JPNIC・JPCERT/CC Security Seminar 2004

不正侵入の発見

株式会社アイアイジェイテクノロジー
技術開発部 セキュリティコンサルティンググループ
加藤雅彦 ＜masa@iij-tech.co.jp＞

おことわり

- 本セッションは「ログ管理・解析」の続きとなりますので、そちらとあわせてご覧ください
- 資料中のコマンド等はLinuxをベースとしています。他のOSでも大きくは変わらないですが、実際にコマンドを使用する場合はそれぞれのOSに付属しているmanualを参照してください
- 使用するソフトウェアはオープンソースを想定しています

Agenda

- ディスク解析の前提知識
- ディスク解析に必要な準備
- 解析ツール
- HDDデータ復旧の可能性
- 総合的な分析ツール
- 不正か否かの判断
- リスクの発見
- 最後に

不正侵入をどうやって特定するか

不正発見の考え方

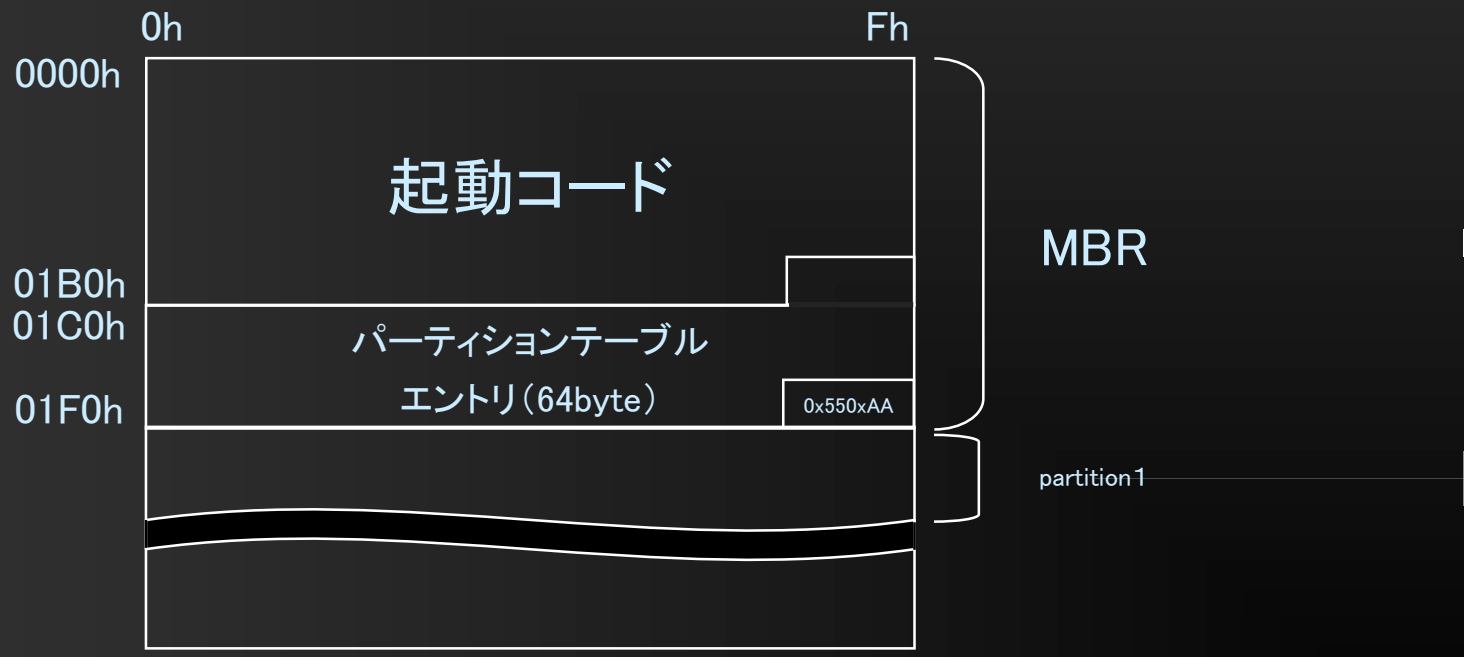
ディスク解析の前提知識

ディスク解析の前提知識

- 簡単に前提知識のおさらい
  - 不正侵入を受けたディスクの解析を行うにあたって知っておいた方がよいこと
    - パーティションの基本
    - UNIXファイルシステムの基本
    - mac time
    - ファイルが消されるとどうなるか
    - ファイル情報保存のためのベカラズ集
    - 作業の流れ

ディスク解析の前提知識

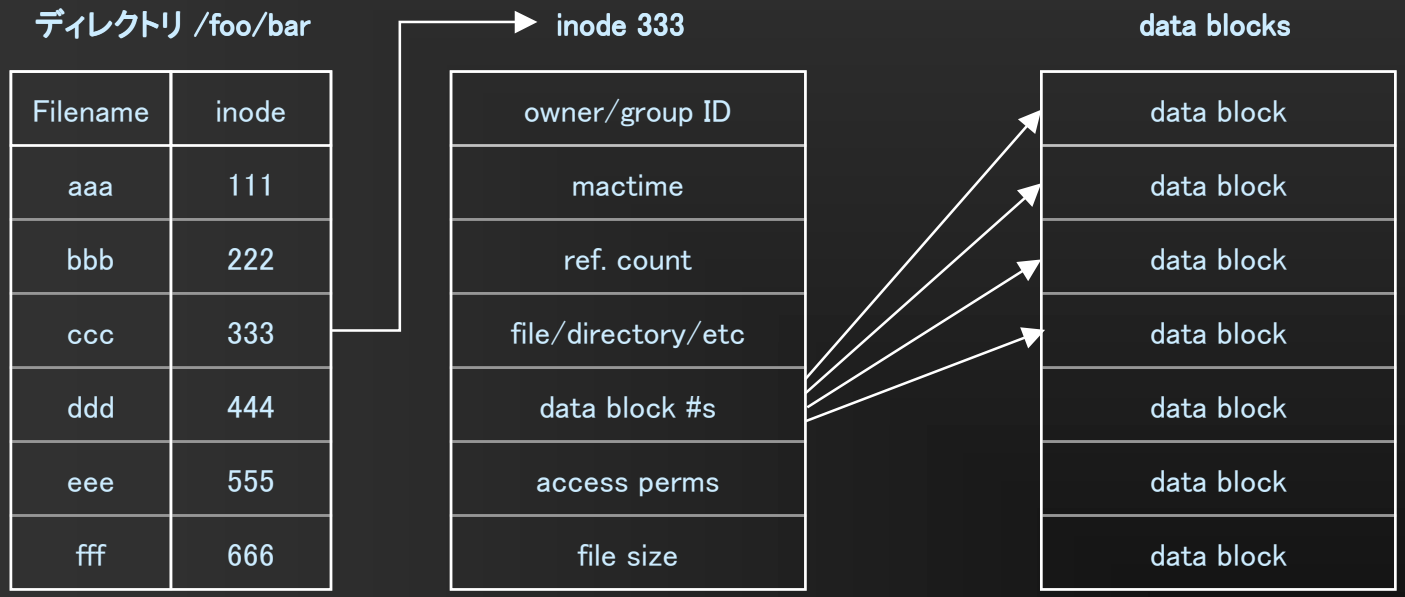
- パーティションの基本
  - パーティション
    - 1本のディスクを論理的に分割して見せる
    - 特定の領域にデータを集中させ、管理の容易さやアクセス速度の向上を図る
    - 起動時に読み込まれる領域(MBR)の中に定義されている
    - プライマリが4領域確保可能なのは1パーティションあたり16byte必要で、エントリが64byte分しかないため。それ以上は拡張パーティションとなる
    - FD等はこの領域にデータがかかれていない
    - ディスクを複数パーティションまとめてバックアップした場合、ファイルシステムとして読み出すにはパーティション情報が必要(後述)



ディスク解析の前提知識

UNIXファイルシステムの基本

- inodeを使った参照方式の概念図



※サイズの大きなファイルは
間接参照される

ディスク解析の前提知識

- mactime
  - ファイルに関する操作が行われた場合に変更される時刻情報
    - mtime(time of last modification)
      - 書き込み、ディレクトリエントリの作成、削除等
    - atime(time of last access)
      - 読み込み、実行、ディレクトリエントリのルックアップ等
    - ctime(time of last status change)
      - ファイルオーナー、パーミッション変更等
  - 残念ながら、必ずしも信用できるものではない
    - mactimeは上書きは可能
    - 最後に操作された時間しか残らない
      - つまり、履歴が残る訳ではない
    - 時間がたてば上書きされて古い時刻情報は消えゆく

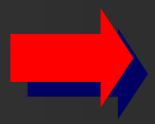
ディスク解析の前提知識

※Linuxの場合

- ファイルが消されるとどうなるか
  - ディレクトリ情報
    - unallocated マークがつく
    - ファイル名とinode番号はそのまま
  - ファイルの属性情報
    - unallocatedマークがつく
    - ctimeに削除時刻が書かれる
    - 参照回数が0になる
    - オーナー、パーミッション、サイズ等の情報はそのまま
  - データそのもの
    - unallocatedされてそのまま残る
- ファイルが消された直後であれば、多くの情報は残ったままとなる

ディスク解析の前提知識

- ファイル情報保存のためのベカラズ集
  - コマンドを実行しない
    - コマンドが不正なプログラムに置き換えられている可能性あり
  - リブートしない
    - 再起動時に何が起きるかわからない
  - 再インストールしない
    - 侵入の痕跡がわからなくなる（特に上書されるとアウト）
  - 電源を抜かない
    - 揮発情報が完全に消える

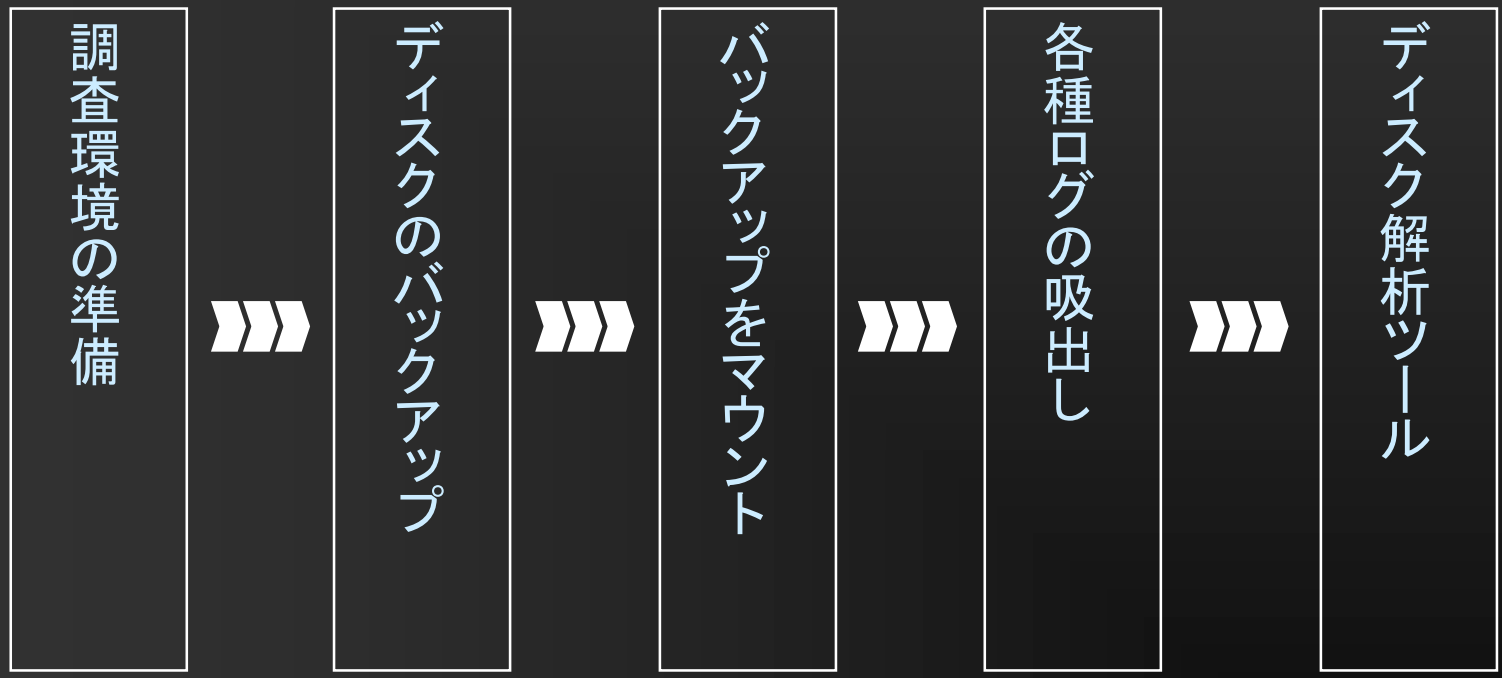


発見した状態を可能な限り保存することを心がける

※被害拡大防止の観点で見ると、そうではないときも多々ある

ディスク解析の前提知識

作業のおおまかな流れ



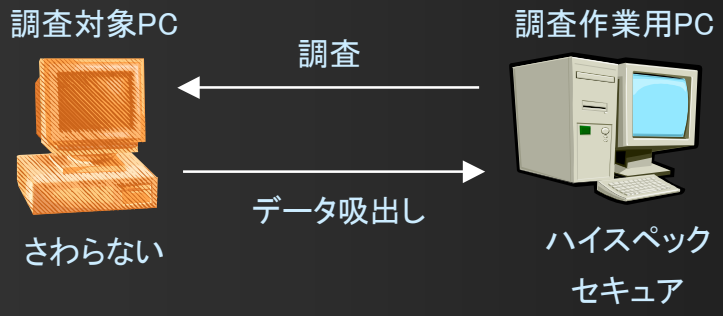
ディスク解析に必要な準備

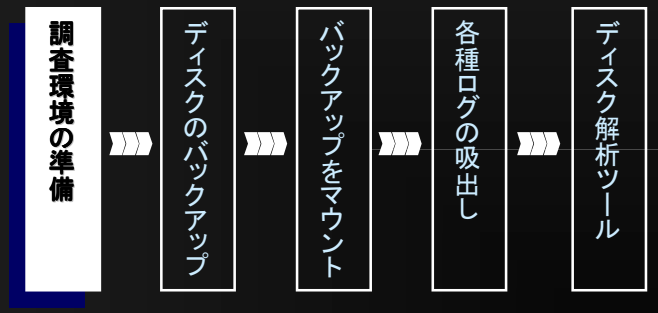
ディスク解析に必要な準備

- ディスクの解析でわかるかもしれないこと
  - プログラムやファイルの改ざんの有無
  - 不正なデータやプログラムの有無
  - 削除されたファイルの復旧
  - 時系列でのファイル操作履歴
  - 特定のキーワードや図形の有無
  - 一部プログラムの操作履歴
- これ以上のことを知りたいのであれば、他の方法を併用する
  - ネットワークの記録
  - 聞き込み　　・・・等

