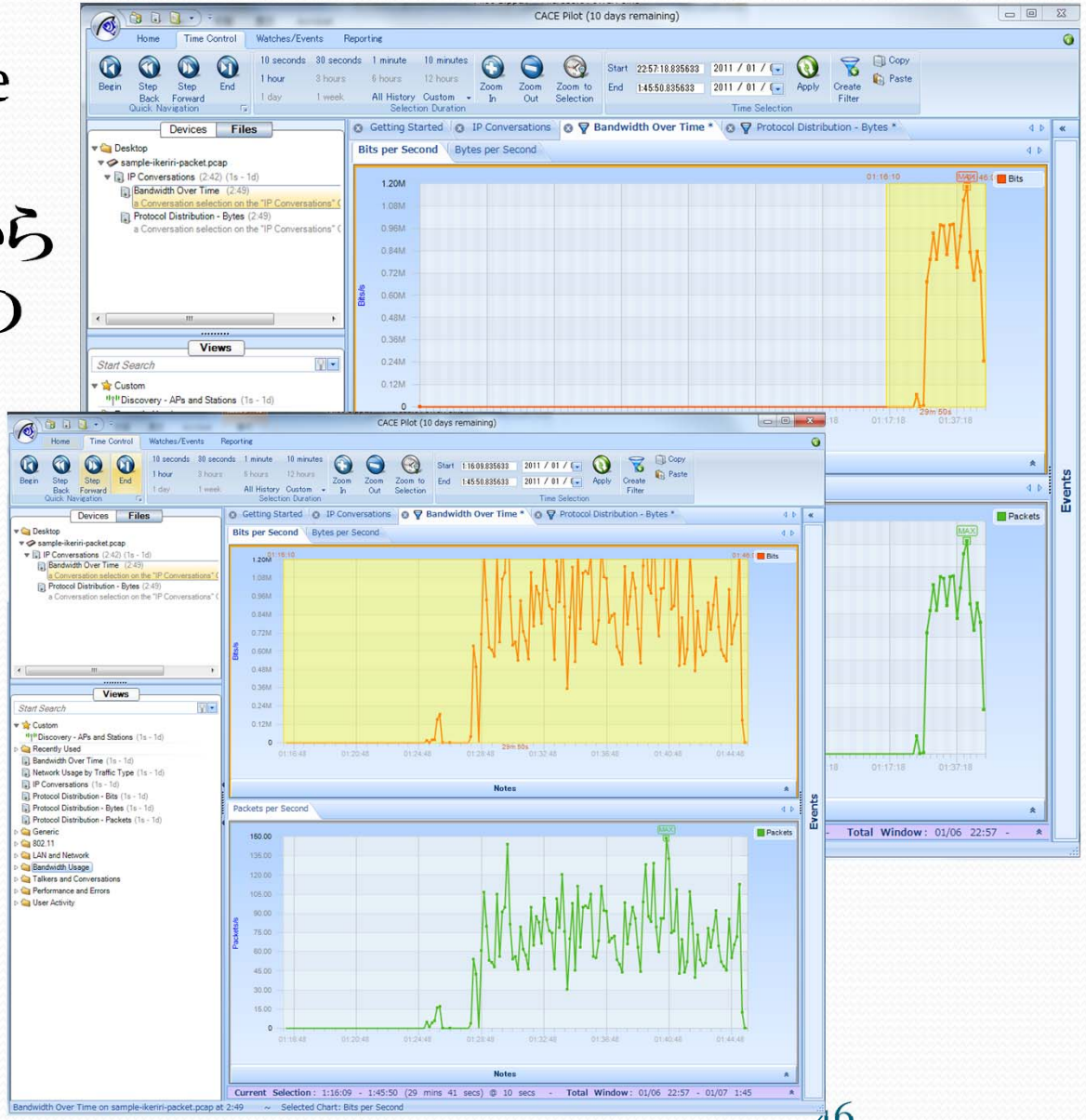
Drill DownとWiresharkとの連携

- Drill Downを組み合わせて目的のトラフィックを多面的に調べることができます。
- また、「Send To Wireshark」でパケット単位の分析を行うことができます。



