Colasoft®
Maximize Network Value

Capsa

Real-time Portable Network Analyzer

技術白書

(Enterprise Edition)

お問い合わせ

電話番号

090-7197-9436

Sales

sales.jp@colasoft.com

技術サポート

support.jp@colasoft.com

ウェブサイト

http://www.colasoft.com/jp/

目次

はじめに

この章では、背景、システムアーキテクチャー、および Capsa の動作原理を説明しています。

背景

様々な電子商取引、電子政府、ネットワークオフィス、および現代情報のほかの用途を含め、有線および無線ネットワークの急速な普及と広い応用は、企業に迅速な発展の機会をもたらしています。しかし、人々はネットワークによってもたらされた便利さと利益を享受している同時に、企業/組織の運転に損害を引き起こし、計り知れない損失をもたらす可能性がある、ネットワークの低効率、トラブル、さらにブレークダウンに悩んでいます。

セキュリティー管理およびパフォーマンス維持がますます重要になっているように、ネットワークエンジニアやネットワーク管理者はどのようにネットワークスピードと効率を向上させるかという問題に直面しています。一方、ネットワークインフラストラクチャーがもっと複雑になり、ネットワーク技術が驚くほど急速に発展しているため、ネットワーク保守の実現とネットワーク管理がより困難になっています。ネットワークトラブルを見つけ、解決するために、効率的なネットワーク管理ソリューションはネットワーク管理者にとって、非常に重要です。

Colasoft により提供される Capsa は、このようなソリューションです。Capsa はリアルタイムにオリジナルパケットをキャプチャーし、キャプチャーされたパケットに対してデコード、解析、診断を実行します。そして、直観的なビュー、視覚化チャート、および構造化されたレポートで結果を表示します。それによって、ネットワーク管理者はネットワーク状態を包括的、且つ迅速的に把握することができます。

動作原理

実際のネットワーク通信では、データの送受信は全てネットワークアダプタを介して行われています。デフォルトでは、ネットワークアダプタは、ネットワークにおけるブロードキャストトラフィック、および MAC アドレスと一致したユニキャストパケットだけを受信できます。ネットワークアダプタをプロミスキャスモードにすると、目的地にかかわらず、アダプタを介している全てのトラフィックを受信します。

Colasoft Capsa はそのようなメカニズムを利用して、パケットをキャプチャーします。そして、Capsa は IP アドレス、MAC アドレス、プロトコル、パケットなどのネットワーク要素を一つのネットワークオブジェクトとして扱い、これらを有機的に結び付けて 1 つの「プロジェクト」（システム中で使われている技術用語）を構成します。これによってネットワーク内のデータ通信の変化が常にリアルタイムでプロジェクトファイルに反映されるようになります。

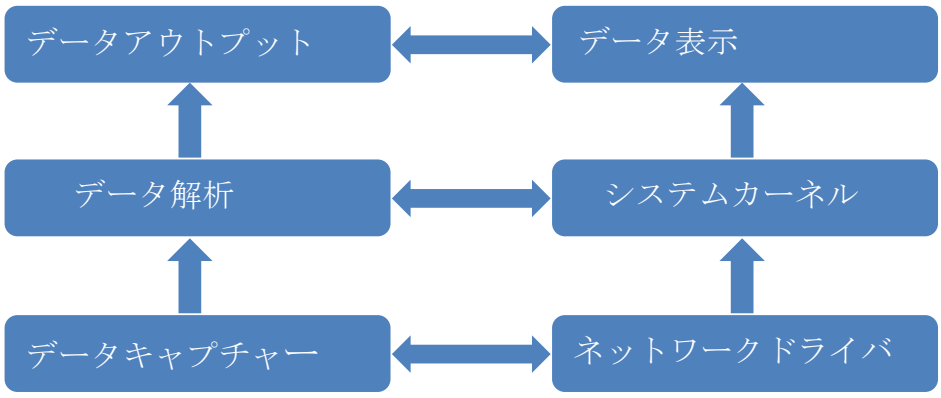
Colasoft Capsa はイーサネットのスニファー技術を基に、迂回アクセスによってトラフィックをキャプチャします。まず初めに Colasoft Capsa がインストールされたコンピューターのネットワークアダプタをプロミスキャスモードに設定し、ネットワーク内の全てのパケットをキャプチャーします。そしてキャプチャーされたパケットを解析モジュールに送り込ん

で解析します。最後にその解析結果をシステムのインターフェースに表示し、ネットワーク内で発生している障害を自動的に診断します。

システムアーキテクチャー

ネットワークに流れているトラフィックを解析するには、まずそのトラフィックをキャプチャーする必要があります。ボトルレベルのネットワークドライバは、転送されたデータを検出し、キャプチャーするためのコアモジュールです。その後、全てのデータはハイレベルのモジュールに転送、解析され、さらにまとめられ、システムインターフェースに表示されます。Capsa のアーキテクチャーは図 1 を参照して下さい。