ディスク解析に必要な準備

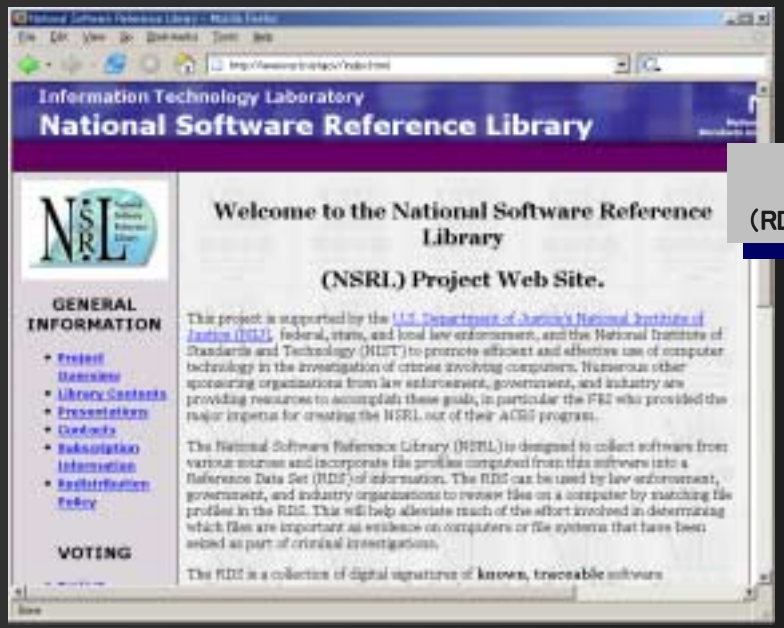
- 調査作業用の環境
  - 調査するためのPCは安全でなければならない
    - OSのハードニング
    - 最新パッチの適用
    - rootkitのチェック
  - ディスクの吸出しから調査まで孤立したネットワーク内で行えると吉
  - CD-ROMから起動するForensic専用Linuxなどを使う方法もある
    - Helix（おすすめ）
    - F.I.R.E.
    - Penguin Sleuth Kit
  - 調査作業用PCはハイスペックなものが望ましい
    - データ量は2倍、3倍に膨れる





ディスク解析に必要な準備

- チェックサム
  - システムファイルが改ざんされていないかのチェックに使用する
  - 以下のようなチェック方法を使う
    - インストール後のMD5を保存しておく
      - 例：find / ¥(-fstype devpts -o -fstype iso9660 ・・・ ¥) -prune -o -type f -exec md5sum {} ¥;
    - RDS(Reference Data Set)等を利用する
      - iso形式なのでマウントしてファイル NSRLFile.txtを読めるようにしておく
    - RedHat等であればrpmコマンドを使用する
      - rpm -checksig packagefile

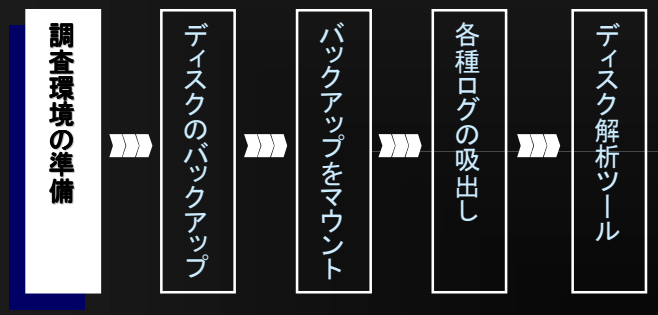


NSRLのWeb
（RDSがダウンロードできる）

調査環境の準備 → ディスクのバックアップ → バックアップをマウント → 各種ログの吸出し → ディスク解析ツール

ディスク解析に必要な準備

- 作業用ユーティリティの導入
  - ネットワーク経由のデータ送受信に使用
    - netcat
      - ネットワーク経由のデータ読み書きツール
  - コマンドの汚染チェックに使用
    - chkrootkit / rkhunter
      - rootkitの検出ツール
  - ディスクデータの分類に使用
    - TCT (The Coroner's Toolkit) / sleuthkit(おすすめ)
      - ディスクイメージからファイルデータの分類ツール
  - 解析操作性向上のために使用
    - autopsy
      - フォレンジックブラウザ(おすすめ)



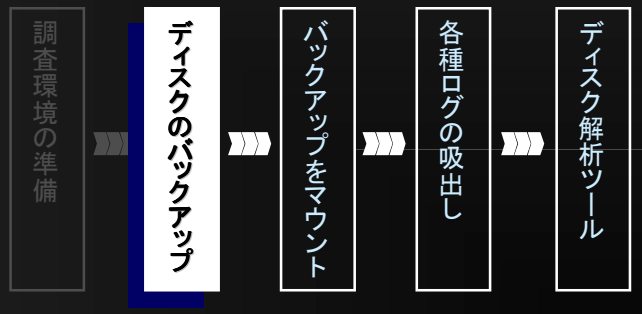
ディスク解析に必要な準備

- ディスクイメージの取得
  - 被害を受けたディスクをそのまま操作してしまうと、情報が変更されてしまうため、複製したディスクを解析する
  - 複製方法
    - 専用ハードウェアを使用して複製を行う
    - ソフトウェアを使用して複製を行う
      - dd
        - ほとんどのUNIXに標準でインストールされている。(おすすめ)
      - sdd
        - 多機能版dd。フォレンジックツールでサポートされる
      - dcfldd
        - US DoD拡張版dd

        ※DCFL = DoD Computer Forensic Laboratory
    - ディスク全体をバックアップ

      dd if=/dev/hda of=image.dd conv=noerror
    - 必要なパーティションのみをバックアップ

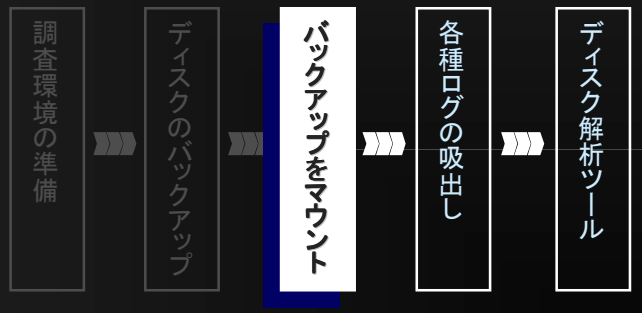
      dd if=/dev/hdaX of=imageX.dd conv=noerror



ディスク解析に必要な準備

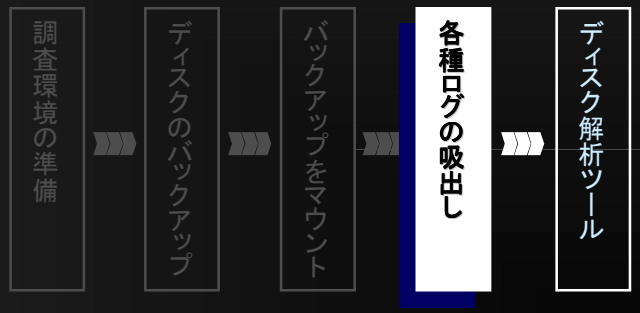
- ディスクのマウント
  - ddで取得したイメージはそのままではファイルシステムとして読み出せない。ddイメージをローカルにマウントすることでアクセス可能となる
  - 例：EXT3のディスクに含まれる1パーティションをddでimage.ddというファイル名でダンプし、それを/mntにマウントする場合
    - mount -t ext3 -o loop,ro /tmp/image.dd /mnt
  - 複数のパーティションをまとめてddした場合はlosetupしてからmountする
    - losetup -o ClinderNo /dev/loopX image.dd
    - mount -t ext3 -o ro,nodev,noexec /dev/loopX /mnt
      - パーティションが始まるシリンダー番号が必要
      - fdisk -lu image.dd等で調べる
      - インストール時に記録しておく

※ autopsyを使用する（後述）場合は
パーティションごとにファイルが別に
見える必要がある



ディスク解析に必要な準備

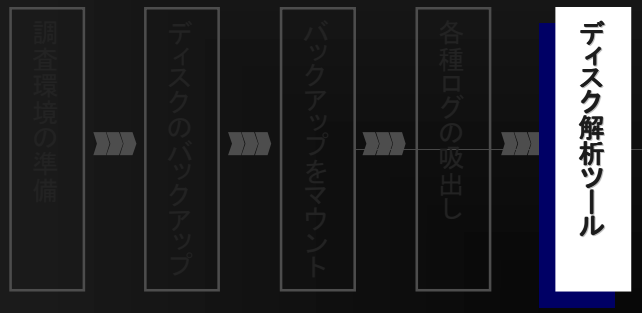
- 各種ログの吸出し
  - 前セッション「ログ管理・解析」をご覧ください :-)



解析ツール

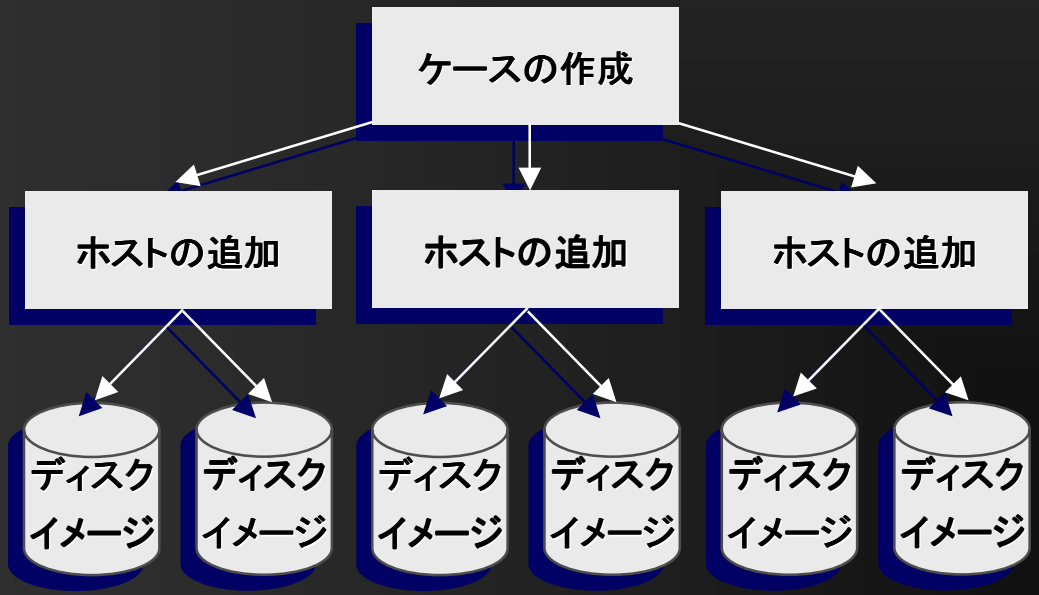
解析ツール

- sleuthkit
  - ディスク解析を効率的に行うためのソフト
  - TCT(The Coroner's Toolkit)をベースとしている
  - ディスクのダンプファイルを解析するためのコマンド群
  - その他の解析ツールのベースとなることが多い



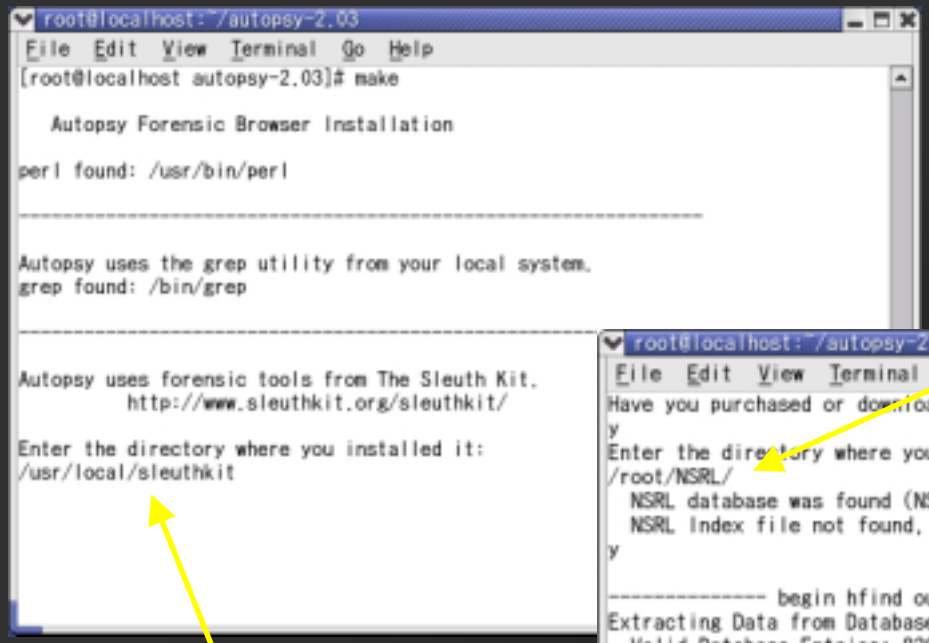
解析ツール

- autopsy
  - ディスクの解析ツール。sleuthkitのフロントエンド
  - autopsy操作手順
    1. 調査ケースの作成
    2. 調査ケースへ対象ホストの追加
    3. 対象ホストへ調査ディスクイメージを追加
    4. タイムラインの作成とファイル解析