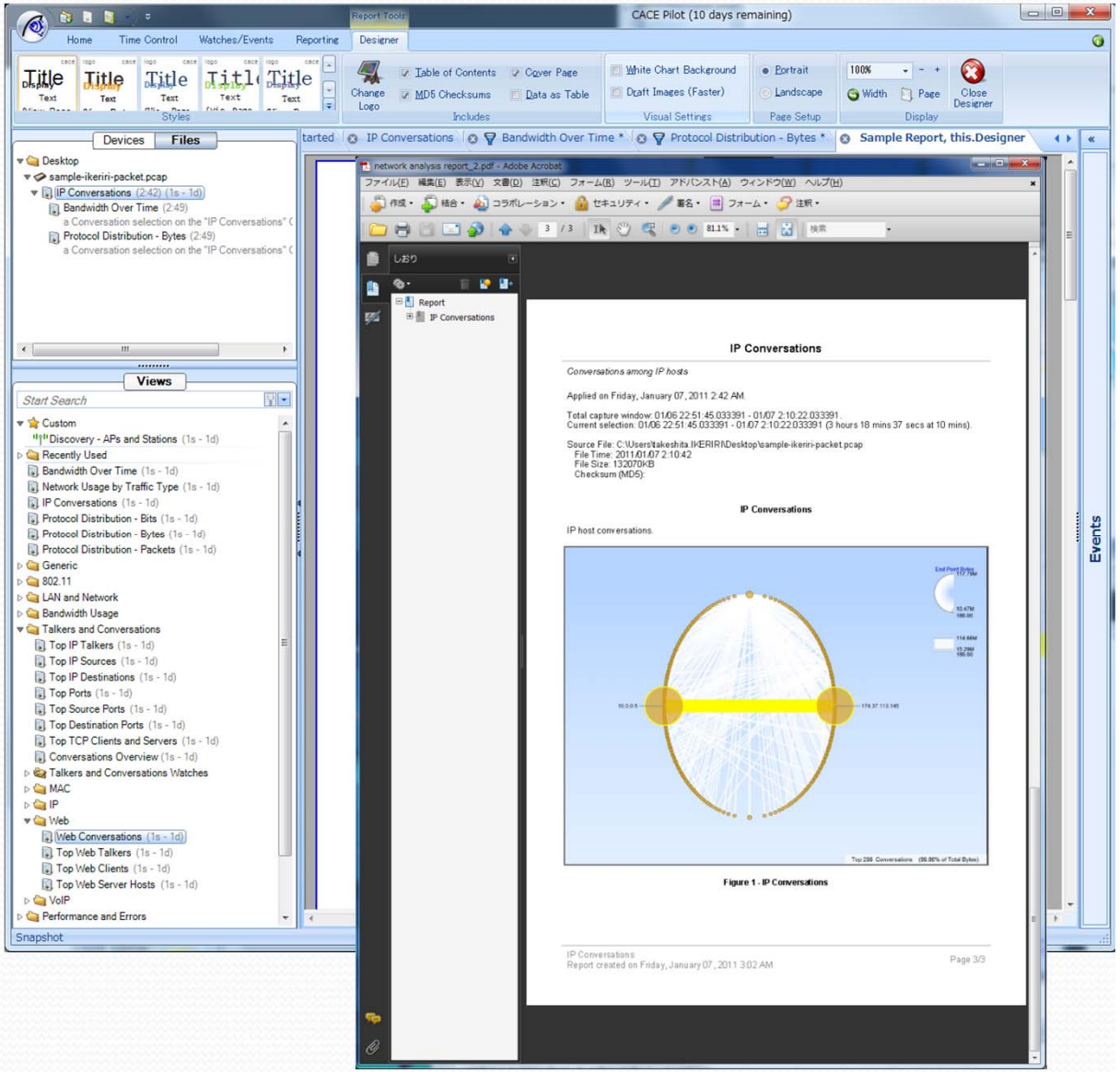
Time Controlの設定

- Bandwidth over TimeなどのViewにおいてTime Controlリボンからマウスクリックで任意の時間を抽出して分析することができます。
- ズームしたり、フィルタを作成したり、後述のWatchを作成したりして、後の調査にも活用できます。