図 1： Capsa アーキテクチャー



1. ネットワークドライブはネットワークトラフィックのキャプチャーを担当し、データが正確且つ完全であることを確保します。
2. リアルタイム診断と解析するためにキャプチャーされた全てのデータは、診断モジュール、統計モジュール、パケットデコーディングモジュール、および他の解析モジュールなどに転送されます。
3. 最後に解析結果はユーザーインターフェースおよび/またはハードディスクにアウトプットされます。

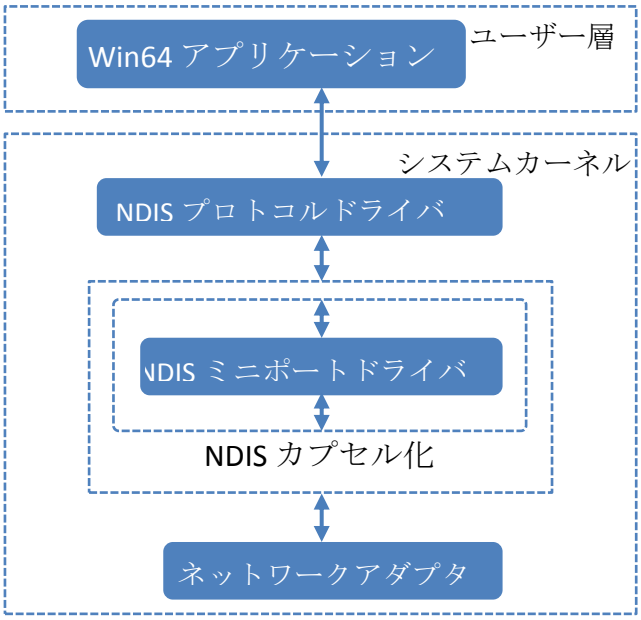
データのキャプチャー

Capsa は、次の三つの方法でパケットをキャプチャーすることができます。

1. Windows における Colasoft NDIS Protocol Driver によって、ネットワークアダプタに流れているパケットをキャプチャーします。
2. Windows における Colasoft NDIS Intermediate Driver によって、ネットワークアダプタに流れているパケットをキャプチャーします。
3. Windows における Colasoft TDI Driver によって、ネットワークアダプタを通過しないローカルループパケットをキャプチャーします。

デフォルトでは、Capsa は Colasoft NDIS Protocol Driver および Colasoft TDI Driver を介して、トラフィックをキャプチャーします。以下の図は Capsa のデータキャプチャープロセスを紹介しています。

図 2：データキャプチャープロセス

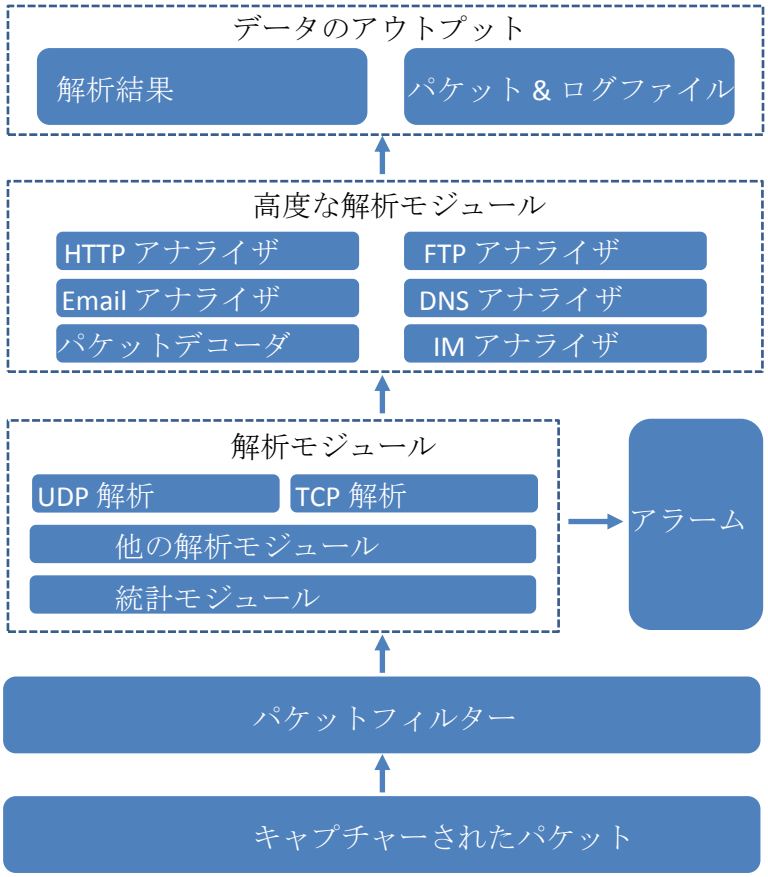


ボトルレベルのデータキャプチャーの効率は以下の解析ミッションに非常に重要です。従って、ドライブレベルからアプリケーションレベルまでのテータ転送によるリソースの浪費を避けるために、フィルターを利用して、このレベルでフィルタリング条件に一致しないパケットを排除します。