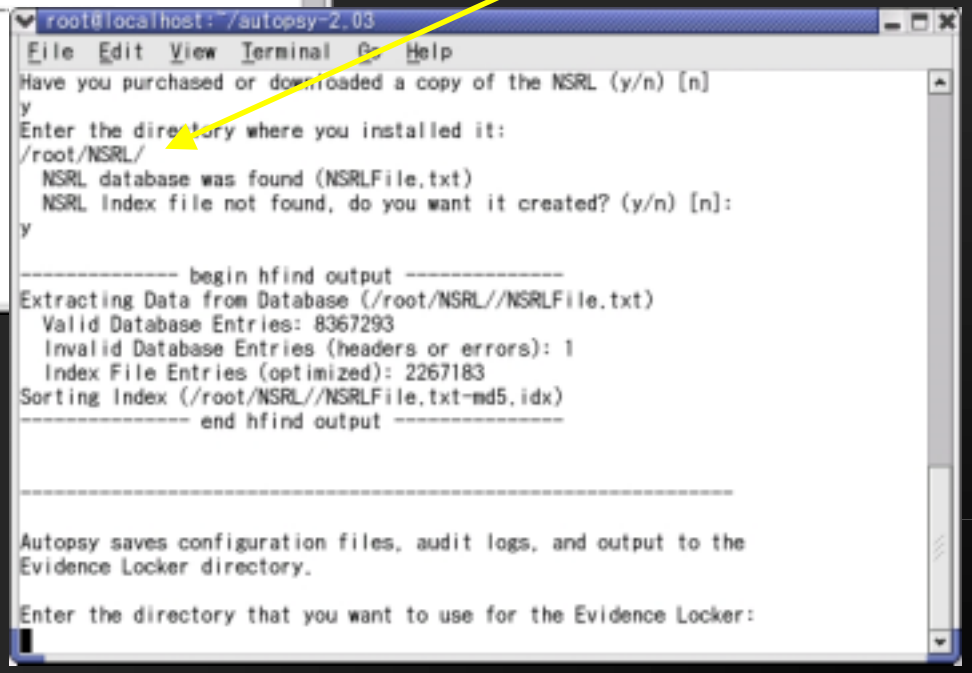
解析ツール

- autopsy
  - インストール



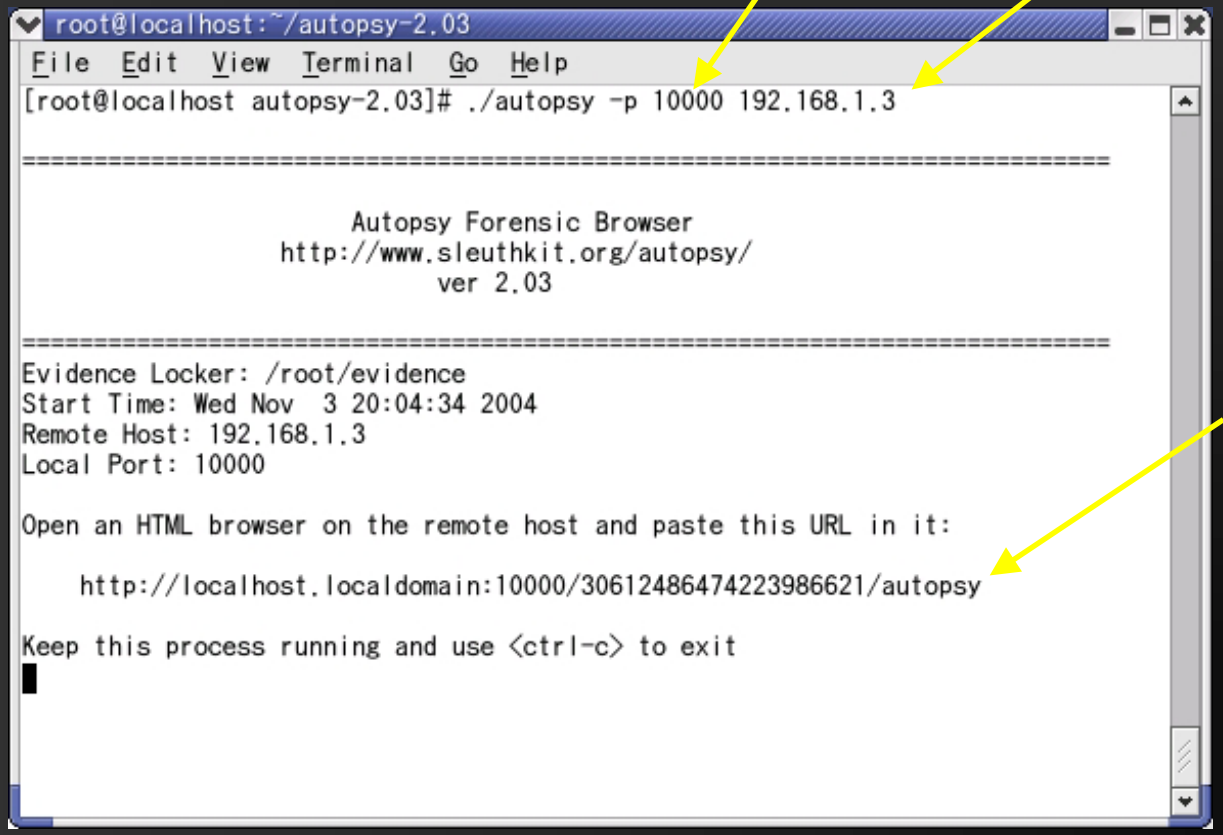
Sleuthkitがインストール
されているpathを入力

NSRLが展開されている
Pathを入力



解析ツール

- autopsy
  - インターフェースはブラウザを使用
  - ランダムな数字列はautopsyを起動する毎に変わる



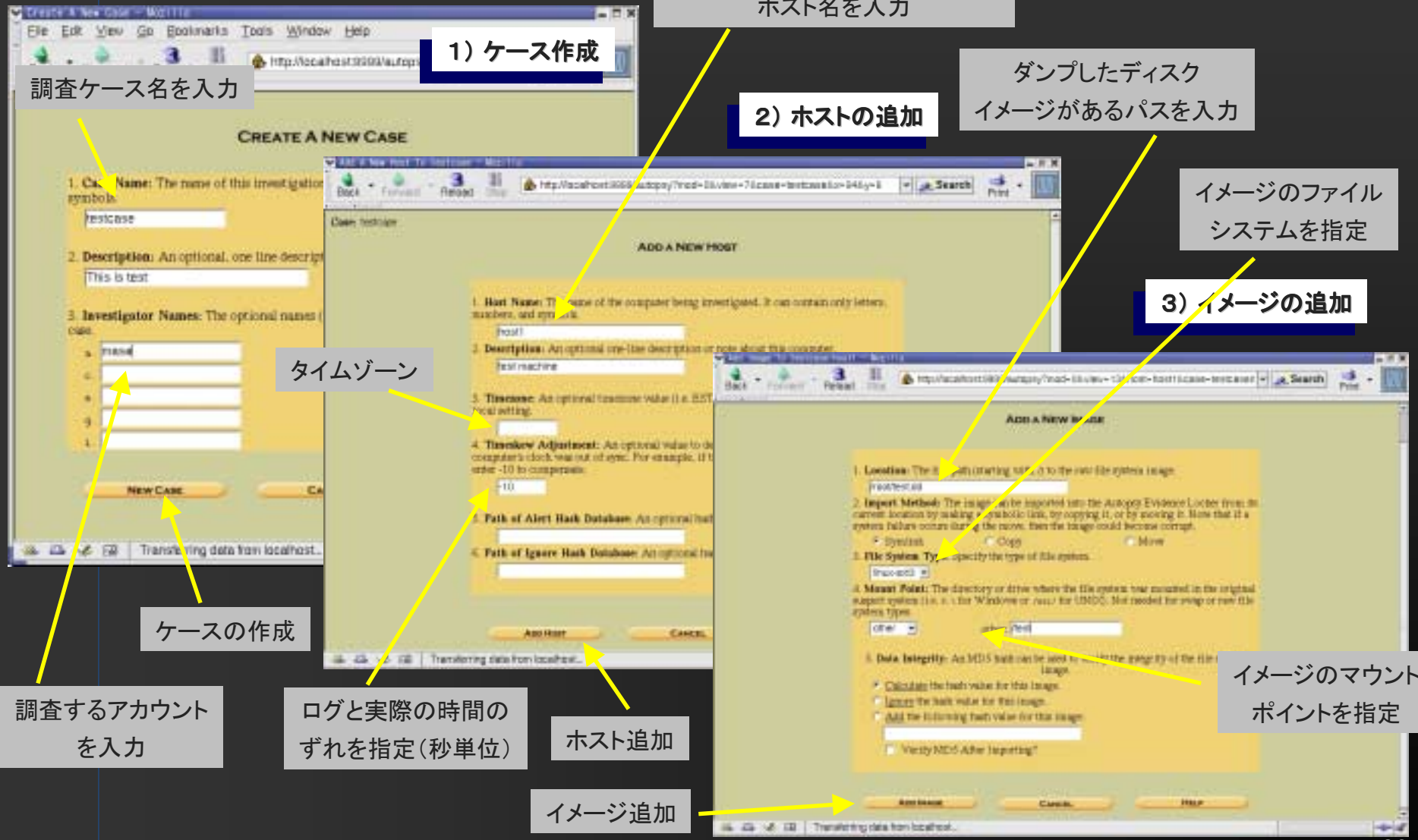
解析ツール

- autopsy
  - autopsy起動画面

ここからスタート

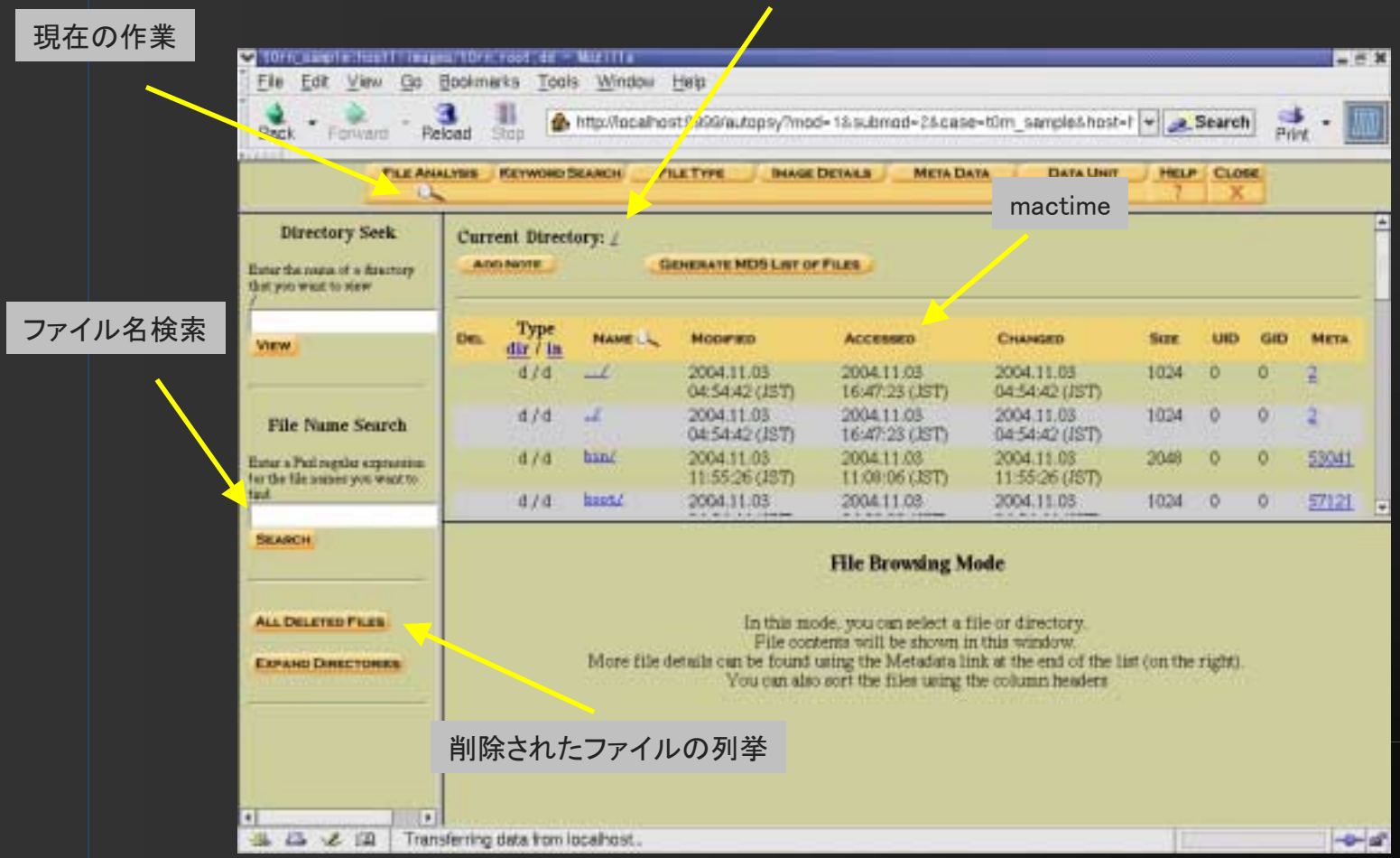
解析ツール

autopsyへの登録



