Sleuth Kit and Open Source
Digital Forensics Conference
June 9, 2010

The Sleuth Kit Overview and Automated Scanning Features

Brian Carrier

Basis Technology Corporation

P 617.386.2000
800.697.2062 (toll-free)
F 617.386.2020
W info@basistech.com
www.basistech.com

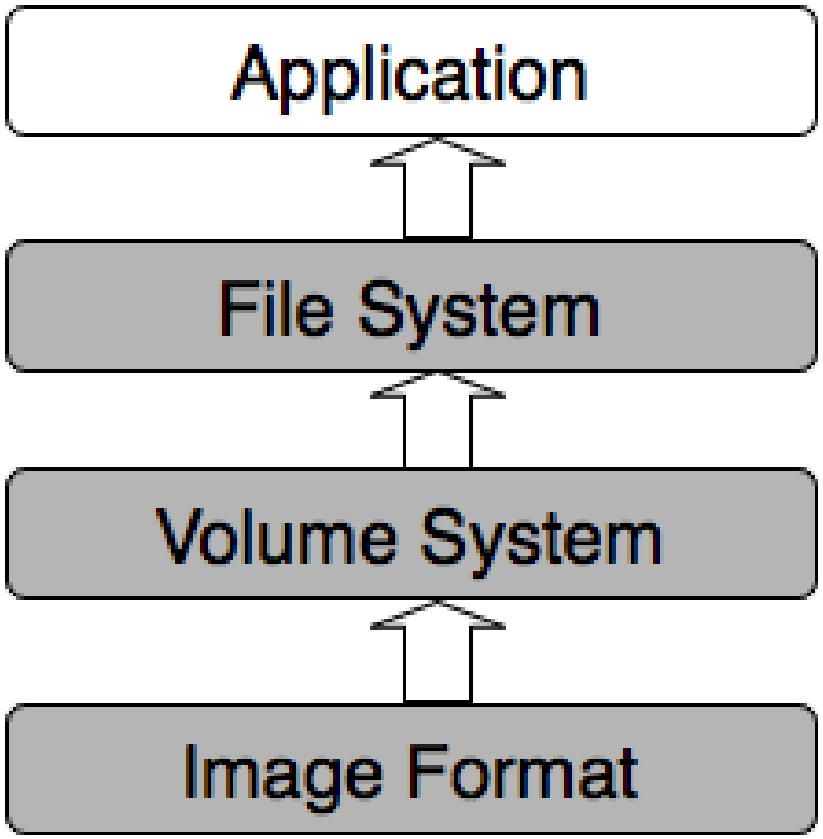
Agenda

- What is TSK?
- What does it do for you?
- How can you use it?
- What is in TSK's future?

BASIS TECHNOLOGY

What Is The Sleuth Kit?

- Open source software that allows you to forensically analyze disk images and local drives.

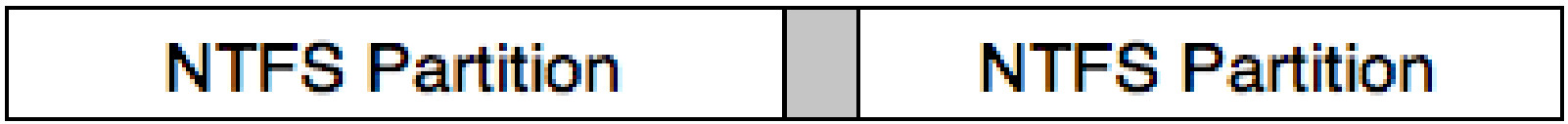


BASIS TECHNOLOGY

Scenario

- You have a disk image and want to look for specific files.