データ解析

ドライバはフィルタリング条件に一致しているパケットをキャプチャーした後、更なる解析のために、直ちにこれらのパケットをシステムカーネルに転送します。データ解析の内容は、パケットの統計、検査、デコード、プロトコル解析等が含まれています。以下の図は、Colasoft Capsa のパケット解析プロセスを示しています。

図 3：パケット解析プロセス



データのアウトプットと表示

パケットを解析した後、全ての解析結果と統計は、チャート、リスト、およびレポートの形式でシステムインターフェースに表示されます。表示された解析内容には、パケットデコード、ノード、プロトコル、IP フロー、TCP フロー、セッション、ログなどが含まれています。また、これらのリスト、レポートおよびログは、更なる使用のために、必要に応じてエクスポートすることができます。

主な特長

他のネットワークスニファ製品とは異なるいくつかのユニークな機能を含め、Capsa は多くの強力な機能を提供します。

Colasoft パケット解析エンジン (CSPAE) II

革新的な CSDOM（Colasof が自主開発したダイナミックオブジェクトモデルのこと）を搭載した第二世代 Colasoft Packet Analysis Engine (Colasoft パケット解析エンジン、CSPAE)は、大量トラフィックネットワークの解析効率性とパフォーマンスを大幅に向上させることができます。次の新しい技術は Capsa に適用されています。

- マルチスレッド解析
  - シングルスレッド解析からマルチスレッド解析にアップグレード。マルチコア CPU の処理能力を最大限に活用
- マルチサイクルバッファー (MCB)
  - 複数のキャッシュバッファーを再利用
  - 解析とデータ照会の待ち時間を回避するため、データ解析とデータアクセスを並行実施
  - メモリ断片化の発生を減少
- ダイレクトメモリアクセス (DMA)
  - バイパスカーネルレベル、ユーザーレベルにデータを直接転送
  - データ転送をスピードアップ
- プロトコルを動的に作成
  - プロトコルツリー構造を動的に作成
  - プロトコルとサブプロトコルタイプを効率的に識別
  - ユーザーがカスタマイズしたプロトコルをサポート

斬新な解析ガイド

Capsa は使いやすいスタートページを提供し、ユーザーに解析プロジェクトの開始をガイドします。通常、四つの簡単なステップで解析プロジェクトを開始することができます。

1. 解析モードを選択する：リアルタイム解析、あるいはリプレイ解析
2. パケットをキャプチャーするネットワークアダプタを選択して、ネットワークプロファイルを選択するか、あるいはリプレイするパケットファイルを選択する
3. 適切な解析プロファイルを選択する
4. 「スタート」をクリックして、解析プロジェクトを開始する

ネットワークプロファイル

Colasoft Capsa はノートパソコンにインストールされることができ、その後、ノートパソコンを利用して、任意のネットワークにアクセスすることができます。各ネットワークは、独自のネットワーク構造とプロパティを有しています。ネットワークプロファイルでは、ネットワーク帯域幅、ネットワーク構造、ネームテーブル、およびアラーム設定を含め、異なる

ネットワークの一般的なプロパティを保存します。同じタイプのネットワークを解析する必要がある場合、そのネットワークのネットワークプロファイルをロードすればよいのです。

解析プロファイル

柔軟で、拡張可能且つ効果的な解析性能を提供するために、Capsa は、解析プロファイルを異なる解析モジュールのコンテナに定義します。異なる解析モジュールを組み合わせて、特定のアプリケーションを焦点にする独自の解析プロファイルを作成することができます。次の表はデフォルトの解析プロファイルについて説明しています。

解析タイプ	解析プロファイル	説明
基本解析	トラフィックモニター	大規模なトラフィックネットワークの解析、またはトラフィックモニターを提供する。
	フル解析	全てのトラフィックとアプリケーションの包括的な解析を提供する。
アプリケーション解析	HTTP 解析	HTTP トラフィックを解析し、クライアントとサーバーのトラフィック統計、パフォーマンス診断および HTTP 活動ログを提供する。
	セキュリティー解析	潜在的なネットワークセキュリティーリスクに対する専用的な解析を提供する。
	FTP 解析	FTP トラフィックを解析し、アップロードとダウンロードに関する統計、パフォーマンス診断および FTP 活動ログを提供する。
	E メール解析	SMTP/POP3 トラフィックを解析し、E メール通信の統計、E メールの複製、E メール活動ログを提供する。
	DNS 解析	DNS トラフィックを解析し、DNS クエリーに関する統計、パフォーマンス診断、DNS 活動ログを提供する。
	IM 解析	インスタントメッセンジャー解析を提供する。
	VoIP 解析	VoIP コールの解析とトラブルシューティングを提供する。
ビルトイン解析	TCP フロー解析	TCP トランザクションを解析し、トランザクションプロシージャの詳細情報を提供します。