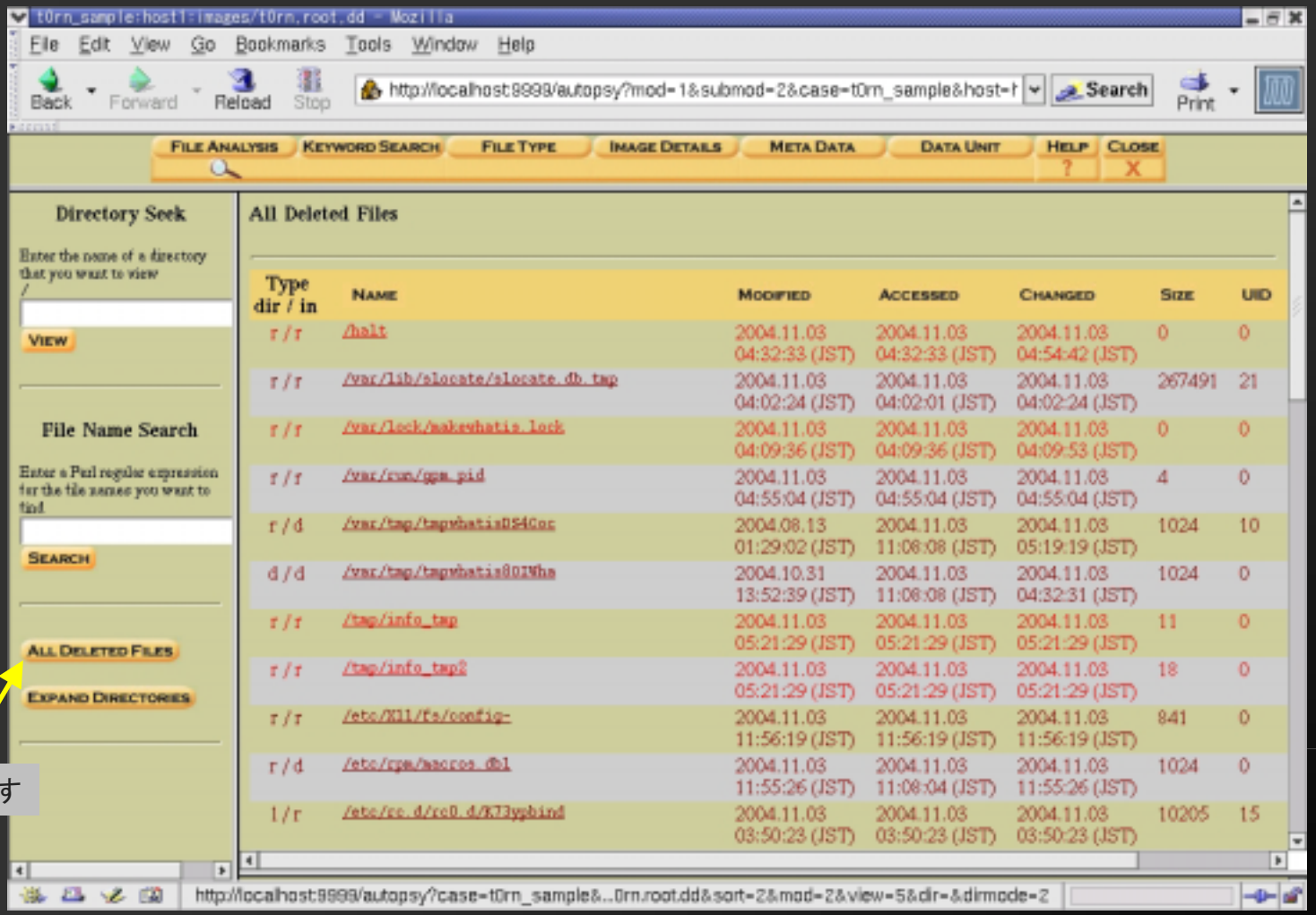
解析ツール

- autopsy
  - ディレクトリの復元



解析ツール

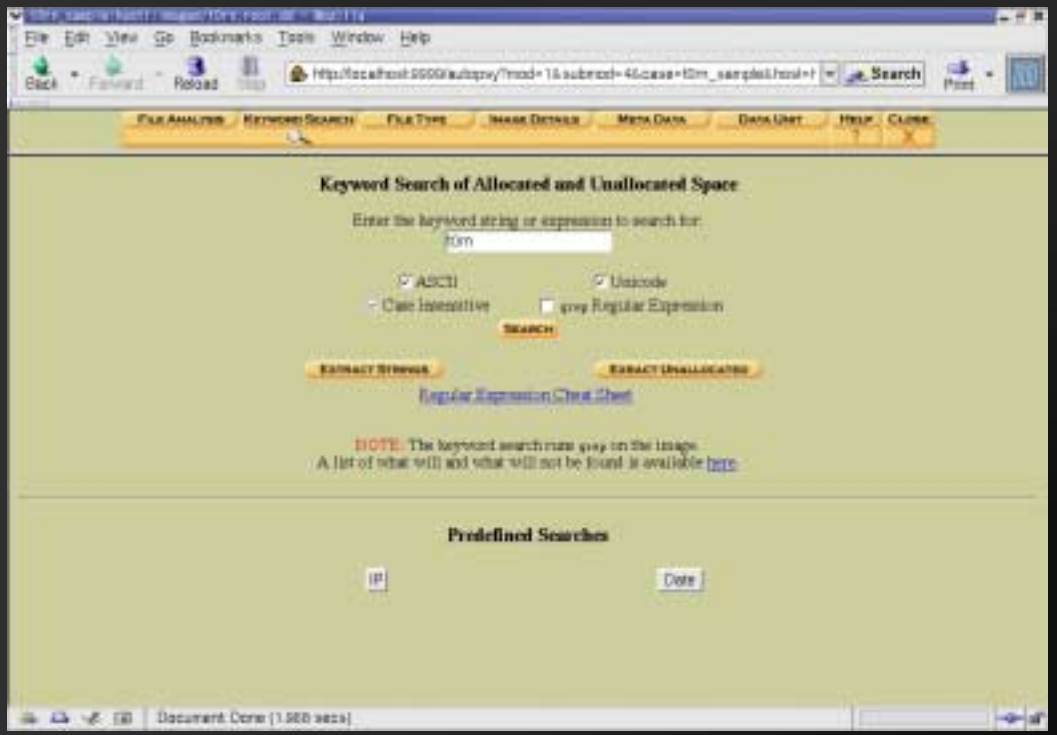
- autopsy
  - 削除されたファイル一覧



ここを押す

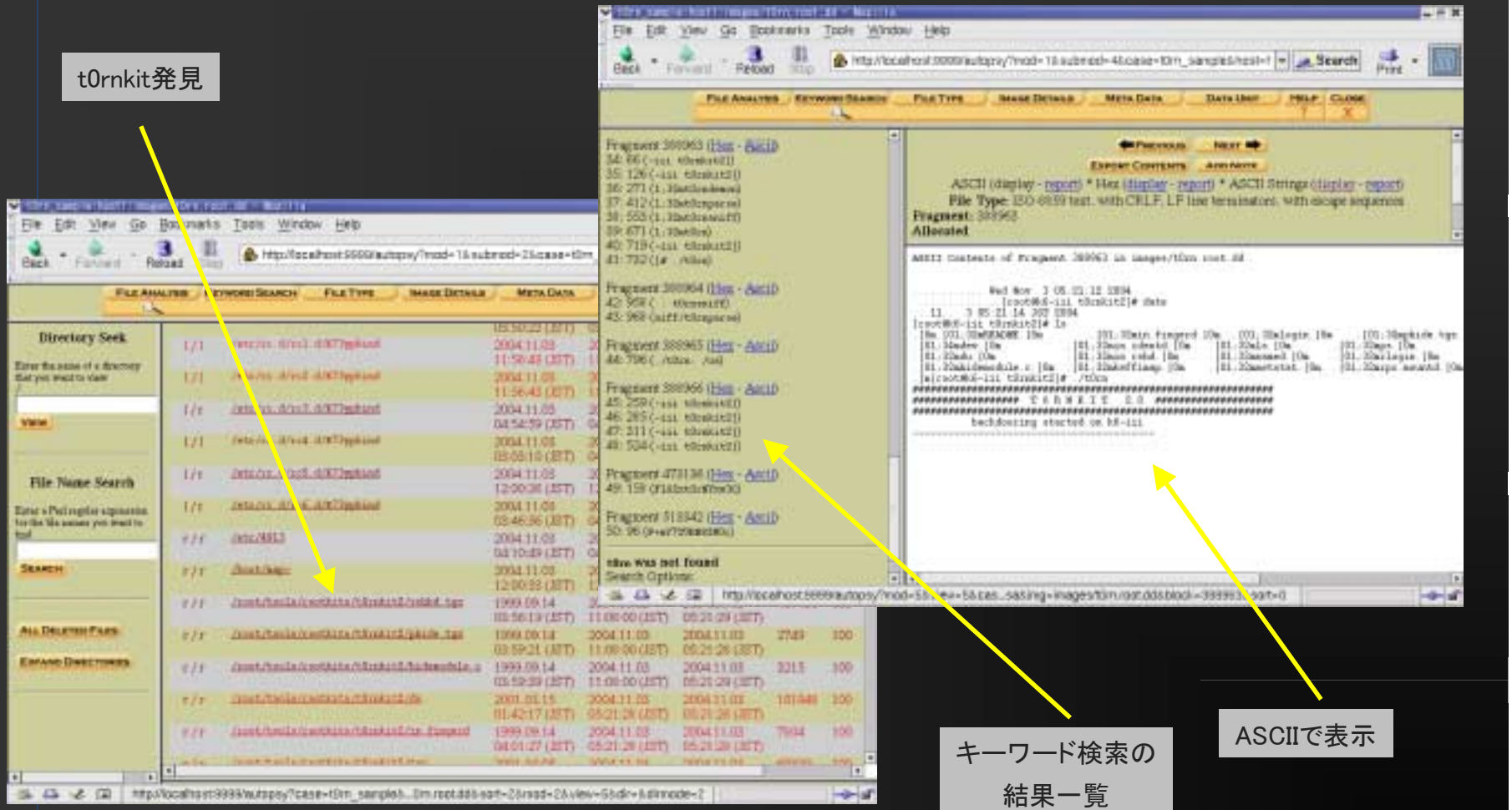
解析ツール

- autopsy
  - キーワード検索
    - キーワード検索は意外と困難
      - キーワードを知っている量がそのまま調査の質に結びつく
      - 1文字変更してあるだけで検出できなくなる可能性
      - ディスク容量が大きくなるほど検索時間が膨大になる
        - 30分、1時間はすぐ過ぎる
      - 力技であり、あくまでも補助的な手段