1. TSK will auto-detect the image format
2. TSK will auto-detect the volume system and layout:
   - What sectors are allocated to partitions
   - What sectors are not allocated to any partitions



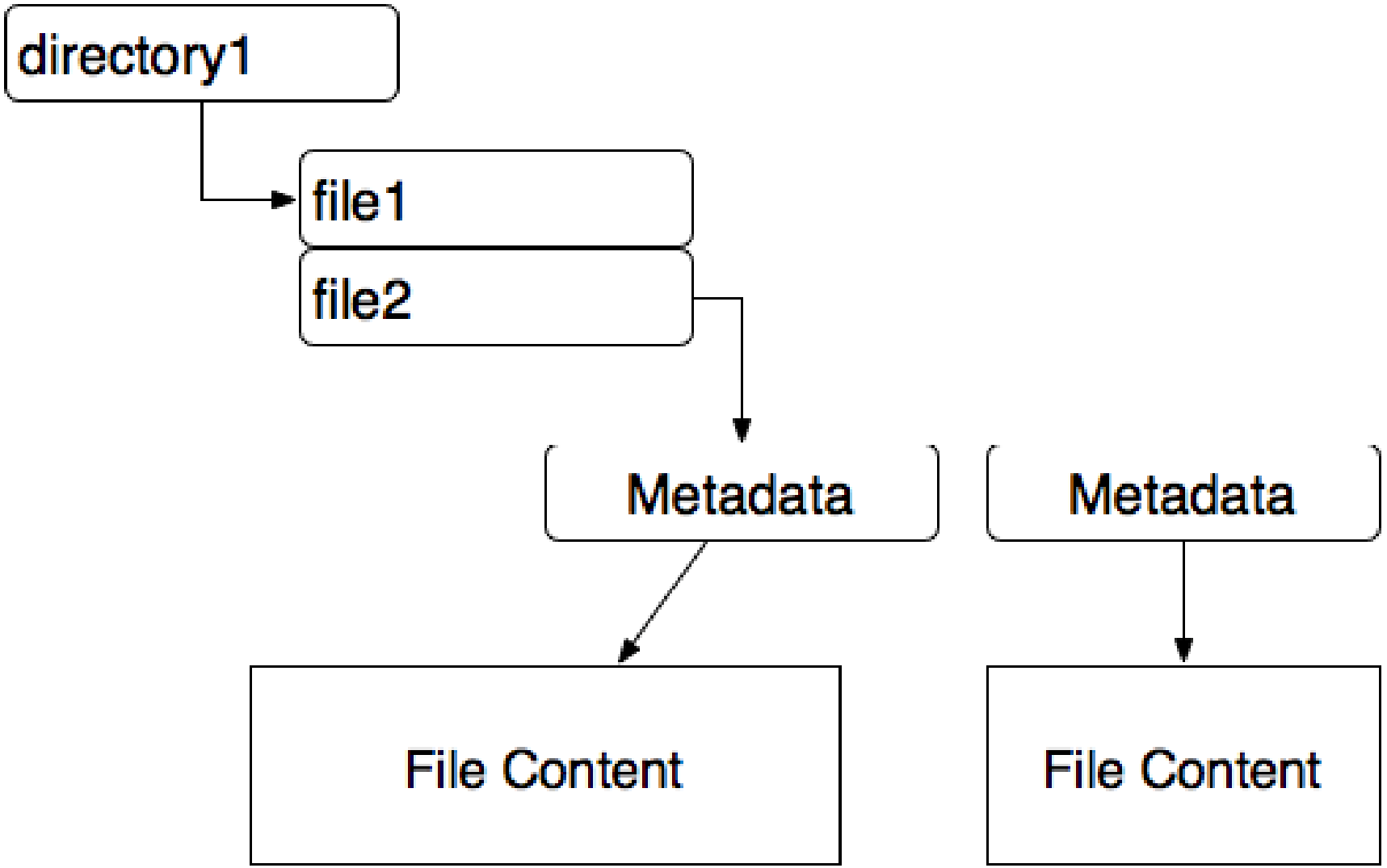
BASIS TECHNOLOGY

©2010, Basis Technology.

Scenario (contd.)

3. TSK will auto-detect the file system type and can search for your file (even if it is deleted)
   - Analyzes the directory hierarchy in file system.
   - Identifies files that have been marked for deletion.
   - Searches for “orphan files” that no longer have a name.

BASIS TECHNOLOGY
©2010, Basis Technology.



©2010, Basis Technology.

Scenario (contd.)