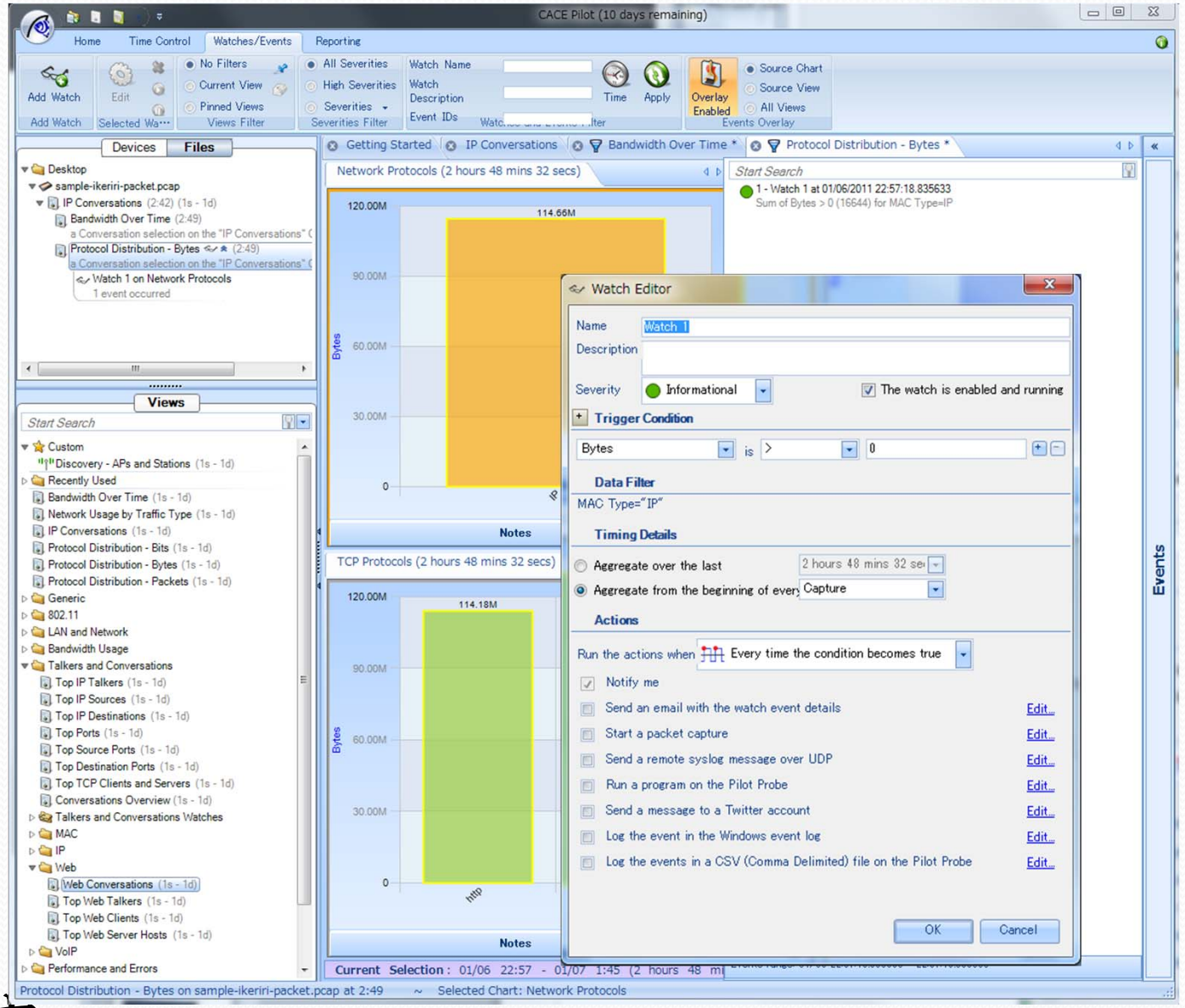
レポートの出力と保存

- Reportリボンより View毎、複数Viewのレポートを作成、出力できます。
- ファイル形式やレイアウトはReportDesignerでカスタマイズできます。