ノードブラウザウィンドウ

ノードブラウザウィンドウは、ユーザーが便利に特定のノード、ネットワークセグメント、またはプロトコルの解析と統計情報を確認するために、提供されます。ノードブラウザは機能において、強力なフィルターで、三つのタイプのノードブラウザからなっています：プロトコルブラウザは、階層的にネットワークにおけるプロトコルを表示する；物理ブラウザは、MAC アドレス間の通信を表示する；IP ブラウザは IP ノードの解析と統計を提供する。

強力なマイグラフ

マイグラフでは、数回クリックすることで、全体ネットワーク、さらに特定のノードに関する様々なチャートとグラフを定義し、表示することができます。また、ここで各 TOP 統計はチャート形式でリアルタイムに表示されます。それによって、直感的且つ包括的にネットワーク状態を把握することができます。

エキスパート診断

Capsa は、異なるレベルでの障害およびパフォーマンス管理を行うエキスパートシステムを提供します。エキスパート診断モジュールは自動的に 40 以上のネットワーク問題を識別し、解析することができます。そして、ネットワーク問題の解析によって、ソリューションをアドバイスします。診断結果だけでなく、Capsa は疑わしいホストアドレス、考えられる原因およびソリューションをユーザーに提供します。無線ネットワークのトラブルシューティングに対して、Capsa は時間を減少させ、効率を向上させることができます。従って、ネットワーク管理者の問題解決に役立ちます。

トラフィック解析

トラフィック解析を利用して、最大通信量を持つホストを容易且つ迅速に特定することができます。バイト数、パケット、ビットレット、TCP セッション数、および他のパラメータによって、ノードを並べけることができます。さらに、最大送信トラフィックを持つホスト、最大受信トラフィックを持つホスト、最大ブロードキャスト量を持つホスト、および最大内部トラフィックを持つネットワークセグメントを簡単に特定することができます。

プロトコル解析

パケット統計、バイト統計、ビットレット、およびトラフィックパーセンテージが含んでいる各プロトコルノードのトラフィック統計とともに、Capsa は実際にネットワークプロトコルがカプセル化された順番に基づいて階層的にプロトコルを表示します。プロトコル解析を利用することで、簡単に最大トラフィック量を持つアプリケーションを特定することができ、さらにネットワークのトラブルシューティングに役だちます。

セッション解析

Capsa は、MAC アドレス間の物理セッション、IP セッション、TCP セッション、および UDP セッションという四つのタイプのセッションを提供します。各タイプのセッションは、送信元アドレス、宛先アドレス、このセッションのパケットとバイト、開始時間と終了時間、持続時間によって提供されます。

TCP トランザクション解析

Capsa はネットワーク上のアプリケーションの健康状態について、包括的に高レベルの概要で表示します。TCP トランザクション解析では、ドリルダウンして、TCP サーバー/クライアントレスポンス時間、遅延、再送信を含む詳細情報を確認することができます。さらにサーバーフローまでドリルダウンして、実際のフローのコンテンツを確認することもできます。

これによって、アプリケーションの問題解決までの時間を短縮し、全体的なネットワークのダウンタイムを最小限に抑えることができます。

ローカルプロセス解析

Capsa はプロセスビューを提供することで、ローカルプロセスに基づきネットワークトラフィックを統計します。プロセスビューであるプロセスをダブルクリックすることで、そのプロセスに関するすべてのパケットが表示されます。そしてプロセスブラウザも搭載され、プロセス名、プロセス ID を階層構造でリストすることで、すべてのプロセスをグループ分けします。さらに TCP セッションビューと UDP セッションビューでは「プロセス」カラムが提供されているので、各 TCP/UDP セッションの属するプロセスを確認することができます。これはユーザーの迅速なトラブルシューティングに役立ちます。

詳細なデコード

デコーディングビューは、サマリデコード、フィールドデコード、16 進数デコード、ASCII デコード、および EBCDIC デコードからなっていて、全てのパケットの詳細的なデコード情報を表示します。これらのデコード情報によって、ユーザーはネットワーク内で転送されたオリジナルデータを把握することができます。

柔軟なレポート

レポートは、概要統計、診断イベント、プロトコル統計、top 10 トラフィックなどの統計情報から構成されています。ネットワーク全体だけでなく、特定のノードに関するレポートを作成することもできます。さらにユーザーは会社名やプライベートログなどのパラメータを含むレポートテンプレートをカスタマイズし、レポートを HTML または PDF フォーマットでディスクに保存することができます。

リアルタイムアラーム

アラームはトラフィック、パケットサイズ、使用率、プロトコル、セッション、アプリケーション、エキスパート診断イベントなど様々なトラフィックパラメータによって、定義され、ネットワークの異常を通知します。また、アラームは全体ネットワークだけでなく、特定のノードに対して、定義されることもできます。アラームがドリガーされると、通知がポップアップされ、アラーム音が出します。コンピューターの周りにいなくても、トリガーされたアラームの詳細情報を E メールで通知することができます。