- Allows search to be conducted based on:
  - File name and extension
  - Temporal data (created, modified, accessed, changed, etc.)
  - File size
  - File location
  - Hash of file content
- With third-party support, can search app-level:
  - Signature analysis of file content
  - Keyword search of text in file content
  - Image analysis of file content

BASIS TECHNOLOGY

©2010, Basis Technology.

Call Now!

- How much would you pay for this functionality?
  - $100?
  - $1000?
- This can all be yours for 3 monthly payments of $0.
- But wait, there's more!

©2010, Basis Technology.

There's more!

- Need to quickly lookup hash values in a hash database? TSK can do that.
- Need to filter out the "Known Good" files, flag the "Known Bad" files, and sort the rest based on file type? TSK can do that.
- Need to view a timeline of activity on the device? TSK can do that too.

©2010, Basis Technology.

TSK History

- The Coroner's Toolkit (TCT) was first released in 2000 by Dan Farmer and Wietse Venema.
  - Ran only on Unix systems
  - Analyzed only local file system type (Ext2 and UFS)
  - Did not know about file names (only blocks and inodes).
- TCTUtils was released in 2001 by me as TCT add-on.
  - Adds file name layer so that directory contents can be listed.
  - Allows you to map between blocks, inodes, and file names (i.e. which file is using block 234?)

BASIS TECHNOLOGY

TSK History (2)

- The @stake Sleuth Kit (TASK) was released in 2002 by me.
  - Integrated TCT and TCTUtils into a single project.
  - Added platform independence (can analyze file system types different than local system).
  - Added FAT and NTFS support.
  - Added OS X and Cygwin support.
- TASK was renamed to TSK in 2003.

BASIS TECHNOLOGY

Current Capabilities

- Platforms:
  - Windows
  - Linux
  - OS X
  - Cygwin
  - OpenBSD, FreeBSD, etc.
  - Solaris
- Image Layer:
  - Raw files or local disks
  - Split raw files (i.e. multiple 2GB files)
  - E01 EnCase files (using libewf library)
  - AFF files (using afflib library)

BASIS TECHNOLOGY

Current Capabilities (2)

- Volume System Layer
  - DOS Partitions
  - GPT partitions
  - MAC partitions
  - BSD Disk labels
  - SUN VTOC
- File System Layer
  - NTFS
  - FAT12, FAT16, FAT32
  - HFS+
  - ISO9660
  - Ext2, Ext3
  - UFS1, UFS2, FFS
- Wyatt Banks / Crucial contributed initial ISO9660 and HFS+.
- ATC-NY contributed HFS+ enhancements.

BASIS TECHNOLOGY

Current Capabilities (3)

- Hash Databases
  - NSRL
  - Hashkeeper
  - Md5sum/sha1sum
- Timelines
  - Sorts files based on modified, accessed, changed, and created times.
  - Open input format.
  - Text output
  - Useful for intrusions.
- Sorter:
  - Ignores “known good” files.
  - Flags “known bad” files.
  - Organizes unknown files by file type.
  - Creates thumbnails of unknown images.

BASIS TECHNOLOGY

How To Currently Use TSK

Command Line Tools

- Original method for using TSK
- Currently, over 20 different tools
  - 2 Image Layer
  - 3 Volume System Layer
  - 13 File System Layer
  - 2 Hash and Signature Search
  - 1 Timeline tool
  - 1 Sorting tool

BASIS TECHNOLOGY

Mmls Example

- Lists the partitions in a disk image.
- Example:

```
# mmls tsk1.img
     Slot    Start        End          Length       Description
00:  -----   0000000      0000000      0000001      Primary Table
01:  -----   0000001      0000062      0000062      Unallocated
02:  00:00   0000063      0032129      0032067      NTFS (0x07)
03:  00:01   0032130      0064259      0032130      DOS FAT16
   (0x06)
```

©2010, Basis Technology.