Watchの作成と適用

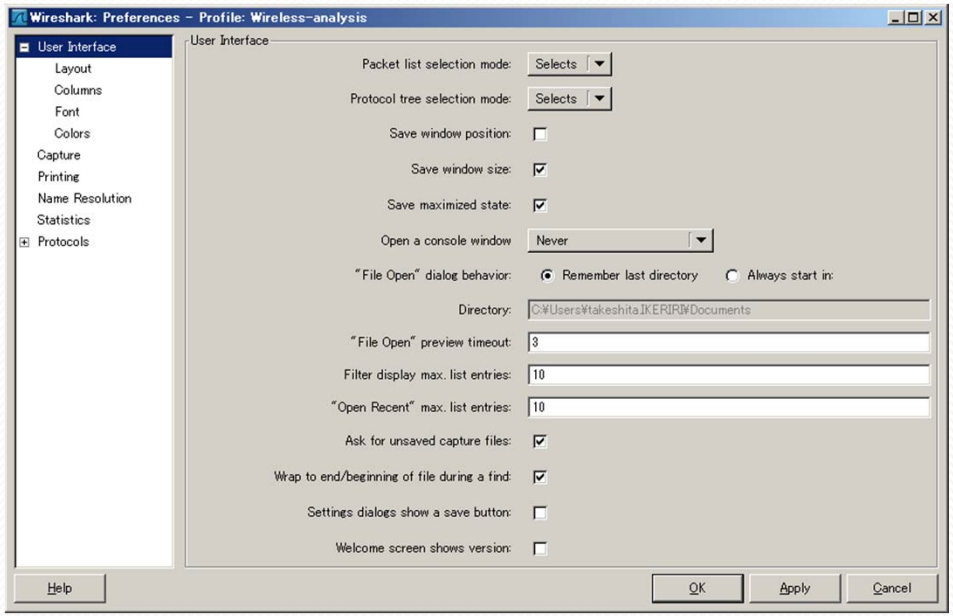
- View等で抽出したトラフィックの時間、内容をもとにトリガを作成して、Watchとして監視できます。
- 該当したパケットはEventsに追加されます。

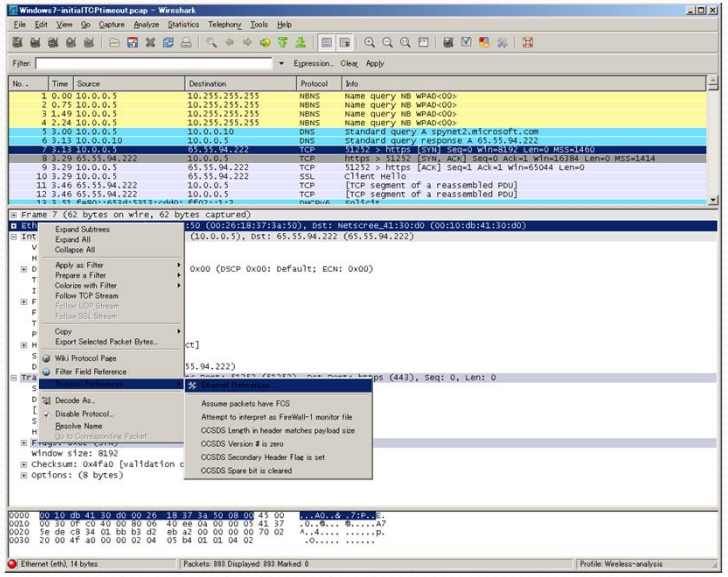


3：Wireshark・Pilot応用（フィルタ）

トピック
3－1：プロファイルの作成と切替
3－2：Wiresharkの設定ファイル
3－3：キャプチャフィルタの利用
3－4：リモートキャプチャ
3－5：エキスパートモード
3－6：ファイルラベル
3－7：遅延に関するフィルタ
3－8：各プロトコル分析のフィルタ
3－9：セキュリティ調査のフィルタ

強力になったWiresharkの設定

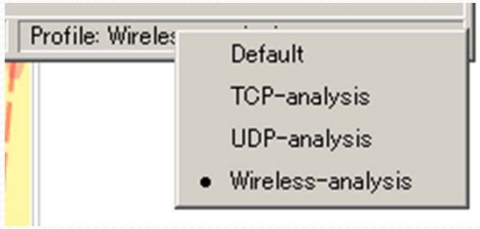


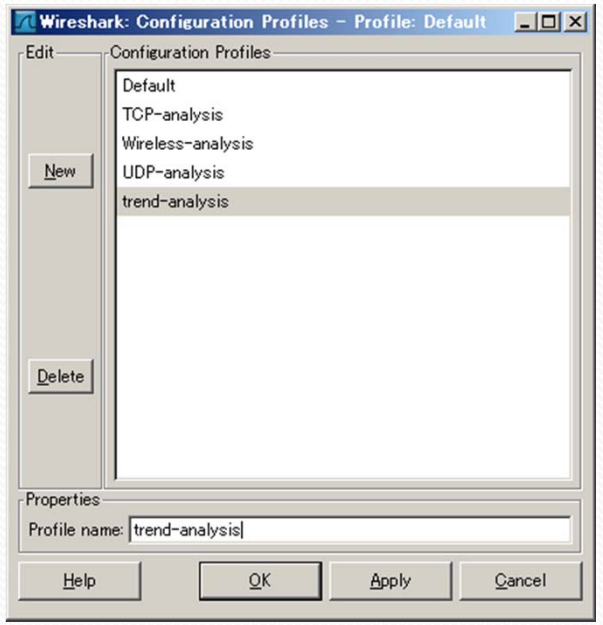


- Ctrl+Alt+Pのほかに、各プロトコルを右クリックしてから、設定を呼び出したり、トグルさせることができます。
- チェックサムエラーを無視させるなど、各プロトコルでよくある設定変更をすぐに行うことができます。