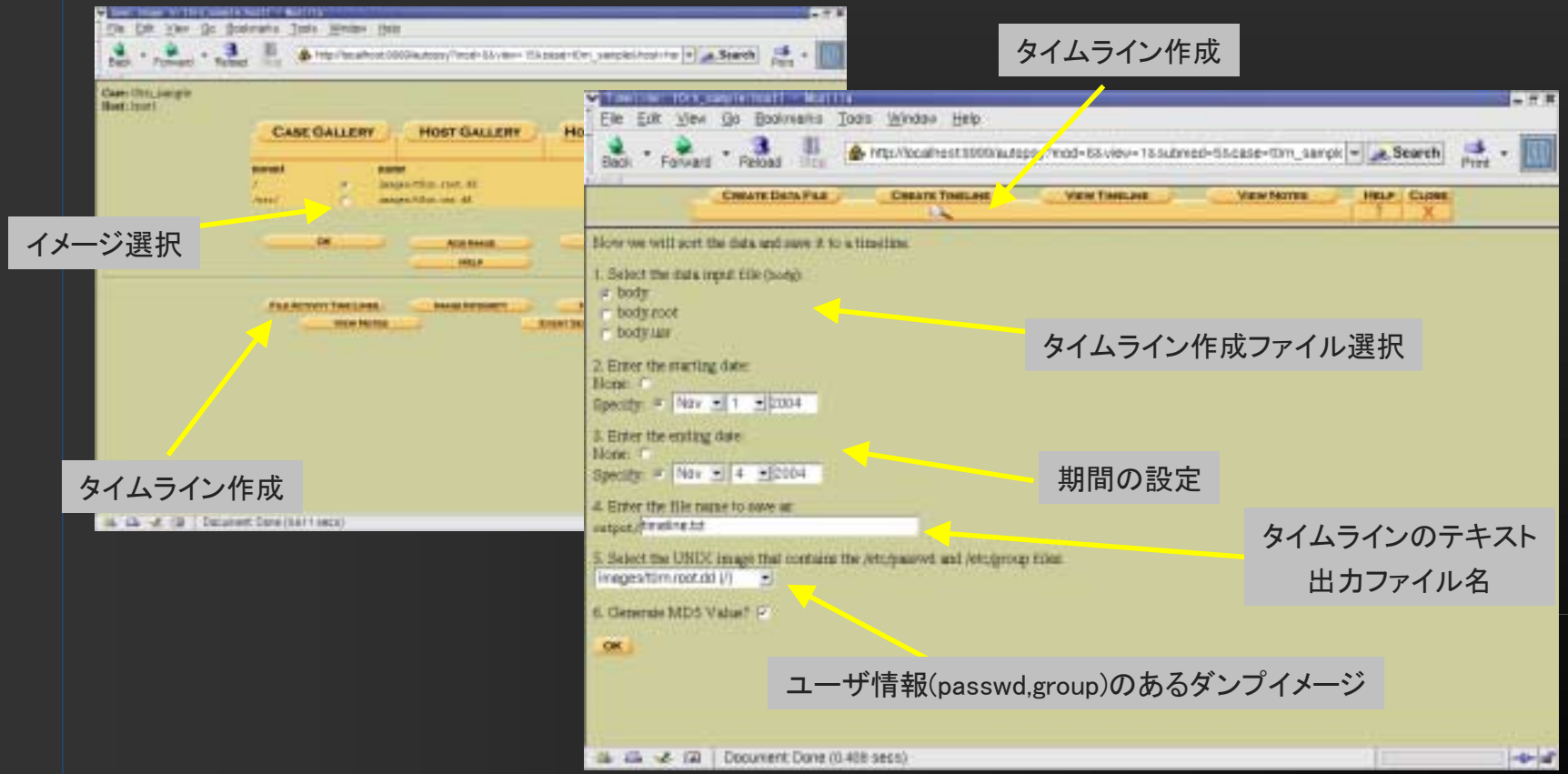
解析ツール

- autopsy
  - キーワード検索の結果例



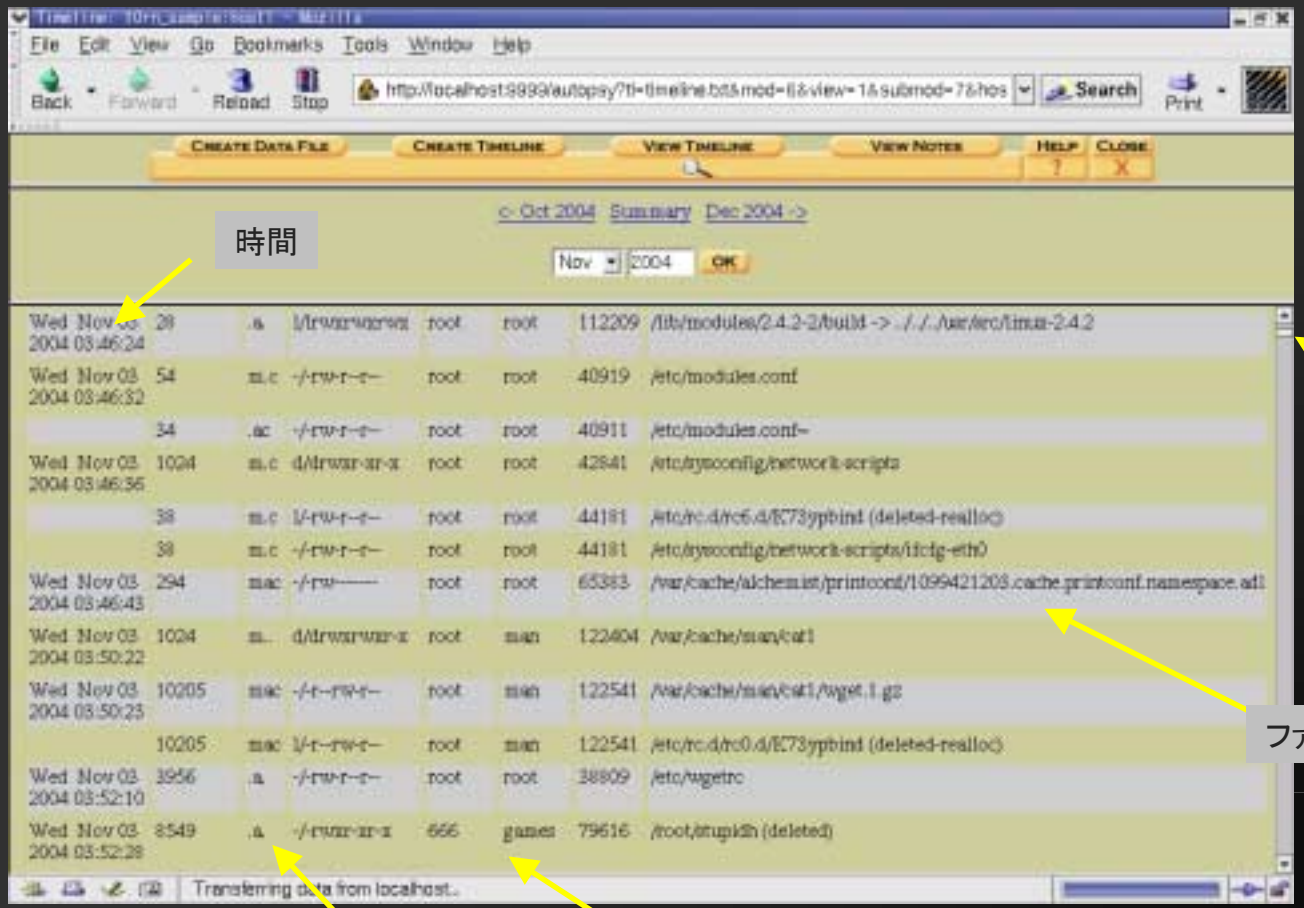
解析ツール

- autopsy
  - タイムライン(時系列情報)の作成
  - これがメインの作業
  - 時系列の変化を追うことで不審な行動がないかどうかを調べる



解析ツール

- autopsy
  - タイムラインを読む

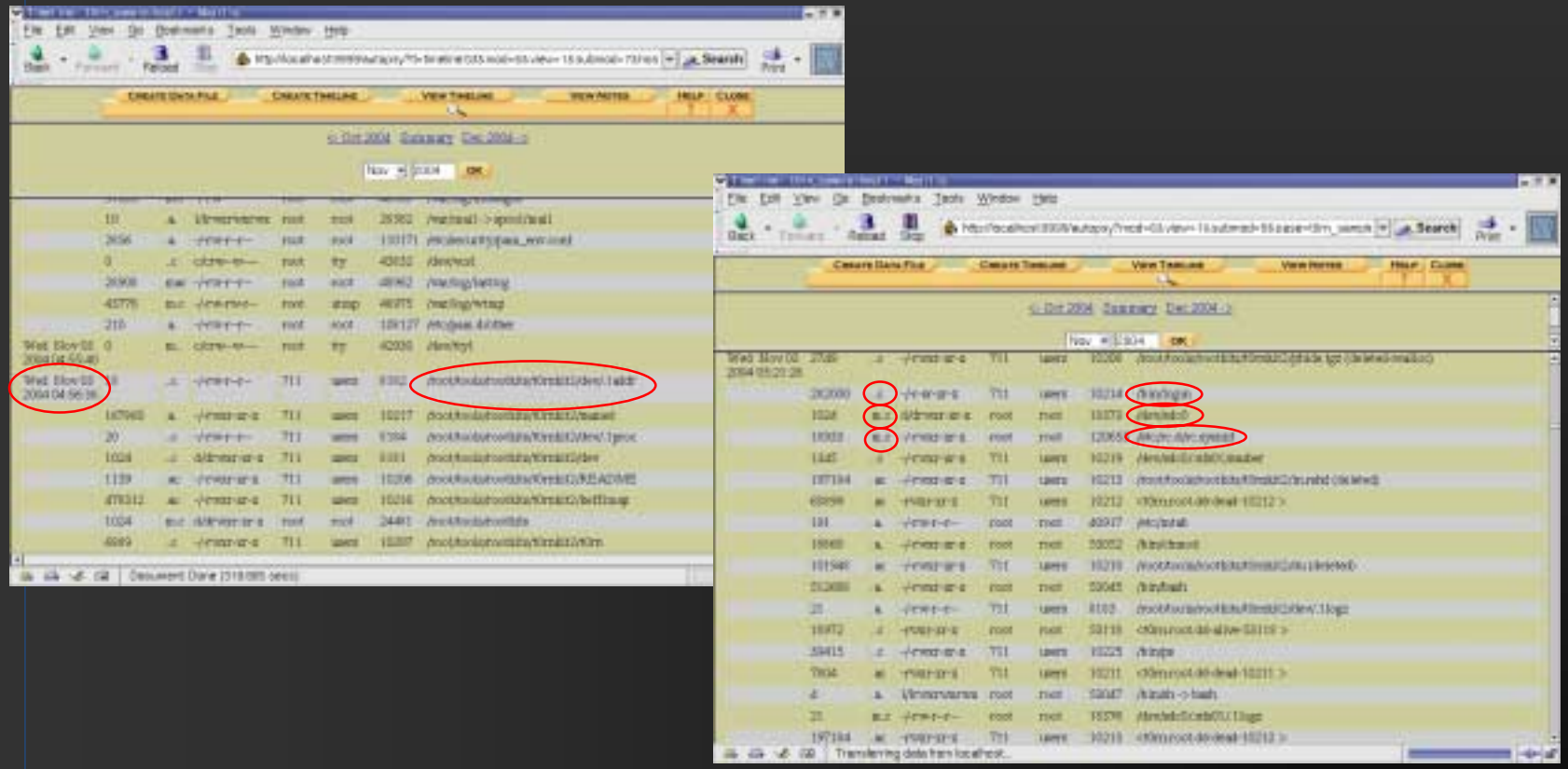


解析ツール

- 今後の検討課題
  - データ量の問題
    - 現在のファイル容量では、シーケンシャルにデータを処理する方式は限界
    - 検査を行うためのPCに対する要求スペックが高すぎる。現実に手に入るPCでは処理が遅くて時間が非常にかかる
  - 時刻の精度の問題
    - DOS/V機のクロックの精度が悪い。せめて月に数秒ずれくらいにして欲しい
  - シグネチャ
    - このコマンドを実行すると、このタイミングでこのファイルがこう変更されるはず、というようなまとまったデータが必要
    - ネットワークやクライアントPCでは実現できている（IDSとかウィルススキャン）ので、そう難しくはないはず
    - ここをインテリジェントに処理してくれれば、作業量は相当減るはず

解析ツール

- autopsy
  - 運良く発見できた場合



これで何もわからなかったらどうする？？？

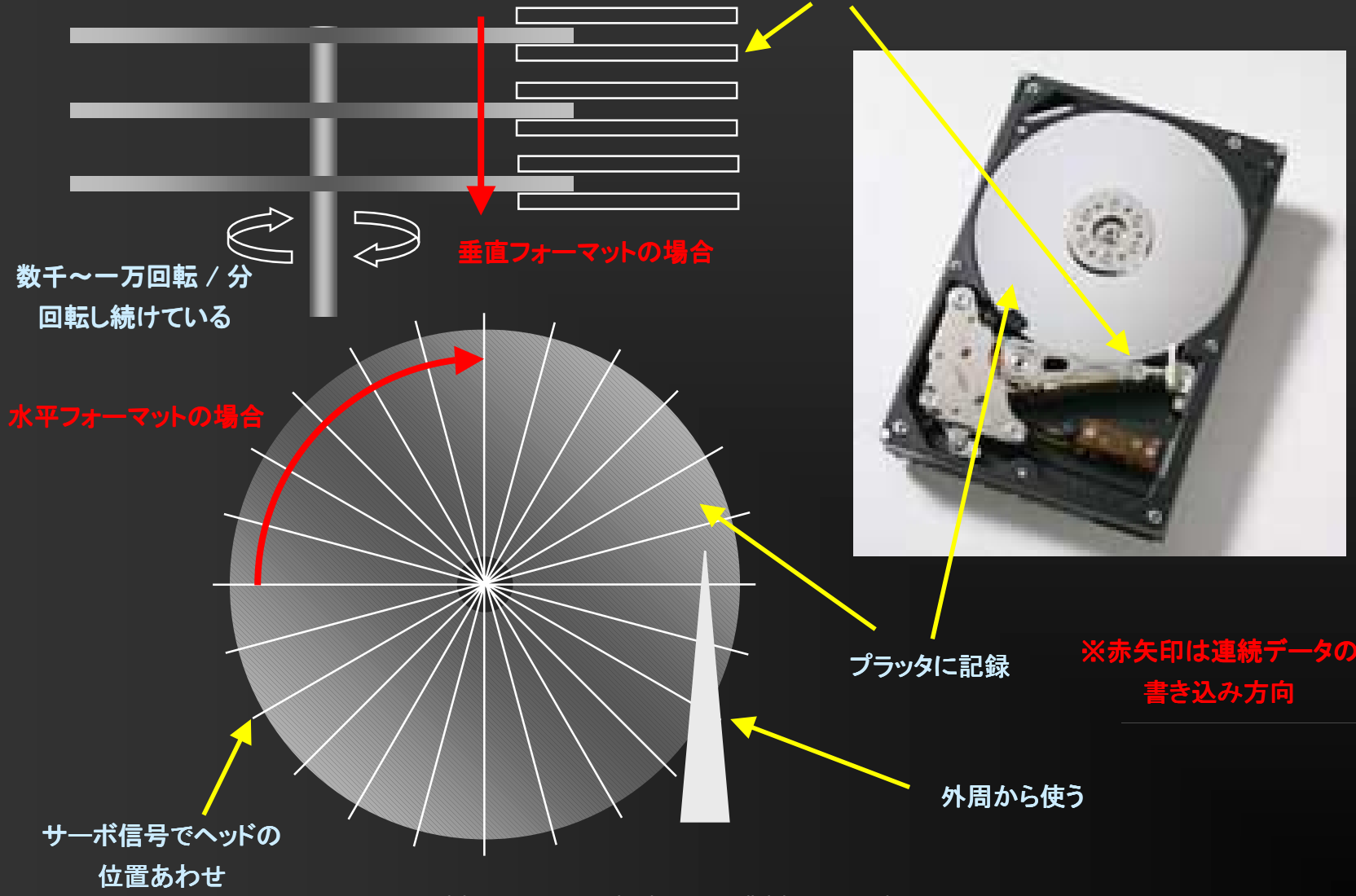
HDDデータ復旧の可能性

HDDデータ復旧の可能性

- ddでダンプしたディスクを調べても有効なデータは出てこない場合、それで終わりと言えるか？
- ディスクは1回消しただけでは「完全に」消えてないと言われているが本当？
- ダンプ以外にハードディスクからデータを読み取る方法はないのか？

HDDデータ復旧の可能性

ディスクドライブの仕組み



HDDデータ復旧の可能性

- ATA
  - AT Attachmentの略
  - ハードディスクのインターフェース仕様
  - CD-ROM等を接続するためにATAPI(ATA Packet Interface)が制定
  - ネットワークと同じようにホスト(CPU)とデバイス(HDD)間で決まったプロトコル(コマンド)を使い、データのやり取りをする

- ディスクの読み書き場所の指定について
  - 現在はLBA方式(Logical Block Addressing)
  - 論理的な番号で指定し、どこのヘッド、シリンダ、セクタに読み書きするかはディスクがエラーセクタを避けて、自動的に計算して割り出す(なので、単純な掛け算ではない)
  - エラーセクタの情報は工場出荷時に書かれている。動作後に出てくるエラーセクタは随時記録される
  - ディスクの回転誤差は0.02%とか0.03%くらいでトラックの幅はミクロン単位。恐るべき精度での制御が行われている