Fls example

- Lists the files in a directory.
- Shows deleted and orphan files

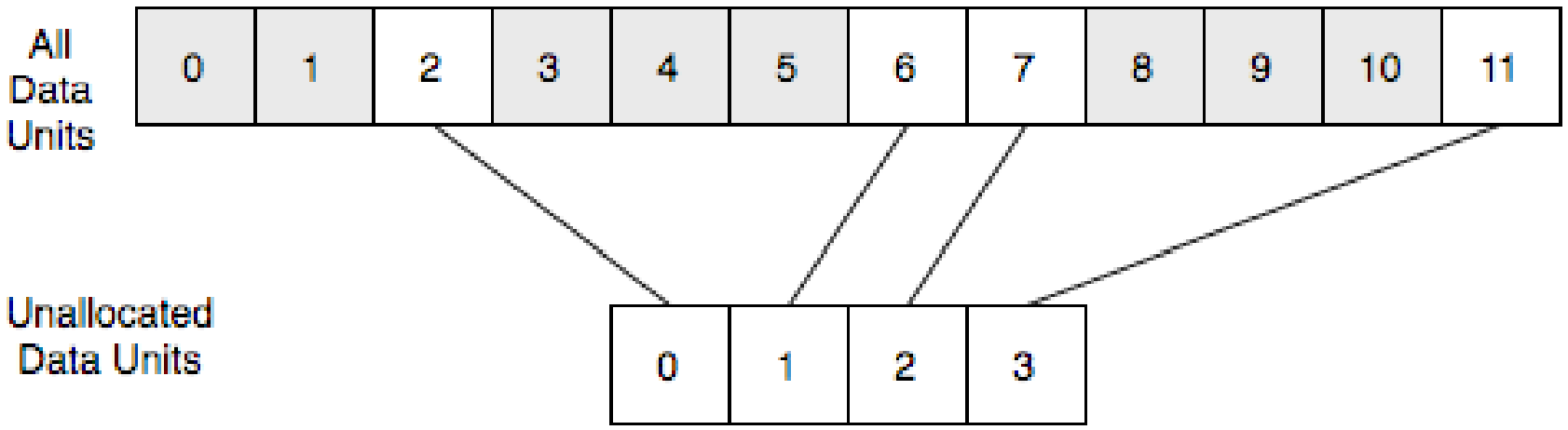
```
# fls -o 63 tsk1.img
r/r 4-128-4:    $AttrDef
[…]
r/r 3-128-3:    $Volume
d/d 29-144-6:   dir1
d/d 31-144-1:   dir2
d/d 34-144-1:   RECYCLER
  v/v 19920-144-1: $OrphanFiles
```


BASIS TECHNOLOGY

©2010, Basis Technology.

blkls Example

- Extracts the unallocated blocks in the file system for additional data recovery.
- Output can be used for carving.



©2010, Basis Technology.

Library

- All of the command line functionality, in a C library.
- More efficient to use when processing a full disk image.
- Reduced overhead:
  - Load general file system data only once
- Full API docs and sample programs exist.