ログ解析

高度な解析モジュールによって解析されたネットワーク通信は、HTTP 要求と応答ログ、DNS クエリーログ、E メール送受信ログ、FTP ファイル転送ログ、インスタントメッセンジャーログなどのログ形式で記録され、表示されることができます。また、E メールログは、送信者と受信者の情報を記録するだけでなく、E メール本文と全ての添付ファイルを含め、E メールコンテンツのコピーを保存することもできます。さらに、全てのログは、自動的に時間や大きさに応じて、一つまたは複数のファイルに保存されます。

専用のセキュリティー解析

Capsa は、ARP 攻撃、TCP ポートスキャン、ワーム活動、DoS 攻撃、不審なセッションなどのセキュリティー脅威を検出するセキュリティー解析プロファイルを提供します。これらの攻撃が検出されると、攻撃されたホスト、攻撃された時間、および攻撃を実行したホストはリストされます。

802.11 a/b/g/n をサポート

無線ネットワークは安価で、使いやすく、且つポータブルで、圧倒的な魅力を持っています。最新の安全な無線ネットワークを構築するための革新的且つ高品質ネットワーク解析ソリューションとして、Capsa Enterprise は、アプリケーションパフォーマンスを測定し、ネットワーク活動を監視し、ネットワーク問題をトラブルシューティングし、ネットワークセキュリティーを評価することができます。Capsa Enterprise は、802.11 a/b/g/n ネットワークを採用しているシームレス Wi-Fi 技術によって起動されます。

効率的な WEP/WPA/WPA2 暗号解読

無線 LAN 用の Capsa は、ワイヤレストラフィックをキャプチャーするだけでなく、暗号化された無線データをデコードすることもできます。AP がどんなタイプの暗号化を使っても、予め指定されたセキュリティキーにより、全ての WEP、WPA 及びもっとも複雑な WPA2 無線トラフィックが解読できます。それに、ユーザーが自ら暗号化タイプを把握する必要がなく、Capsa は自動的にキーを暗号化タイプと一致させます。

プロトコルのカスタマイズ

Capsa は 900 以上のプロトコルとサブプロトコルを認識することができます。ユーザーは自分のニーズに応じて、新しいプロトコルを識別するルールを簡単に作成することができます。イーサネットタイプ、IP カプセル化プロトコル ID、TCP ポート、UDP ポートによってプロトコルをカスタマイズすることができます。

自動的にパケットをキャプチャー

予め指定された解析設定によって自動的パケットをキャプチャーするタスクスケジューラが提供されています。この機能を利用して、ネットワークから離れていても、パケットをキャプチャーする任務を実行することができます。例えば、Capsa は真夜中でパケットをキャプチャーするために、自動的に起動され、キャプチャーされたパケットは次の日の朝に解析されることができます。そして、Capsa は、タスクスケジューラを作成することによって、定期的に毎日、あるいは毎週指定された日にパケットキャプチャーを実行することができます。例えば、出勤日のネットワークパケットだけを解析する必要がある場合、月曜日から金曜日までの午前 9 時と午後 5 時の間のパケットキャプチャーを自動的に実行するタスクを作成するすることができます。

VoIP 解析をサポート

Capsa は VoIP コールをリアルタイムにキャプチャーし、解析する VoIP 解析モジュールを提供し、VoIP 解析結果をグラフィカルに表示します。VoIP ビューには、全ての VoIP コートお

よび関連統計がリストされます。そして下における音声とビデオ制御フロー、メディアフロー、ジッタ、ロス、MOS などを解析するパネルでは、解析データが表示され、さらに音声とビデオの品質の評価が行われます。VoIP ブラウザには、VoIP コールのプライベートとパブリックの IP アドレスが集まっています。マイグラフにおける VoIP タブでは、VoIP 解析チャートがグラフィカルに表示されます。そのほかに VoIP 診断イベントと VoIP ログがあります。

ポート番号に基づく統計

TCP/UDP ポート番号に基づくトラフィック統計を表示するポートビューが提供されています。この特長は特定のアプリケーションを解析したいときに便利です。ポート番号は上記の層のプロトコル、パケット、バイト、変パケット長さ、およびコモンアプリケーションと一緒に提供されています。選択されたポート番号の TCP および/または UDP セッションは、下のパネルに表示されます。

使いやすい表示フィルター

キャプチャーフィルターのほかに、Capsa は関心のある項目を表示できる表示フィルターを提供しています。簡易な表示フィルターは統計ビューにおけるフィールドカラムによってフィルタリングを実行するものです。高級な表示フィルターはパケットビューでだけ利用可能になり、パケットのプロトコルフィールドに基づいて感心のないパケットをフィルターアウトすることができます。さらに高級な表示フィルターは指定された時間範囲のパケットを表示することもできます。

システムの代表的な機能

Capsa は、トラフィックキャプチャー、解析と統計、故障診断、およびパフォーマンス評価を統合させたネットワーク管理ソリューションです。また、Capsa はネットワーク管理者のトラブルシューティングに役立ち、ネットワークセキュリティーを確保し、ネットワークパフォーマンスを向上させ、ネットワーク価値を最大限にします。