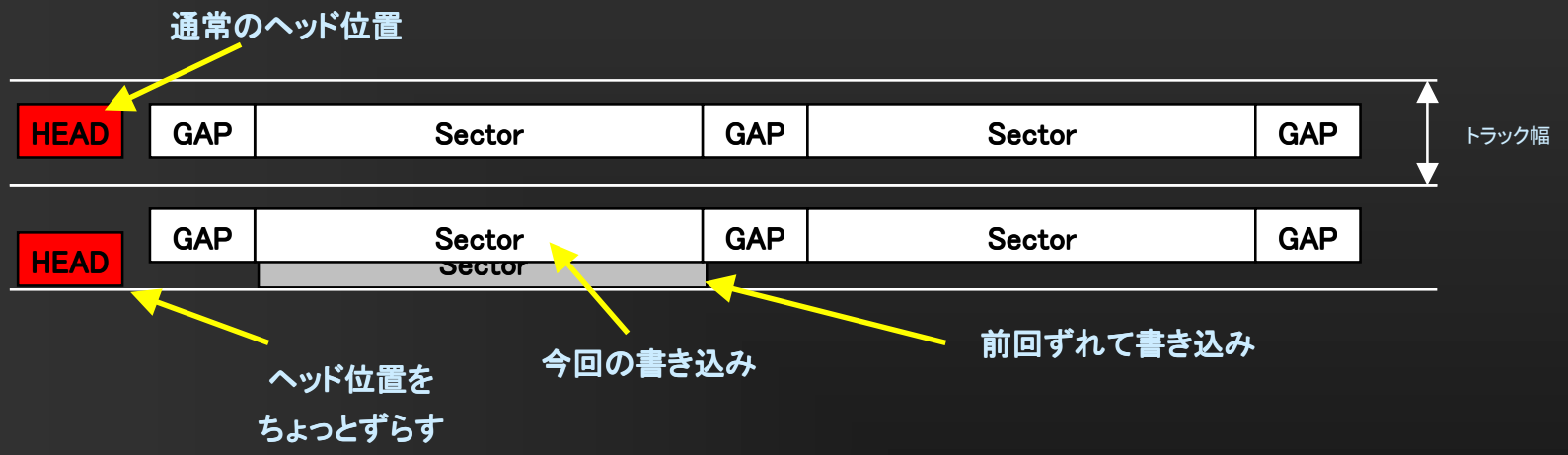
※余談

HDDパスワードは意外と(失礼)強い！？

利用できるなら利用しておくとよい

HDDデータ復旧の可能性

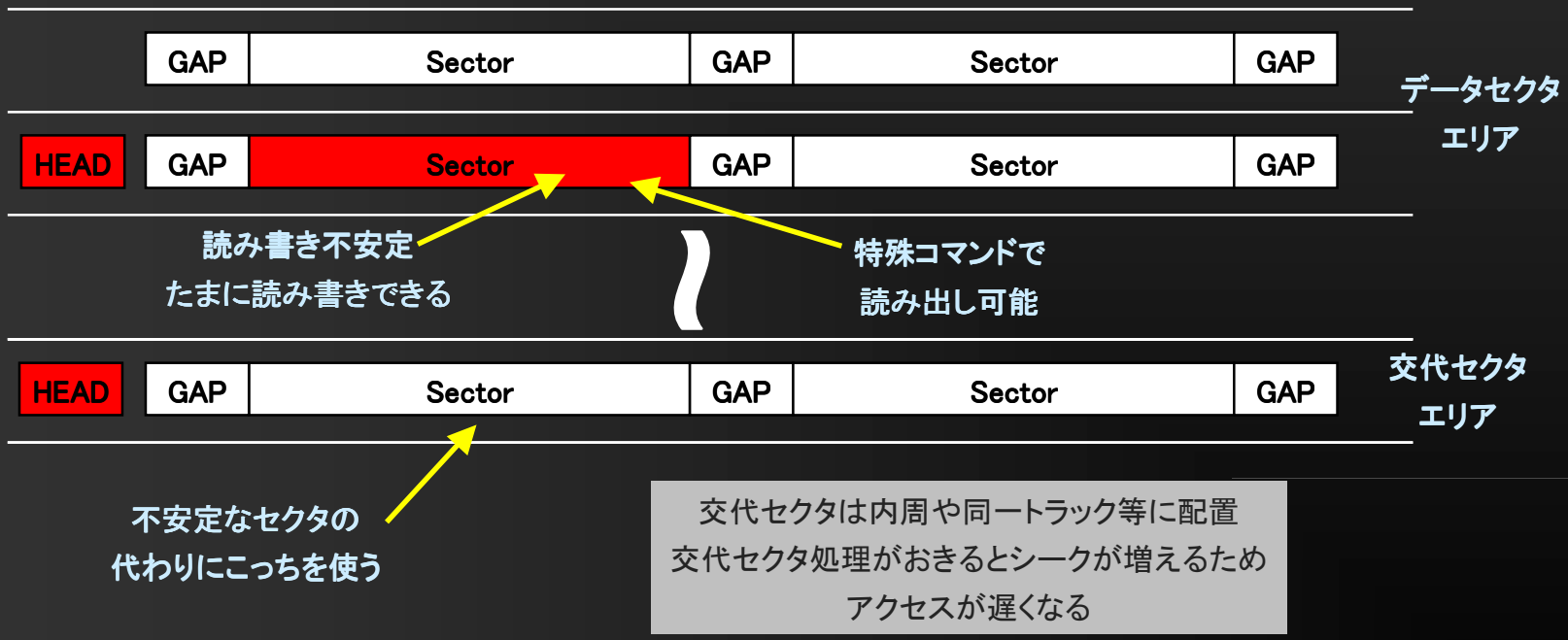
- データの残る可能性
  - オフセットリード・ライト
    - 書き込み誤差でちょっとだけ、位置がずれたものを読み出す



  - ライト不良
    - 以前に書き込みがあり、再度書き込みが発生したが、何らかの原因により書き込みできなければ以前の書き込みが残るので読み出し可能

HDDデータ復旧の可能性

- データの残る可能性
  - 交代セクタ
    - 読み込みや書き込みにおいてリトライしてなんとか読み書きできるようなセクタはスキップし、別の専用エリア（交代セクタエリア）を使ってデータを読み書きする。そのため、旧セクタのデータは残ったままになる。残ったエリアは特殊コマンドで読み出しが可能



HDDデータ復旧の可能性

- 強制的にデータを読み出すことはどこまで可能か
  - コントローラを直接制御
    - 現在のATA仕様では決まったプロトコル内でのやり取りになっており、コントローラを直接制御してディスクを操るのは無理
    - Vender Specificなコマンドを使用すればできる可能性もあるが、当然ながら専用の設備や企業秘密を知らなければできない
  - プラッタを入れ替え
    - 垂直フォーマットでは連続したデータが拾えない
    - そもそもディスクを分解した時点でアウト。クリーンルームのあるオフィスがあれば別かもしれないが。
    - 位相ずれを起こせば元のデータと全く異なるものしか読めない
    - そもそも、出荷時に書かれた制御情報（不良クラスタ等）がないので読み様がない
  - 顕微鏡とかで見る
    - 200GBとか300GBを？
    - 太平洋の中から石ころ1個探すようなもの
    - 微視的に見ることができても巨視的に有効かどうかはわからない
- 膨大な時間とお金と労力をかけて、読み出せるデータはほんのちょっとだけ。実質的には難しい
- 他の方法を考えたほうがよい場合がほとんど

HDDデータ復旧の可能性

- データ量問題
  - ハードディスクの容量は順調に増加している
    - 500GBも登場
  - まだまだ容量は増えつづけると考えられる
- データが破壊されたときのインパクトは増大
  - バックアップは必須となる
- しかし、バックアップが困難
  - HDDのバックアップはHDDで取るしかない
- データ量が増えれば情報処理時間も増える

➡ 今後解決が必要な課題

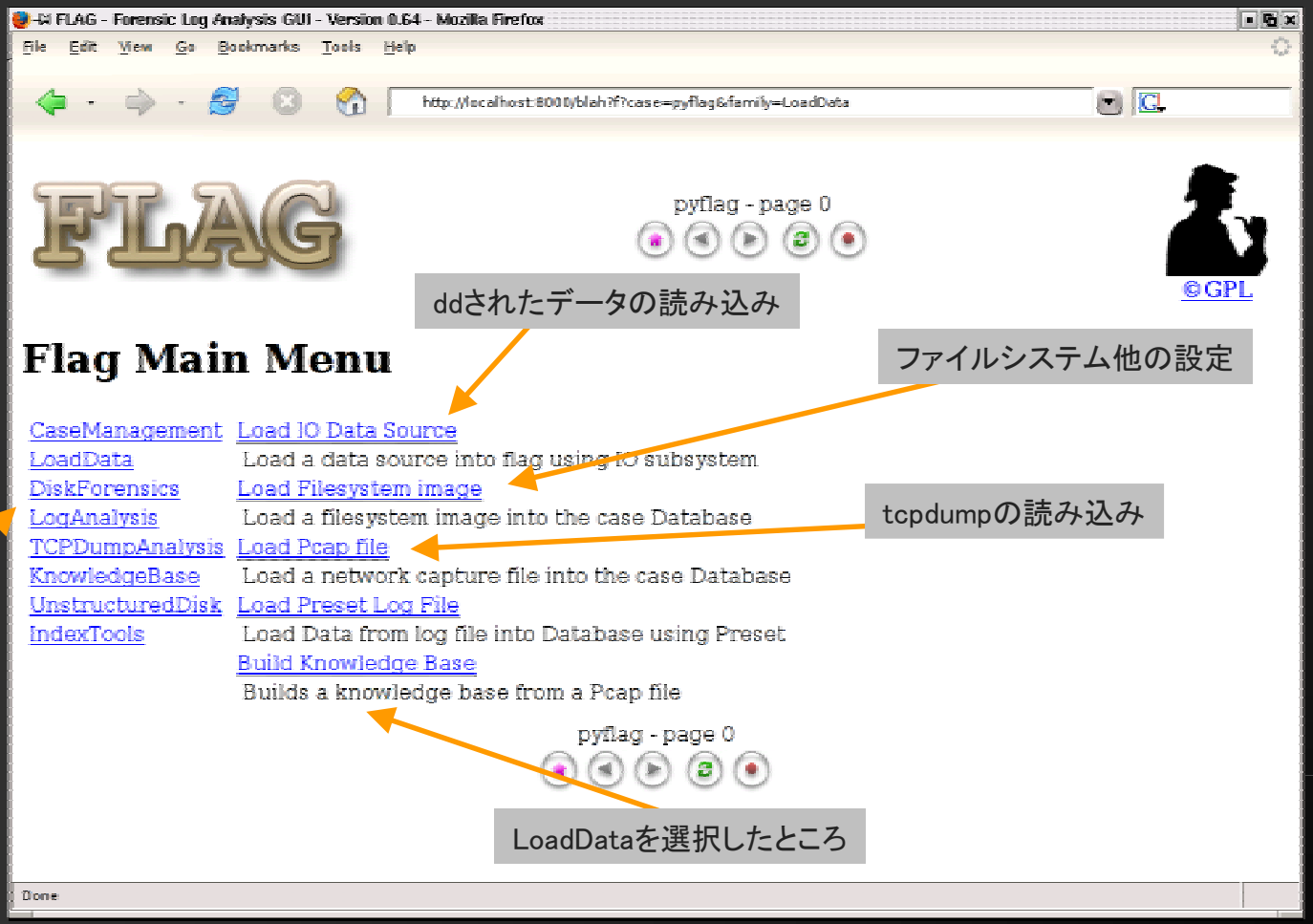
総合的な分析ツール

総合的な分析ツール

- FLAG
  - ディスクダンプ、ネットワークダンプ、ログをまとめて解析するツール
  - データを効率的に処理するため、データベース（mysql）を使用
  - 様々なログフォーマットの読み出しが可能
  - pcap方式のネットワークダンプの分析が可能
  - ddで出力したディスクイメージの読み込みが可能