プロファイルの作成と切替

- プロファイル画面（Ctrl+Alt+A）を表示して、分析したい内容に応じてプロファイルを複数準備しましょう。
- プロファイルは画面右下のProfileをクリックして、いつでも切り替えて使うことができます。





Wiresharkの設定ファイル

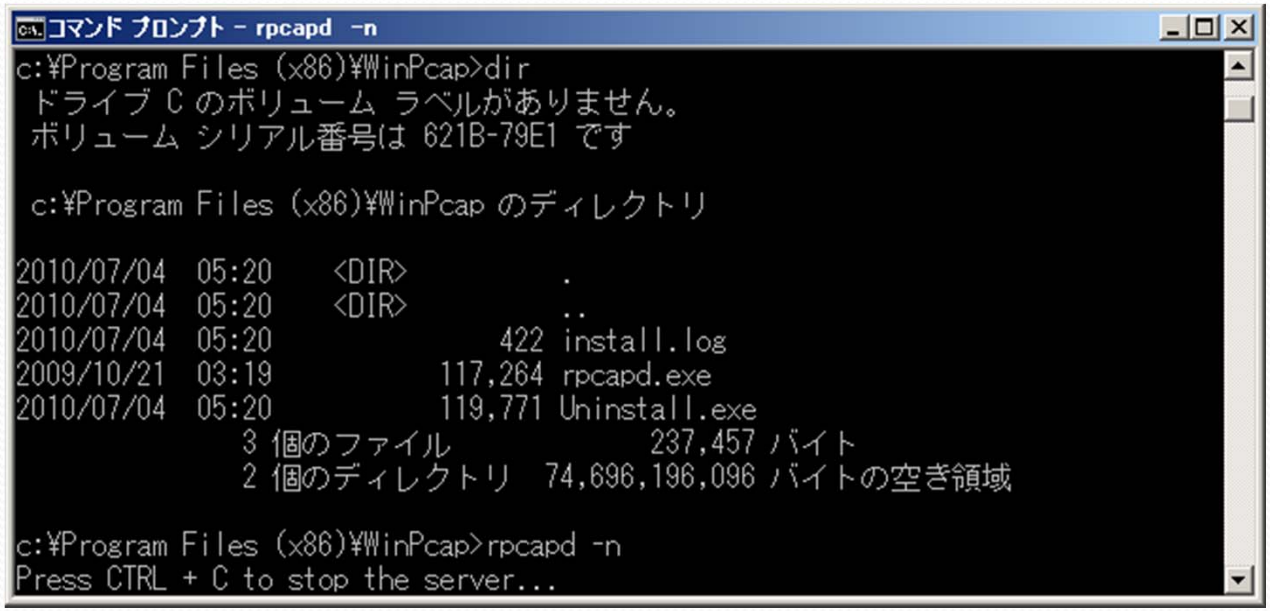
- About Wiresharkより、Foldersを探すと、Wiresharkの設定ファイルの場所が分かります。
- cfilter(テキスト)キャプチャフィルタ
- dfilter(テキスト)表示フィルタ
- hosts (テキスト)ホスト名解決用
- manuf(テキスト)MACアドレス解決用
- colorfilters(テキスト)フィルタ色分け用
- GeoIPフォルダ　すごい！特にEndpoint

キャプチャフィルタの活用

- WinPcap/AirPcap/libpcapでフィルタをかけるのがキャプチャフィルタで、キャプチャサイズをとても小さくできます。
- 書き方が表示フィルタと異なるので注意してください。
  例：ether host 00-90-cc-cc-cc-ccやether proto 0x0800
  not broadcast and not ulticastやip and arp
  host 192.168.1.9など
- キャプチャフィルタではホスト名を使えます。
  具体的には　dst host www.ikeriri.ne.jp のように記述することで、アドレスと同様に名前でフィルタを書けます。
- ネットワークに対するフィルタも書けます。
  net 10/8 やnet 172.16やsrc net 192.168 mask 255.255.255.0
- Wiresharkのインストールされたディレクトリにあるcfiltersを編集することで、フィルタを準備できます。