Library Quick Start

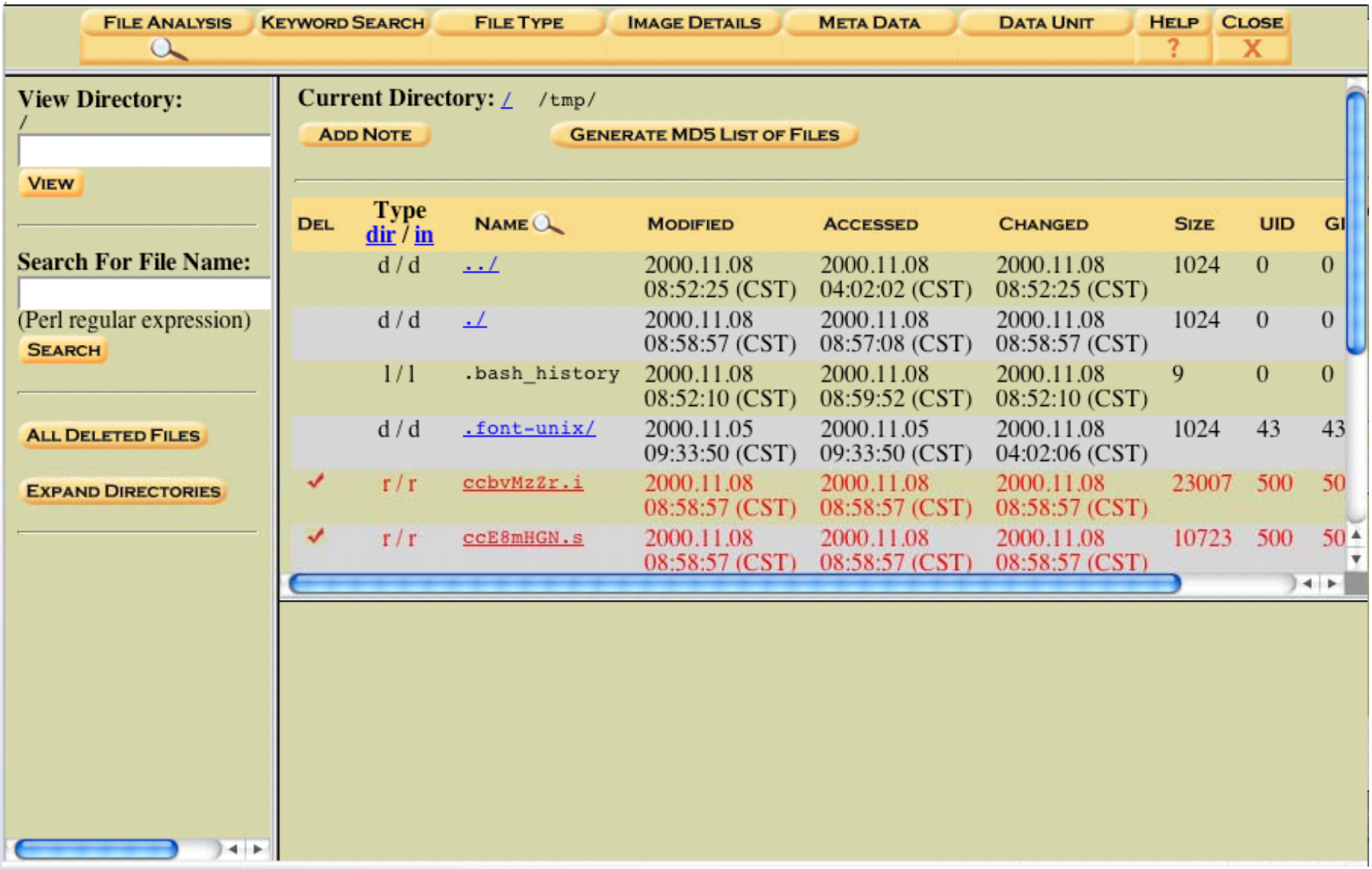
1. Open the disk image.
2. Open the volume system in the disk image.
3. Open the file system in each volume
4. Access data in the file system:
   - List all files in a given directory.
   - Read the contents of any file.
   - Access any block in the file system.

BASIS TECHNOLOGY
©2010, Basis Technology.

Autopsy

- Original graphical interface to TSK
- First released in 2001
- HTML-based interface:
  - Runs TSK command line tools
  - Parses output
  - Displays with HTML tags added in
- Does not use the library interface.

BASIS TECHNOLOGY



©2010, Basis Technology.

Tools that you'll hear about later today:

- Mandiant Intelligent Response
- Mac Marshall
- PTK

BASIS TECHNOLOGY

Bootable CDs

- From wiki.sleuthkit.org:
- BackTrack2
- CAINE (Computer Aided INvestigative Environment)- GUI Forensics Interface
- DEFT (Digital Evidence & Forensic Toolkit) - Xubuntu based
- CCU Gnu/Linux Forensic Boot CD (knoppix)
- Forensic and Incident Response Environment (FIRE)
- Helix (knoppix)
- Knoppix STD
- Local Area Security Linux
- Penguin Sleuth Kit (knoppix)
- Plan-B
- Snarl (FreeBSD)
- HeX (Freesbie2)
- Stagos FSE (Ubuntu based)
- IRItaly Live CD Project (Gentoo based)
- ForLEx Live CD - Forensic Linux Examination (Knoppix based)

©2010, Basis Technology.