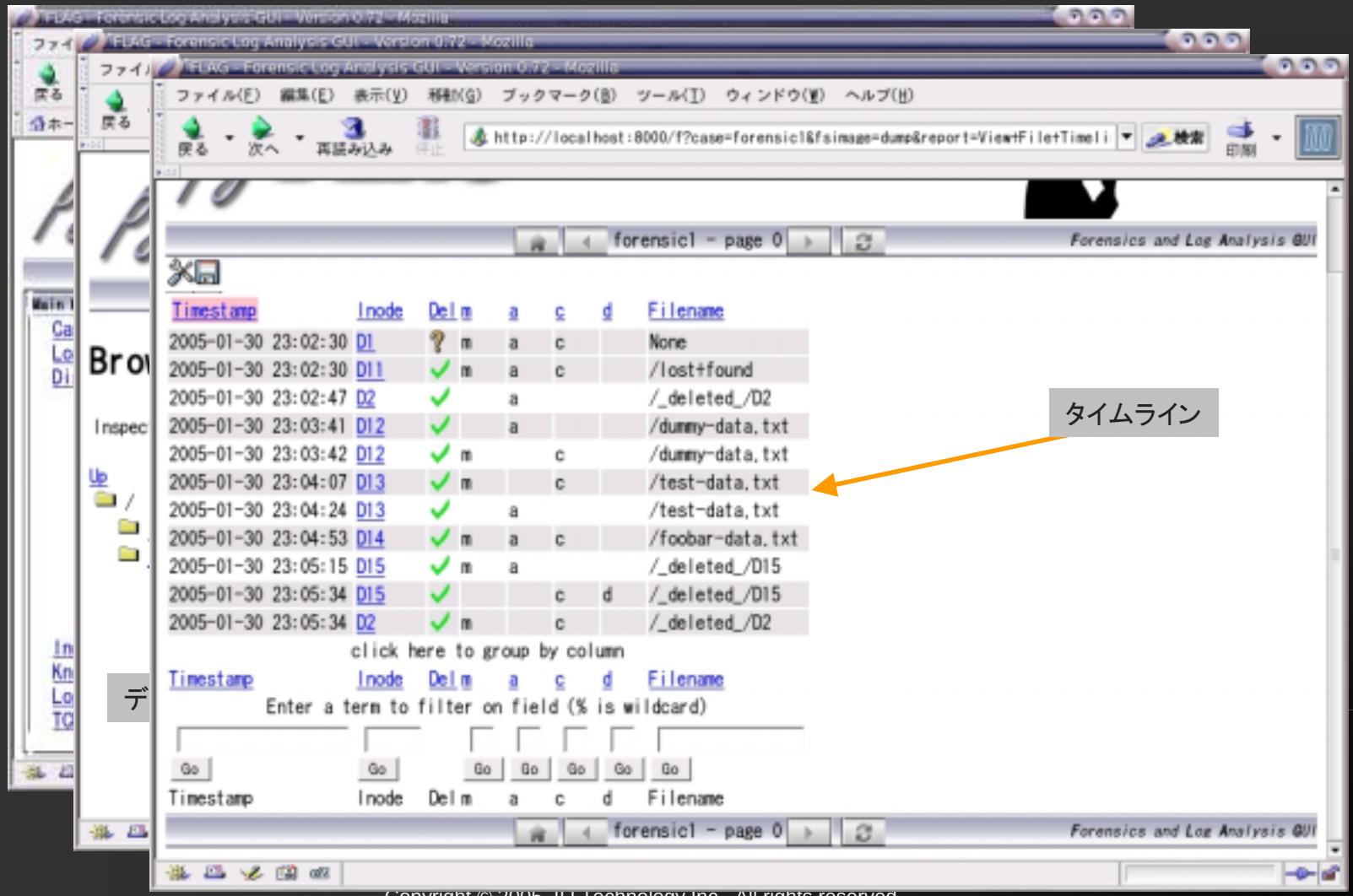
総合的な分析ツール

- FLAG
  - メインメニュー



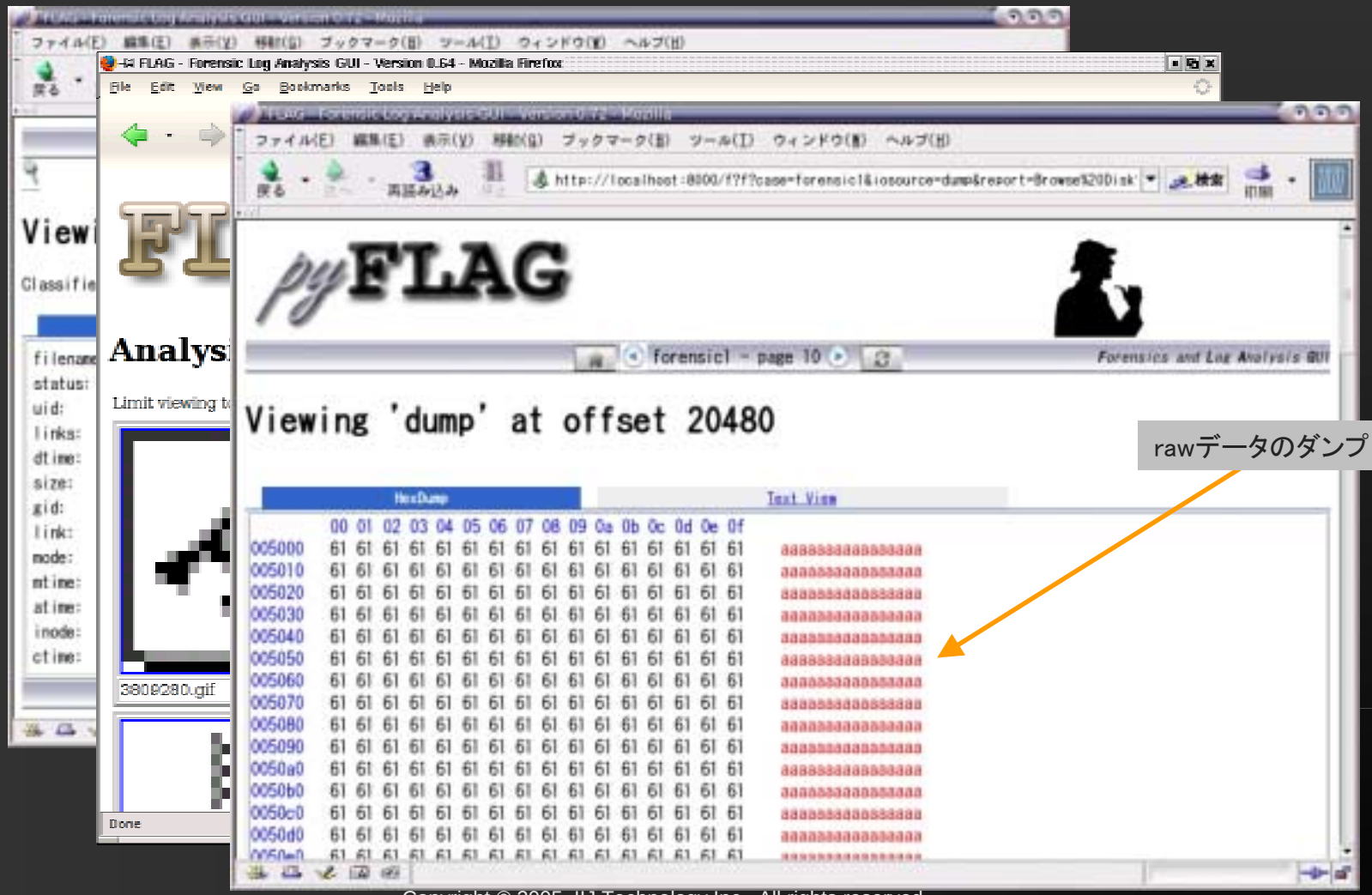
総合的な分析ツール

- FLAG
  - Disk Forensics



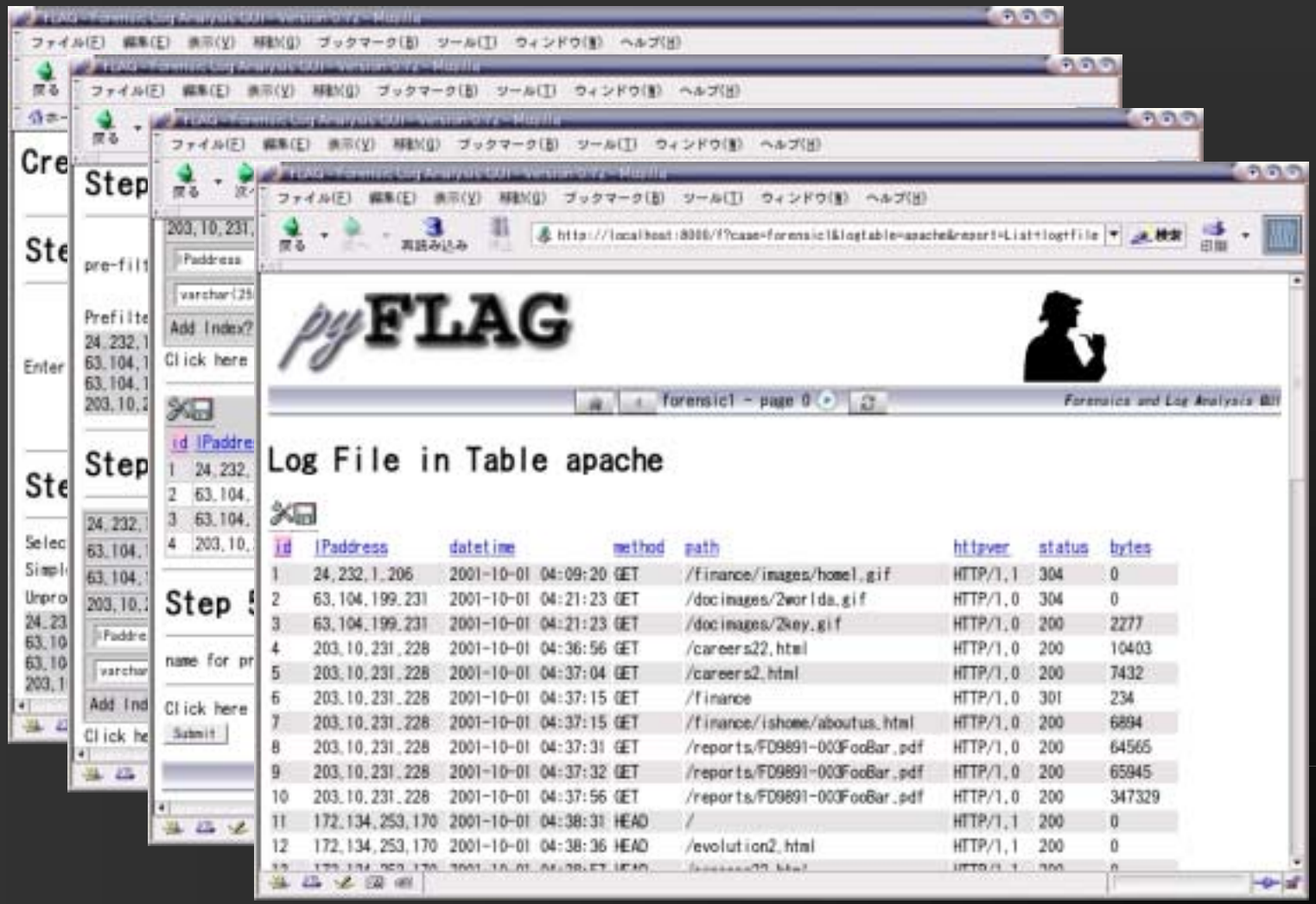
総合的な分析ツール

- FLAG
  - Disk Forensics



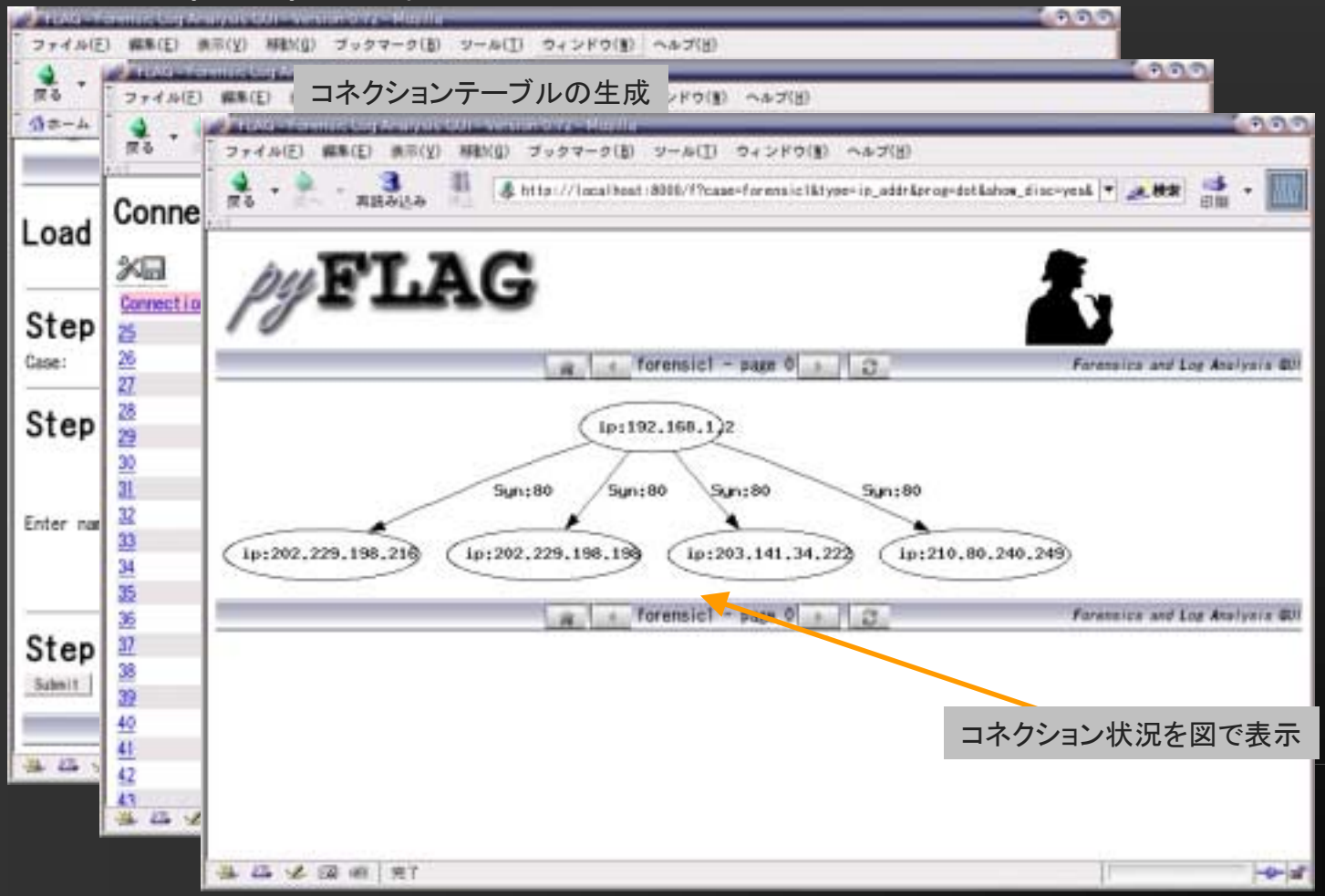
総合的な分析ツール

- FLAG



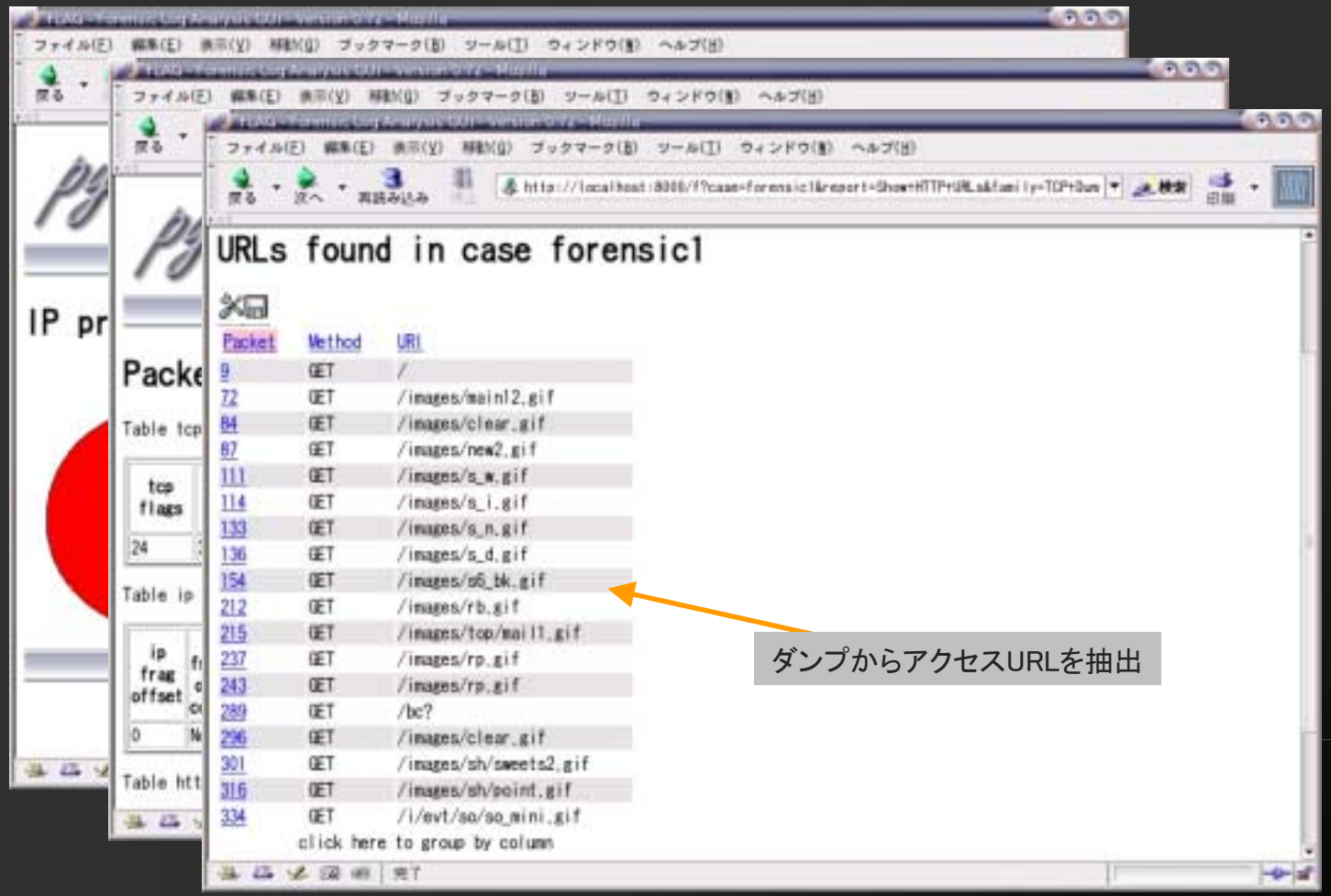
総合的な分析ツール

- FLAG
  - Tcpdump Analysis



総合的な分析ツール

- FLAG
  - Tcpdump Analysis



総合的な分析ツール

- FLAG
  - 現時点での注意点
    - Debian推奨（RedHat系でもOK）
    - mysql入りバイナリパッケージの使用を推奨（pyflag_0.74_bin_mysql）
    - バイナリパッケージではいくつかのpluginがdisableになっている（例えばUnstructuredDiskメニュー）ので、使用する場合は若干手直しが必要
      - 例：plugins/UnstructuredDisk.pycを削除
      - UnstructuredDisk.pyの中のActive=FalseをTrueに変更
    - 複数の別ソフトウェアのインストールが必要
      - Network解析用にethereal
      - グラフ表示用にgraphviz
      - アンチウィルス機能でclamav
    - まだVer 0.7
      - DBエラーとかが時々出る