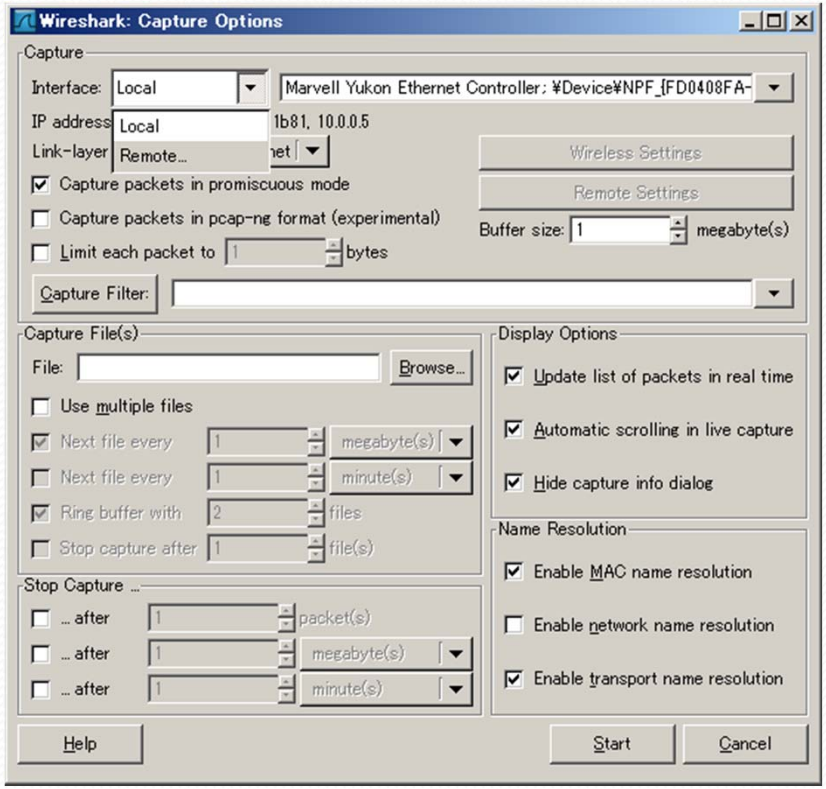
リモートキャプチャー(サーバー側)

- WinPcapのインストールされたディレクトリにrpcapd.exeがあり、これを用いてリモートキャプチャーすることができます。
- rpcapd –nで実行すると、ポート2002番でキャプチャを受け付けます。-lでホスト制限できます。(必要に応じて認証をかけられます。)



リモートキャプチャー（クライアント側）

- キャプチャオプションでインタフェースにRemoteを選ぶと、rpcapdの場所とポート（デフォルト2002）を確認して、パケットキャプチャを行うことができます。



アドレスの解決

- Wiresharkのインストールされたディレクトリにあるmanufファイルを編集することで、MACアドレスを使いやすく解決できます。例： 00:E0:99:11:11:11　MyPC
- Wiresharkのインストールされたディレクトリにあるhostsファイルを編集することで、MACアドレスを使いやすく解決できます。例：192.168.1.1　Router

表示フィルタ

- よく使う表示フィルタはdfilterに登録しておきます。
- Preferenceより最大数を変えておくと便利です。
- フレームに対しても表示フィルタが使えます。
  実践的なフィルタ例として、前のパケットから応答が1秒以上のパケットは frame.time_delta_displayed>1

引数付き表示フィルタ

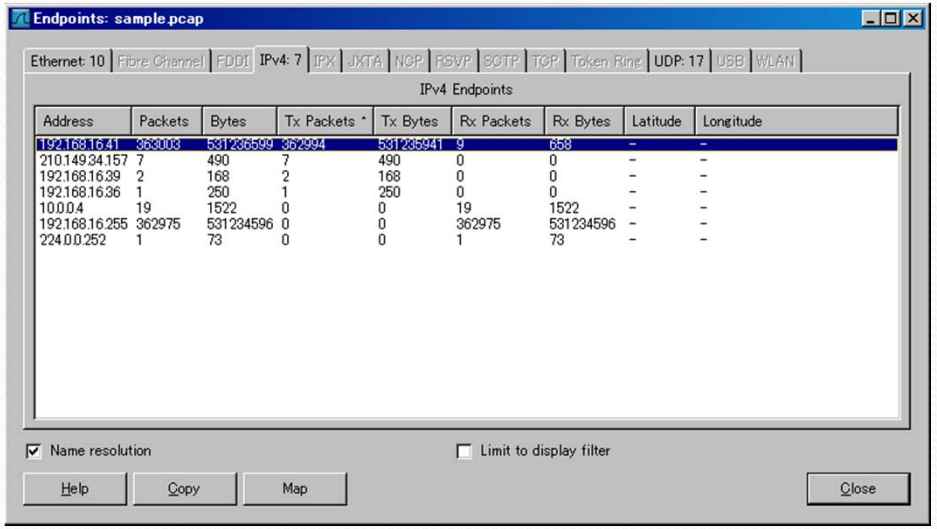
- 引数を入れた表示フィルタを作成できます。
- 引数は第一引数 $1、第二引数 $2、第三引数$3...のように指定して、
  {フィルタ名:第一引数;第二引数;第三引数;...}のように呼び出します。