fiwalk

- Analysis program that extracts metadata about files in an image:
  - Names
  - Hashes
  - Block locations
  - …
- Saves output in XML
- Written by Simson Garfinkel

BASIS TECHNOLOGY

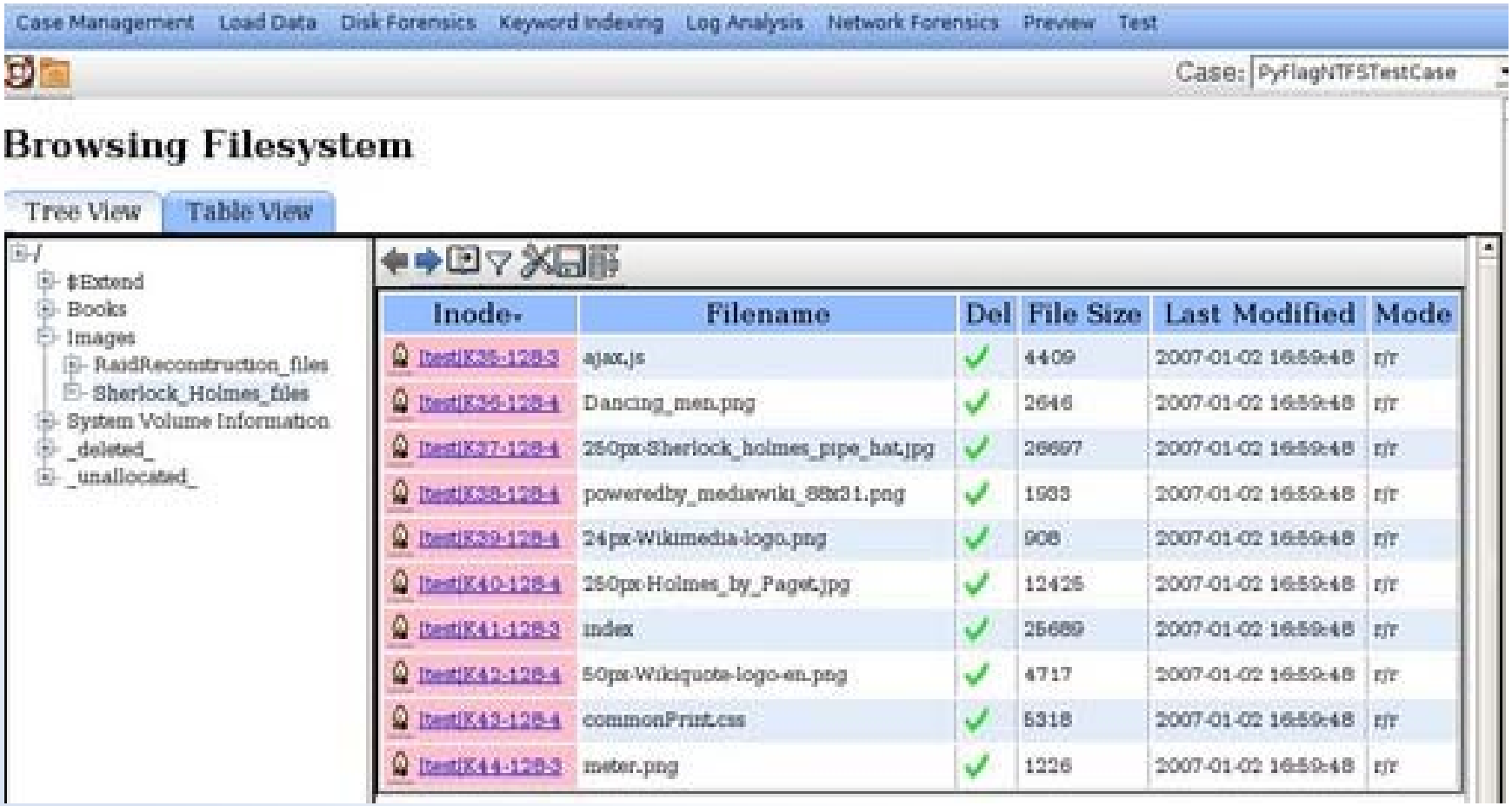
©2010, Basis Technology.