以下のリスト、システムの代表的な機能について説明しています。

包括的なトラフィック統計

- 全体ネットワークトラフィック概要
- 全体ネットワーク通信量
- ブロードキャスト通信量
- マルチキャスト通信量
- 内部トラフィック
- 一つの IP アドレスのトラフィック
- 一つの MAC アドレスのトラフィック
- 一つのセグメントのトラフィック
- 一つの VLAN のトラフィック
- 一つのアプリケーション（プロトコルのトラフィック
- ダウンリンクトラフィック
- アップリンクトラフィック
- ダウンリンクパケット数
- アップリンクパケット数
- 総パケット数
- 物理層のセッション統計
- IP 層のセッション統計
- TCP セッション統計
- UDP セッション統計
- 1 秒当たりのパケット (pps) 統計
- インバウンド/アウトバウンドトラフィック
- インバウンド/アウトバウンドパケット比率
- IP 国家グループ
- トラフィック、プロトコルと診断に関するアラーム
- ポートに基づく統計
- Top ドメイン名統計

エキスパート診断

- ARP スキャン
- ARP 中間者攻撃
- ARP スプーフィング攻撃
- TCP ポートスキャン
- UDP ポートスキャン
- ICMP スキャン
- データリンク層診断
- IP 層診断
- トランスポート層診断
- アプリケーション層診断
- P2P アプリケーション解析
- IP アドレスの競合
- ネットワークループ
- ワーム活動
- DNS サービス障害
- E メールサービス障害(SMTP & POP3)
- HTTP サービス障害
- FTP ファイル転送障害
- ポート 80、23 、53、110 のプロキシーサービス
- 異常トラフィック診断
- スパ無トラフィック診断

プロトコル解析

- ユーザー定義のプロトコルを識別
- ネットワークサービスを識別
- ネットワークサービスを解析
- 帯域幅の使用状況を解析
- アプリケーションパケットを統計
- 特定のサービスを実行しているホストを特定
- Hex、ASCII と EBCDIC によってプロトコルをデコード
- 異常プロトコルを識別

- 偽造パケットを識別
- OSI 7 階層に基づきプロトコルを表示

セッション解析

- MAC アドレス間のセッション
- IP アドレス間のセッション
- TCP セッション
- TCP 通信を再構築
- TCP トランザクション
- UDP トラフィック
- BitTorrent トラフィック
- マトリックスにおけるネットワーク通信
- TCP タイムシーケンス図

セキュリティー解析

- 急速にネットワーク攻撃を特定
  - フラグメント攻撃
  - TCP スキャン
  - UDP スキャン
  - ICMP スキャン
  - E メールワーム
  - DoS 攻撃
  - MAC フラッディング攻撃
  - 不審なセッション
  - プレーンテキスト転送
  - 不正アクセス
- 他の異常ネットワーク活動
- 潜在的なネットワークセキュリティー脅威
- ウェブサイトセキュリティー評価
- E メールセキュリティー評価
- DNS セキュリティー評価
- FTP ファイル転送セキュリティー評価
- 端末セキュリティー評価
- ネットワークセキュリティーベースライン

パフォーマンス評価

- アウトバウンド帯域幅需要を評価
- アウトバウンド帯域幅使用率を評価
- 内部帯域幅の使用状況を評価
- パケットサイズ分布を評価
- ネットワークアップグレードパフォーマンスを評価
- TCP トランザクションパフォーマンスを解析
- 重要なビジネストラフィックと非業務トラフィックを評価
- ネットワーク転送パフォーマンスを評価
- ネットワークパフォーマンスベースライン
- アプリケーションパフォーマンスの詳細解析

製品仕様

サポートしているネットワークタイプ

- イーサネット
- 高速イーサネット
- ギガビットイーサネット
- 2.4 GHz と 5 GHz で転送している 802.11 a/b/g/n ワイヤレスネットワーク
  - 802.11a: 6, 9, 12, 18, 24, 36, 48, 54, 72, 96, 108 Mbps
  - 802.11b: 1, 2, 5,5, 11 Mbps
  - 802.11g: 5.5, 6, 9, 11, 12, 18, 22, 24, 33, 48, 54 Mbps

サポートしているアダプタ

- 10/100/1000 Mbps イーサネットアダプタ
- サポートしているワイヤレスアダプタ:
  - Atheros AR7015, AR6004, AR9380, AR9382, AR9390, AR9485, AR9462, AR958x
  - Intel 1000, 4965, 5100, 5150, 5300, 5350, 6200, 6250, 6300, 6350, AC 7260, 82579LM
  - Realtek RTL8188CU, RTL8192CU, RTL8187
  - Broadcom 4313GN 802.11 b/g/n
  - TP-Link TL-WDN3200(5.1.7.5014), TL-822N v2
  - D-Link DWA-160 B2(5.1.7.5014)