エキスパートモードの活用

- エキスパートモードに簡単にアクセス
  左下の〇をダブルクリック
- ARPストームの検知　IPアドレスの重複（Preferenceより）
- エキスパートモードに関するフィルタ
- expert.severity==1536 Warning以上
- expert.message contains XXX エキスパートモードにあがっているもの
- TCP分析に関するフィルタ
- tcp.analysis.retransmission

簡単にはじめるTopN分析

- まずはEndpoint　→なんだこのトラフィックは？
- Endpoint表から表示フィルタを作ることができます。
- Endpointで気になったホストを右クリックしてカンバセーションフィルタへ
- フィルタを適用



遅延に関するフィルタ

- 固定遅延を算出してから、10ms－100msに設定
- ユーザーが遅いといったら特定のプロトコルに表示フィルタを適用して、Timeメニューより直前に表示されているパケットからの経過時間を設定して確認します。
- Frame.time == “時間”
- Frame.time?delta > 1
- frame.time_relative < 0.01

Hexで確認するファイルラベル

- エクセルやZip、JPEG画像の各ファイルの先頭には特徴的な16進数のコードがあり、ラベルといいます。
- 添付ファイル・ダウンロードファイル・FTPで取得するファイルの先頭のラベルは知っておくと非常に便利です。
- ファイル名の偽装に対しても一定の効果があります。
- 狐‘s Hex Editorをはじめとして、バイナリエディタを併用することで、さらに検索することができます。
- Pcapを直接WindowsVista／7などの全文検索にかけることで、日本語文字を拾ってくることもできます。

有名なファイルラベル

アプリケーション	拡張子	ラベル
ワード	doc	D0 CF 11 E0 A1 B1 1A E1
エクセル	xls	D0 CF 11 E0 A1 B1 1A E1 00
パワーポイント	ppt	D0 CF 11 E0 A1 B1 1A E1 00
Open Office	odp	50 4B 03 04
JPEG	jpg	FF D8 FF
PNG	png	89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52
ZIP	zip	50 4B 03 04
Wireshark他	pcap	D4 C3 B2 A1
パワポ2007	pptx	50 4B 03 04
ワード2007	docx	50 4B 03 04

FTPのフィルタ

- まずはftp or ftp-dataでトラフィックを絞ります。
- ログイン試行は
  ftp.request.command == “USER”
  ftp.request.command== “PASS”
  などで確認できます。
- クライアント側からポートを開くのがPASSIVEモードです。
  ftp.response.code == 227で確認します。
- アップロード、ダウンロードはファイルラベルやファイル名の一部を利用して検索や抽出を行います。
- 遅延フィルタを用いて応答時間を調べます。

CIFS/SMB

- もともとNetBEUI over Ethernet
- NetBIOSヘッダーのついたSMBパケットをリクエスト・レスポンス形式で交換します。
- 135のポートマッパーでクライアント、サーバーで開くポートを指示します。
- ファイルを開く時に読み・書き・削除を指定します。
- 一定のバイト範囲で、読み・書きにロックをかけられます。
- クライアントはキャッシュができます。

Header (Variable Length – Starts with 0xFFSMB)
Data, length defined by header

CIFSやSMBのフィルタ

- CIFSやSMBを直接pcapで追いかけるのは少し大変です。(Microsoft Network Monitorの方がここは便利)

Type	Offsets	Field
uchar	0-3	Protocol (0xFFSMB)
uchar	4	Command
ulong	5-8	Status (Several variants)
uchar	9	Flags
ushort	10-11	Flags2
uchar	12-23	Security/Extra
ushort	24-33	TID, PID, UID, MID
uchar	34	WordCount
ushort	35-xx	ParameterWords[WordCount]
ushort	xx+1	ByteCount
uchar	xx+2 - yy	Buffer[ByteCount]