PyFlag

- Graphical tool that integrates:
  - Network Forensics
  - Log Analysis
  - Disk Forensics (Sleuth Kit)
  - Memory Forensics (Volatility)
- Developed by Michael Cohen and David Collett
- Database oriented approach

BASIS TECHNOLOGY
©2010, Basis Technology.

PyFlag Screen Shot



©2010, Basis Technology.

Nanni Bassetti

- Raw2FS: Resolves carved data to file names
- MultiFS: Detects file systems
- SFDumper: Selective file extractor
- FUNDL: Selected deleted file extractor

©2010, Basis Technology.

Odyssey Digital Forensic Search

- Basis effort to integrate language tools with keyword searching hard drives.
  - Sleuth Kit to extract files from image
  - Basis Rosette tools to tokenize and normalize text.
  - dtSearch to create an index of keywords.
  - Basis Rosette tools to triage documents by identifying names and translating them.
  - Simple GUI

BASIS TECHNOLOGY

Normalizing Keywords

á = a + ´

U+00E1 U+0061 + U+00B4

- لُغَوِيَّة
- لُغوِيَّة
- لغويّة

الصبر

الصـــبـــر

الـصـــبـــر

BASIS TECHNOLOGY


Basis Technology - Odyssey Digital Forensics™ Keyword Search
Case Edit Settings Help
Keyword Search
Language Statistics
Case: case1
Odyssey
DIGITAL FORENSICS
1425
Language
Auto Detect
Detected Language: Unknown
Search
Reset
Keyword List
Files Found: 8
/norm2/thread2361.html
/Numbers/num2.htm
/Numbers/num1.htm
-doc/norm2/أسعار الأسهم.doc
-doc/numbers/الصفحة الرئيسية.doc
-doc/numbers/الحكومةالسعودية.doc
-doc/numbers/التاريخ البيان التسلسل.doc
-doc/numbers/wikipedia.doc
File Contents
Name Translation
File Metadata
ان هذا (القانون) الذي وضعه مجلس غير منتخب وفي ظل الاحتلال وبتأثير مباشر منه يفيد الجمعية الوطنية المقرر انتخابها في بداية العام الميلادي القادم لغرض وضع الدستور الدائم للعراق .
وهذا أمر مخالف للقوانين ويرفضه معظم ابناء الشعب العراقي . ولذلك فان أي محاولة لاضفاء الشرعية على هذا (القانون) من خلال ذكره في القرار الدولي يعد عملاً مضاداً لارادة الشعب العراقي وينذر بنتائج خطيرة .
يرجى ابلاغ موقف المرجعية الدينية بهذا الشأن الى السادة اعضاء مجلس الأمن المحترمين، وشكراً.
١٤٢٥/٤/١٧
٢٠٠٤/٦/٦
بسم الله الرحمن الرحيم
أسئلة مجلة "دير شبيجل " الألمانية الموجهة إلى سماحة السيد السيستاني (دام ظله)
1- هل تمت عملية إسقاط نظام صدام حسين بالشكل المنشود ؟
2- إنكم يا سماحة السيد تحثون إجراء إنتخابات عامة قبل نهاية شهر حزيران في حين يعمل المحتلون على اطالة فترة بقائهم ويدعون الى تشكيل مجلس انتقالي .
Files
Hits
Report
/img0/vol0/Arabic/ArabicPages-doc/numbers/الصفحة الرئيسية.doc
Ready to search

1990 : بداية رحلته إلى Afghanistan .

1991 : شارك في القتال ضد الروس في منطقة Khust. وأتخذ اسم Abu-Mus'ab al-Zarqawi بعد انضمامه إلى مجموعة التوحيد والهجرة السلفية التي يترأسها Abu-Muhammad al-Maqdisi .

1994- حكم عليه بالسجن في Jordan لمدة 15 عاما لكنه خرج بعفو عام 1999 .