システム要件

オペレーティングシステム

- Windows Server 2008 (64-bit)*
- Windows Server 2012 (64-bit)**
- Windows Vista (64-bit)
- Windows 7 (64-bit)
- Windows 8/8.1 (64-bit)
- Windows 10 Professional (64-bit)

*はワイヤレス解析モジュールがこのオペレーティングシステムと交換性がないことを示しています。

**は Colasoft Packet Builder はこのオペレーティングシステムと交換性がないことを示しています。

最小要件

- CPU: P4 2.8GHz
- RAM: 4GB
- Internet Explorer 6.0
- 100 MB のディスク空き領域

推奨システム要件

- CPU: Intel Dual-Core 3.2GHz

- RAM: 8GB 以上
- Internet Explorer 8.0 以上
- 10 GB のパケットファイルとログのための追加スペース

サポートしているパケットファイルフォーマット

Capsa でリプレイできるパケットファイルフォーマットは以下の通りです。

- Accellent 5Views Packet File (*.5vw)
- Colasoft Packet File (*.cscpkt; *rapkt; *.rawpkt; *.cacproj)
- EtherPeek Packet File (V7/V9) (*.pkt)
- HP Unix Nettl Packet File (*.TRCO; TRC1)
- Libpcap (Wireshark, Tcpdump, Ethereal, etc.) (*.cap; *pcap)
- Wireshark (Wireshark, etc.) (*.pcapang; *pcapang.gz; *.ntar; *.ntar.gz)
- Microsoft Network Monitor 1.x 2.x (*.cap)
- Novell LANalyer (*.tr1)
- Network Instruments Observer V9.0 (*.bfr)
- NetXRay 2.0, and Windows Sniffer (*.cap)
- Sun_Snoop (*.Snoop)
- Visual Network Traffic Capture (*.cap)

Capsa でキャプチャーされたパケットは以下のパケットファイルフォーマットにエクスポートすることができます。

- Accellent 5Views Packet File (*.5vw)
- Colasoft Packet File (V3) (*.rapkt)
- Colasoft Packet File (*.cscpkt)
- Colasoft Raw Packet File (*.rawpkt）
- Colasoft Raw Packet File (V2) (*.rawpkt）
- EtherPeek Packet File (V9) (*.pkt)
- HP Unix Nettl Packet File (*.TRCO; *.TRC1)
- Libpcap (Wireshark, Tcpdump, Ethereal, etc.) (*.cap; *pcap)
- Wireshark (Wireshark, etc.) (*.pcapang; *pcapang.gz; *.ntar; *.ntar.gz)
- Microsoft Network Monitor 1.x 2.x (*.cap)
- Novell LANalyer (*.tr1)
- NetXRay 2.0, and Windows Sniffer (*.cap)
- Sun_Snoop (*.Snoop)
- Visual Network Traffic Capture (*.cap)

サポートしているプロトコル

Capsa は 1500 以上のプロトコルおよびサブプロトコルをサポートしています。以下はサポートしているアプリケーション層プロトコルのリストです。

MiNT, MIPv6, MONGO, MSDP, Netsync, MSNMS, NBDS, OLSR, OMAPI, OPSI, PacketBB, PCEP, PCP, PGSQL, PKTC, PULSE, QUAKE, QUAKE2, QUAKE3, QUAKEWORLD, RDT, Rlogin, RSIP, RSYNC, SAMETIME, SCoP, SEBEK, SIGCOMP, SIR, SliMP3, SMRSE, SMUX, Socks, SoulSeek, SPDY, SRVLOC, T.38, Tetra, TFP, TNS, TPCP, TPNCP, TZSP, UDPENCAP, ULP, VICP, WASSP, WINS-Replication, WoW, WTLS, X11, XDMCP, XMPP, XOT, XYPLEX, ZEP, AllJoyn NS, MRP-MMRP, MRP-MSRP, MRP-MVRP, NSRP,