POPのフィルタ

- pop.response.indicator == “+OK”
- pop.response.indicator==“+NG”
- pop.request.command == “USER && pop.request.parameter ==“Megumi”
- pop.response.indicator==“+OK” && pop.response.description contains “octets”

SMTPのフィルタ

- smtp.req.command==“EHLO”
- smtp.req.command == “MAIL” &&
  smtp.req.parameter ==“FROM <t@ikeriri.ne.jp>
- smtp.req.command == “RCPT” &&
  smtp.req.parameter ==“TO <t@ikeriri.ne.jp>
- smtp.response.code > 399　**問題あり**

SSLの解読

- SSLの解読はRSA Keys listにIPアドレス,ポート,デコードするプロトコル,鍵ファイルを指定します。
- 鍵ファイルはpem（秘密鍵付きの公開鍵証明書）である必要があります。
- 鍵がない場合にはRSA鍵生成ツールで作成します。
  RSAでないDH鍵などではデコードできないので注意！
- 他にSSLアクセラレーター前でキャプチャしたり、サーバーでキャプチャすることで、これらのかわりをすることができます。
- 無線LANの場合はPreferenceより鍵を入力します。

アノマリなフィルタ(1)

- tcp.flags == 0x00
- tcp.options.wscale_val == 10
- tcp.options.mss_val <1460
- tcp.flags == 0x29 && tcp.urgent_pointer ==0
- tcp.flags==0x02 && frame[42:4] !=00:00:00:00
- tcp.flags==0x02 && tcp.window_size<65535 && tcp.options.wscale_val >0
- tcp.window_size < 65535 && tcp.flags.syn==1
- tcp.port==6666 || tcp.port ==6667 || tcp.port==6668 || tcp.port==6669
- dns.count.answers >5

アノマリなフィルタ(2)

- Icmp.type==3 && icmp.code==2　アンリーチャブル
- icmp and tcp　ICMPエラー（TCP接続に対して）
- icmp type==3 && icmp.code==4 ブラックホール検出
- icmp.type==13 || icmp.type==15 || icmp.type==17　OS検出？
- icmp.type==8 && !icmp.code==0
- tcp.window_size<1460 && tcp.flags.reset ==0
- tcp.window_size ==0 && tcp.flags.reset==0

ポートスキャンやOS検出

- tcp.flags==0x02 && tcp.window_size<1-25
- tcp.flags==0x2b SYN/FIN/PSH/URG
- tcp.flags==0x00
- icmp.type==13 && frame[42:4] == 00:00:00:00
  タイムスタンプ要求、時間が0
- tcp.options.wscale_val ==10
- tcp.options.mss_val < 1460

Time-Sequenceグラフ

- Time-Sequenceグラフ
  踊り場は停滞の印
  tcptraceではウインドウサイズの認識
- Round Trip Timeグラフ
  上につながる点は遅延の増大
- Throughputグラフ
  疎な間隔で低速になる部分に問題

IOグラフのY軸の応用

- IOグラフのY軸の設定にはAdvancedという項目があり、これを活用することで、単位時間ごとのグラフを作れます。棒グラフがおすすめです。
- SUM(*)　時間単位での合計
- MIN (*)　時間単位での最小
- AVG (*)　時間単位での平均
- MAX (*)　時間単位での最大
- COUNT (*) 時間単位での個数
- LOAD(*) 時間に対して 例smb.time rpc.time

tsharkを使っての統計

- コマンドラインツールのtsharkは落ちないでパケットが取れるだけでなく、リアルタイムに統計を出力できます。
- tshark –qz io,phs プロトコル階層
- tshark –qz conv,eth-z conv,ip –z conv,tcp
  Ethernet とIPとTCPのカンバセーション
- tshark –qz io,stat,10,ip,udp,tcp
  10秒間隔でのIP/UDP/TCPの統計
- tshark –qz io,stat,5,tcp.port==80 –w http.pcap
  5秒ごとにTCP80番ポートの統計を表示してファイルに保存

他のコマンドラインツール

- capinfosは巨大ファイルを俯瞰するのに便利
- editcapはキャプチャファイルの複雑な操作
  結合、分割、時間で割るなどに最適
- mergecapは数百メガのpcapの結合など
- text2capはHEXダンプからpcapを生成
- dumpcapはpcapファイルを生成

どうもありがとうございました

Thank You !!

いけりり★ネットワークサービス

www.ikeriri.ne.jp