1999 : نسب إليه التخطيط لشن هجوم "إرهابي" في احتفال Jordan بالألفية، حيث استهدف الهجوم فندق RAdyswn ساس في Oman ومواقع أميركية وإسرائيلية ومسيحية أخرى، وأحبطت المحاولة قبل تنفيذها، لكنه هرب قبل القبض عليه .

2000 : انتقل al-Zarqawi إلى Afghanistan حيث أشرف على معسكر لتدريب مقاتلي al-Qa'idah، كما تخصص في الأسلحة الكيماوية والبيولوجية .

2001 : حكم عليه غيابيا بـ15 سنة لتورطه في ما سمي "العمليات الإرهابية" في Jordan .

أكتوبر/ تشرين الأول 2001 : فر al-Zarqawi إلى Iran بعد أن فقدت Taliban سيطرتها على Afghanistan، ومن هناك جند فلسطينيين اثنين وأردنيا دخلوا Turkey وكان من المفترض أن يذهبوا إلى Israel للقيام بهجمات بالقنابل هناك .

15 فبراير/ شباط 2002 : إلغاء القبض على الثلاثة الذين أرسلهم al-Zarqawi في Turkey .

مايو/ أيار 2002 : سافر al-Zarqawi إلى Iraq حيث فقد إحدى رجليه واستبدل بها أخرى صناعية .

مايو/ أيار- يوليو/ تموز 2002 : تعافى من إصابته في Baghdad والتقى بعض المقاتلين هناك حيث أقام قاعدة عمليات .

نهاية صيف 2002 : سافر al-Zarqawi إلى Lebanon لمقابلة قادة من Hizballah ومجموعة مسلحة أخرى .

بداية 2003 : عاد al-Zarqawi إلى معسكر أنصار الإسلام في Iraq. وقام شخص آخر تدرب في هذا المعسكر بالتخطيط لهجمات كيميائية باستخدام سموم مختلفة في Britain France Georgia Chechnya .

يناير/ كانون الثاني 2003 : القبض على بعض "الإرهابيين" في Britain بتهمة التخطيط لوضع ريسين في أغذية الجيش، ومرة أخرى يربط بين "الإرهابيين" Wa'alzzarqawi .

5 فبراير/ شباط 2003 : وزير الخارجية الأمريكي Colin Powell تحدث أمام Majlis al-Amn مشيرا إلى معلومات لديه عن علاقات al-Zarqawi بتنظيم al-Qa'idah في Iraq .

Future of TSK

Version 3.2

- Automation, Automation, Automation
- Easier to create programs that need access to all files in an image or local disk.
- New C++ class that automates:
  - Identification of partitions in disk.
  - Identification and extraction of files in file system.
- Instead of duplicating the sample program, just create a super class and implement a couple of methods.

BASIS TECHNOLOGY

Version 3.2 Tools

- Dump all file metadata data to a SQLite database:
  - Can be processed by non-C tools and interfaces.
  - Allows for correlation.
  - Schema is not yet finalized – contact me if you have needs.
- Extract files to a local directory hierarchy:
  - Frequently requested data recovery feature.
- Compare raw data with local directory hierarchy:
  - Finds rootkits that are hiding directories
  - Useful for testing

Post Version 3.2

- More language-specific bindings:
  - Python
  - Java
- File systems:
  - ExFAT
  - YAFFS
  - Ext4
  - ...
- More higher-level tools:
  - Sorter in C++

BASIS TECHNOLOGY

Analysis Framework

- At application layer, there are many independent tools with different APIs.
  - Registry
  - Internet history viewers
  - Text extraction
  - …
- An open framework would make it easier to use open source software in fully automated system.
  - Different modules would be called for different file types.
  - Different reporting modules could create output in different formats.

BASIS TECHNOLOGY

©2010, Basis Technology.

New GUI

- A new Autopsy needs to be created:
  - Simple to install
  - Simple to use
  - Uses TSK library and application-level framework
  - Integrates open source search tools (Lucene, etc.)

©2010, Basis Technology.

Merchandise

©2010, Basis Technology.

Contact

Brian Carrier

Brianc[at]basistech.com
carrier[at]sleuthkit.org

http://www.sleuthkit.org/

BASIS TECHNOLOGY

©2010, Basis Technology.