不正か否かの判断

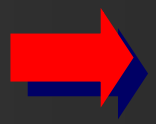
不正か否かの判断

- ありえそうな例え話を一つ
- 勝手にカードが使われていた！
  - ある日カードの明細を見ると、自分で買った記憶が無いものが購入されていた
  - カード管理はきっちり行っている。情報が漏れるはずはない
  - 自分は絶対使っていないので、これはスキミングされたか、システムの不具合
- でも、システム担当者から見ると。。。
  - ログを調べたが本人のアカウントで普通に使用されている
  - カードシステムに不正侵入された形跡は無い
  - スキミングされたのかもしれないけれど、本当にそうかどうかはわからない
  - 利用者のPCが不正侵入されてるのでは？
  - 実は使ったのを忘れているだけでは？
  - 本当は使ってるのに、うそをついているのでは？

情報の不足による判断の限界
不正かどうかはシステムからは判断ができない

不正か否かの判断

- どこまで調べれば判断できるか
  - ログの調査が全て、ではない
  - ディスクの調査が全て、ではない
  - ネットワークの調査が全て、ではない
  - 1台の機器を調べれば終わり、ではない
  - 一人の人間に状況を聞けば終わり、ではない
  - 例えば、アカウントを詐称されていたら？
  - 例えば、有権限者による不正操作だったら？
- 何が正規のアクセスで何が不正なアクセスか？
  - 機械の記録だけでは判断を行うのに十分ではないのは自明



単純な情報収集による
問題解決の限界

- 現実のforensic現場はどうやっている？？？

不正か否かの判断

- real forensicの世界
  - First Responderの役割
    - 現場を確保する
    - 人身の安全を確保する。すでに現場にいる人々だけでなく、これから到着する人々についても
    - 必要に応じてけが人の手当てをする
    - 目撃者、被害者、容疑者を、それぞれ別々の場所に確保する
    - 見張りを置き、活動記録をとりはじめる
    - すべての資料を確保する

ログ
ネットワークダンプ
ディスクダンプ

- 「完全科学捜査マニュアル」より
  - ここまでは単なる情報収集

- 確保された情報はただの「点」
  - 「点」をつなぐ作業が重要
    - 「点」と「点」をつないで「線」に、「線」と「線」をつないで「面」に。しかし、これでもまだ不正かどうかはわからない
  - 不正かどうかはそこにどのような「意図」があるかによる
  - 情報に意図が加わることで有益な判断材料となる

不正か否かの判断

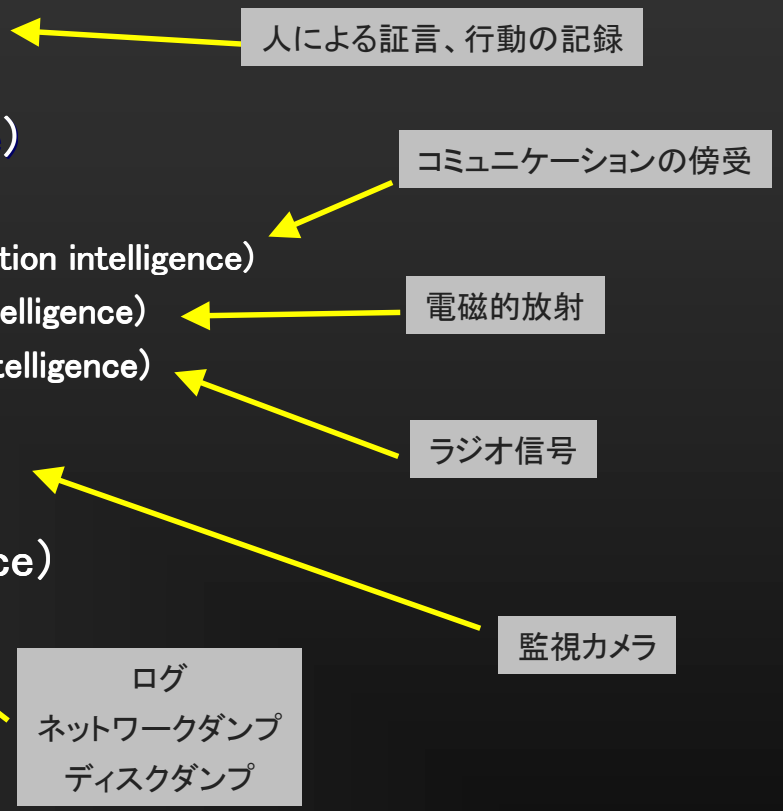
- Intelligence Cycle
  - 単なる「情報」を目的に添った形の「知識」にするプロセス
  - 以下、CIAモデルの例
    - Planning and Direction
      - 計画と指示（要求事項）
    - Collection
      - 情報の収集
    - Processing
      - 情報の加工
    - All-Source Analysis and Production
      - 情報の統合、分析、評価、解釈
    - Dissemination
      - 情報の配布

  - The Intelligence Cycle is the process of developing raw information into finished intelligence for policymakers to use in decisionmaking and action.

※ CIA Webより（http://www.cia.gov/cia/publications/facttell/intelligence_cycle.html）

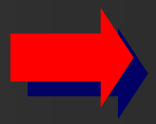
不正か否かの判断

- Intelligence Cycleにおける情報の種類
  - HUMINT（Human intelligence）
    - 人的情報のこと
    - SIGINT（Signal intelligence）
      - 信号情報のこと
        - COMINT（Communication intelligence）
        - ELINT(Electronics intelligence)
        - TELINT(Telemetry intelligence)
    - IMINT(Image intelligence)
      - 画像情報のこと
  - TECHINT（Technical intelligence）
    - 技術情報のこと
  - 多くの情報があればより正確に判断が行える



不正か否かの判断

- 不正か否かの判断をするには
  - 要求事項を明確にし
    - いつからいつまで、何に対して、何のために
  - 要求事項にしたがって情報収集し
    - 人的情報と技術情報の収集
  - 情報を見やすい形に加工する
    - ツール等と使用
  - 時間を軸に情報を整理、判断
  - 要求事項に沿ったoutputを行う

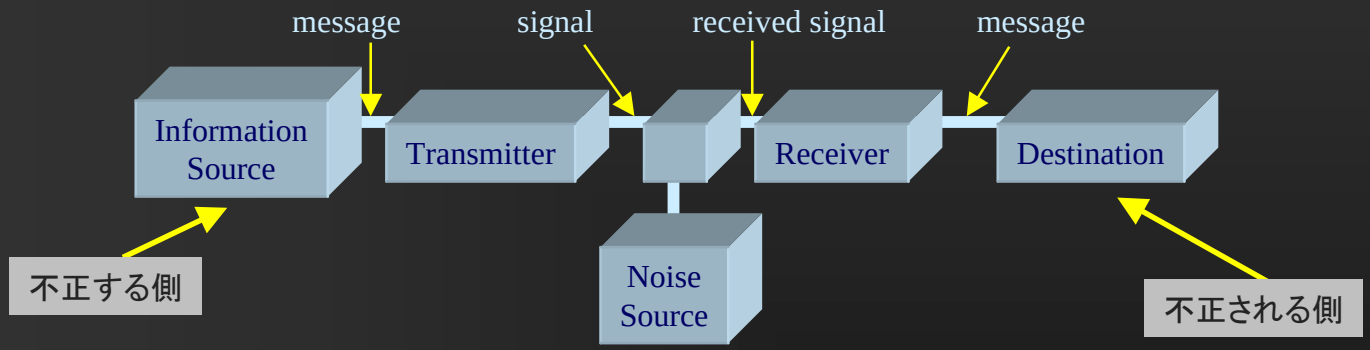


これらを繰り返し
outputの精度を上げる

リスクの発見

リスクの発見

- 情報とは
  - 情報の定義
    - 情報って何？
  - 情報の流れ



- セキュリティとは
  - 誰にとっての安全か
- 情報セキュリティって何？
  - 情報セキュリティも「情報」であることに変わりはない
  - 情報理論から逸脱することはない

リスクの発見

- 情報セキュリティの「リスク」とは何かについて考えてみる
  - リスクが高い状態とは
    - 安全が脅かされる可能性が高い
      - risk = 脅威の発生頻度 x 被害の大きさ（コートニィ理論）
      - risk = threat x vulnerability （SANS Institute）
      - risk = 資産価値 x 脅威 x 脆弱性（BS7799-GAP方式）
    - 脅威や脆弱性が増加すれば安全でなくなる
    - 安全ではない＝不利益をこうむる確率が高い
    - 脅威や脆弱性は不利益を起こす確率をあげる要因
  - 安全＝安定としてみる
    - 安定状態＝変化の少ない状態
    - 変化の少ない状態＝変化する確率が低い状態
  - ここで情報エントロピー
    - 不確定度を表す（確率）
    - 「情報」を得ることで不確定度を減らす
    - 安定＝不確定度が低い
    - 不確定度が低い＝情報エントロピーが低い
  - 脆弱性
    - 内部的な情報エントロピーの増加
  - 脅威
    - 外部的な情報エントロピーの増加

リスクの発見

- リスクが高い状態
  - 情報エントロピーが最大
  - 不確定なことがめちゃくちゃたくさんある
  - こうなると何がおきるかわからない＝不安定＝安全ではない
  - リスクを低減するには、情報エントロピーを減らす。つまり、情報を与える
- 変化を見極める
  - 「巨視的状態」と「微視的状態」
    - 10秒以内に訪れる危機と10万年以内に訪れる危機はどちらがリスクが高いか
    - 10行に1行不正アクセスがあるのと10万行に1行不正アクセスがあるのは同じか
    - 同じ事象でも巨視的か微視的かで異なってくる
    - 不正侵入というのは、おきないはずのことがおきている状態。つまり、確率の低いことが発生している。確率の低いことほど情報量は大きい
  - 「量」と「時間」を考える
    - 情報が多ければ情報エントロピーは減少する
    - 情報エントロピーが減少している状態を作るには、母数を広げるか時間をかける
    - つまり、巨視的に見て情報エントロピーの発生が少ない状態を維持すれば、確率の低いことが発生した場合の影響が大きく、気がつきやすい
  - 定常状態
    - ある目的を達成する場合に定常状態を保って行えば、エントロピーの発生は最小となる
- 要するに・・・
  - 安定した状態の維持があって初めて不正を正確に把握できる、ということ
  - もっと平たく言うと、安定して運用された環境を作りましょう、ということ

リスクの発見

- 変化をとらえる
  - 情報がどう変化しているか？
  - その変化量は？
  - 変化した意味は？

- 例えば
  - IDSとは何をしているのか
    - 微視的状態の変化を検出
  - 定点観測とは何をしているのか
    - 巨視的状態の変化を検出

※IDSや定点観測はもと評価されてもよいはず。
使う側がうまくつかえていないだけ。

  - IDSを定点観測することで精度高く変化をつかむことはできる？
  - 変化がおきたとき、つまり、ネットワークが定常状態から非定常状態へ遷移したとき、安全な状態ではなくなる
  - その安全ではない状態に対して、不正ととらえるかどうか、何らかの「意図」が加わることで初めてIntelligenceとして情報の活用が可能となる

リスクの発見

- 結局、不正侵入を発見するには
  - 不正侵入：意図の把握（人的情報）
  - 発見：情報エントロピー変化量の検出（技術情報）
  - ・・・の把握につきるのではないか
  - IDSを置いていればよいというものではない
  - 特定のキーワードを検出すればよいというものではない
  - 閾値を超えればアラートあげればよいというものでもない

最後に

最後に

- まとめ
  - 最後のほうがぜんぜん具体的じゃないのですが・・・
    - 結局、不正侵入の発見でやるべきことは
      - まず、安定したシステムにすること
      - 継続的に観察しつづけること
      - 情報の収集を心がけること

安定した運用基盤

情報が収集できる仕組み

最後に

謝辞

– 「HDDデータ復旧の可能性」について、株式会社 日立グローバルストレージテクノロジーズの三枝様、高師様、渡部様、上村様に多大なるご協力をいただきました。この場をお借りしてお礼を申し上げます。

最後に

参考文献・URL

- Linux Filesystems HOWTO
- Linux Ext2fs Undeletion mini-HOWTO
- FIRST Conference 2002 “Forensic Discovery & Hawaii” dan farmer & Wietse Venema
- 「Linuxのブートプロセスをみる」白崎博生 著　アスキー
- Sleuthkit http://www.sleuthkit.org/sleuthkit/index.php
- Autopsy http://www.sleuthkit.org/autopsy/index.php
- HELIX http://www.e-fense.com/helix/
- 「セキュリティウォリア」サイレス・パイカリ、アントン・チュバキン 著　オライリージャパン
- 「不正アクセス調査ガイド」渡辺勝弘、伊原秀明 著　オライリージャパン
- 「ATA(IDE)/ATAPIの徹底研究」CQ出版社
- pyFLAG http://pyflag.sourceforge.net/
- 「情報セキュリティ技術大全」ロス・アンダーソン 著　日経BP社
- 「完全科学捜査マニュアル」N.E.ゲンジ 著　河出書房新社
- 「鑑識捜査三十五年」岩田政義 著　中公文庫
- 「なぜ、正しく伝わらないのか」ジョン・ヒューズ＝ウィルソン 著　ビジネス社
- 「インテリジェンス入門」北岡元 著　慶應義塾大学出版会
- CIA Factbook on Intelligence 2002
- 「エントロピーの科学」細野俊夫 著　コロナ社
- 「情報とは」青柳忠克 著　産業図書
- 「時間のなぞ」Newton Press

ご清聴ありがとうございました