ROHC, Roofnet, RTcfg, Rtmac, SERCOS III V1.1, SNAETH, TDMoE, TELKONET, TIPC, TRILL, TTE PCF, VMLAB, VNTAG, WAI, WRETH, WSMP, swIPe, UDPlite, XTP, HOPOPT, ST, BBN-RCC-MON, NVP-II, ARGUS, EMCON, XNET, MUX, DCN-MEAS, TRUNK-1, TRUNK-2, LEAF-1, LEAF-2, MFE-NSP, MERIT-INP, 3PC, IDRP-CMTP, TPPP, IL, IPv6-Route, IPv6-Frag, BNA, I-NLSP, MOBILE, IPv6-NoNxt, IPv6-Opts, AHIP, ALN, SAT-EXPAK, SAT-MON, KRYPTOLAN, RVD, IPPC, ADFS, VISA, IPCU, CPNX, CPHB, WSN, BR-SAT-MON, SUN-ND, WB-MON, WB-EXPAK, VMTP, SECURE-VMTP, VINES, TTP, IPTM, NSFNET-IGP, DGP, TCF, Sprite-RPC, LARP, MTP, AX.25, IPIP, MICP, SCC-SP, ENCAP, APES, GMTP, IFMP, PNNI, ARIS, SCPS, QNX, A/N, IPComp, Compaq-Peer, IPX-in-IP, 0-hop, DDX, IATP, STPoIP, UTI, SM, IS-IS over IPv4, FIRE, SSCOPMCE, IPLT, RSVP-E2E-IGNORE, Mobility Header, MPLS-in-IP, manet, Shim6, WESP, DCE, FSPFoE, IEN, DOSP, DRCP, RBCP, BSP, MVP, IETF-TRILL, HDBTCMP, HCfB, GHP, AES50-2005, TPC, ES, IN, MXSP, WIO, STISA, TEP, VNTSMP, Eth-Trunks, MEF, NN, IEEE 802.1 ECP, IPDoE, IEN LAN-to-LAN, IEEE 802.1 CFM, MPLS-LS, IS-IS, EBP, VSP, XDP, DRP, FMACS, NMCS, NSMCP, MRP, LSPP, MACSP, MISIDRP, SET, CPNSH, TCN, EoIB, MDC, REAC, PACU, TLDP, CDMA-ANI, XSHD, NC-SI, E-LMI, JRC-LTP, BCN, DOCSIS, DOCSIS MAC MGMT, DOCSIS B-INT-RNG-REQ, DOCSIS BPKM-REQ, DOCSIS BPKM-RSP, DOCSIS CM-CTRL-REQ, DOCSIS CM-CTRL-RSP, DOCSIS CM-STATUS, DOCSIS DBC-ACK, DOCSIS DBC-REQ, DOCSIS DBC-RSP, DOCSIS DCC-ACK, DOCSIS DCC-REQ, DOCSIS DCC-RSP, DOCSIS DCD, DOCSIS DPV-REQ, DOCSIS DPV-RSP, DOCSIS DSA-ACK, DOCSIS DSA-REQ, DOCSIS DSA-RSP, DOCSIS DSC-ACK, DOCSIS DSC-REQ, DOCSIS DSC-RSP, DOCSIS DSD-REQ, DOCSIS DSD-RSP, DOCSIS INT-RNG-REQ, DOCSIS MAP, DOCSIS Mdd, DOCSIS REG-ACK, DOCSIS REG-REQ, DOCSIS Reg-Req-Mp, DOCSIS REG-RSP, DOCSIS Reg-Rsp-Mp, DOCSIS RNG-REQ, DOCSIS RNG-RSP, DOCSIS Sync, DOCSIS type29ucd, DOCSIS UCC-REQ, DOCSIS UCC-RSP, DOCSIS UCD, FNTP, MRME, HBLLVoE, IPMP, T-VLAN, WNSIA, N-Ring, CLP, TAEPoL, PXLVD, FCMP, APP, MMP, GAC, ZLLS, FLDP, CEC, TLP, PCCP, VARAN, RDMAoE, BTSI, 2dparityfec, EVRC, RTP PCMU, RTP LPC, RTP PCMA, RTP G.722, RTP L16, RTP QCELP, RTP CN, RTP MPA, FGP, PIPO, CALCAPP, SSP, NPMP-CONTROL, NPMP-DATA, CHARGEN, 3GPP M2AP, 3GPP RNA, 3GPP M3AP, SSHoSCTP, DSDC, DDDC, R14P, WebRTC DCEP, WebRTC String, WebRTC Binary Partial, WebRTC Binary, WebRTC String Partial, 3GPP PUA, WebRTC Binary Empty, WebRTC String Empty, 3GPP XwAP, 3GPP Xw-Control Plane, PPP ROHC-S, PPP ROHC-L, PPP OSI NL, PPP XNI, PPP DEC, PPP Appletalk, PPP IPX, PPP VJC, PPP VJU, PPP BRID, PPP STREAM, PPP Banyan Vines, PPP AppleTalk EDDP, PPP AppleTalk SB, PPP Multi-Link, PPP NETBIOS Fram, PPP Cisco Sys, PPP Ascom Timeplex, PPP LBLB, PPP SDTP, PPP DCA-RL, PPP 802.2 SNA, PPP SNA, PPP IPv6 HC, PPP KNX-BD, PPP Encryption, PPP ILE, PPP Muxing, PPP VSNP, PPP TNP, PPP SLCM, PPP CDP, PPP NTR, PPP STP, PPP EDP, PPP OSCP, PPP SNS, PPP ACSP, PPP MFTP, PPP CCCP, PPP EAP, PPP CNDP, PPP RefTek, PPP EMIT, PPP VSP, PPP TLSP, PPP OSI-NLCP, PPP ACP, PPP SPCP, PPP BVCP, PPP MLCP, PPP CSCP, PPP RLNCP, PPP SDCP, PPP ECP, PPP ILECP, PPP VSNCP, PPP TNCP, PPP SBCP, PPP CCP, PPP CDPC, PPP ACSPC, PPP SPAP, PPP for POS