SANS Digital Forensics and Incident Response Blog

11 May **2009**

A Step-by-Step introduction to using the AUTOPSY Forensic Browser (/blog/2009/05/11/a-step-by-step-introduction-to-using-the-autopsy-forensic-browser#)

4 comments (/blog/2009/05/11/a-step-by-step-introduction-to-using-the-autopsy-forensic-browser#comments) Posted by craigswright (/blog/author/craigswright)
Filed under Computer Forensics (/blog/category/computer-forensics)

by Craig Wright (https://blogs.sans.org/computer-forensics/author/craigswright/)

This is a brief tutorial on how to use the Autopsy Forensic Browser as a front end for the Sleuthkit. This tool is an essential for Linux forensics investigations and can be used to analyze Windows images.

We will start with the presumption that you have the Forensic Toolkit Installed (whether through the use of a Live CD such as Helix or if it is installed on a Forensic Workstation). Autopsy is built into the SANS Investigative Forensic Toolkit Workstation (SIFT Workstation (http://forensics.sans.org/community/downloads/)) that you can download (http://forensics.sans.org/community/downloads/)from forensics.sans.org (http://forensics.sans.org). You can start Autopsy by clicking on the magnifying glass in the upper right corner.

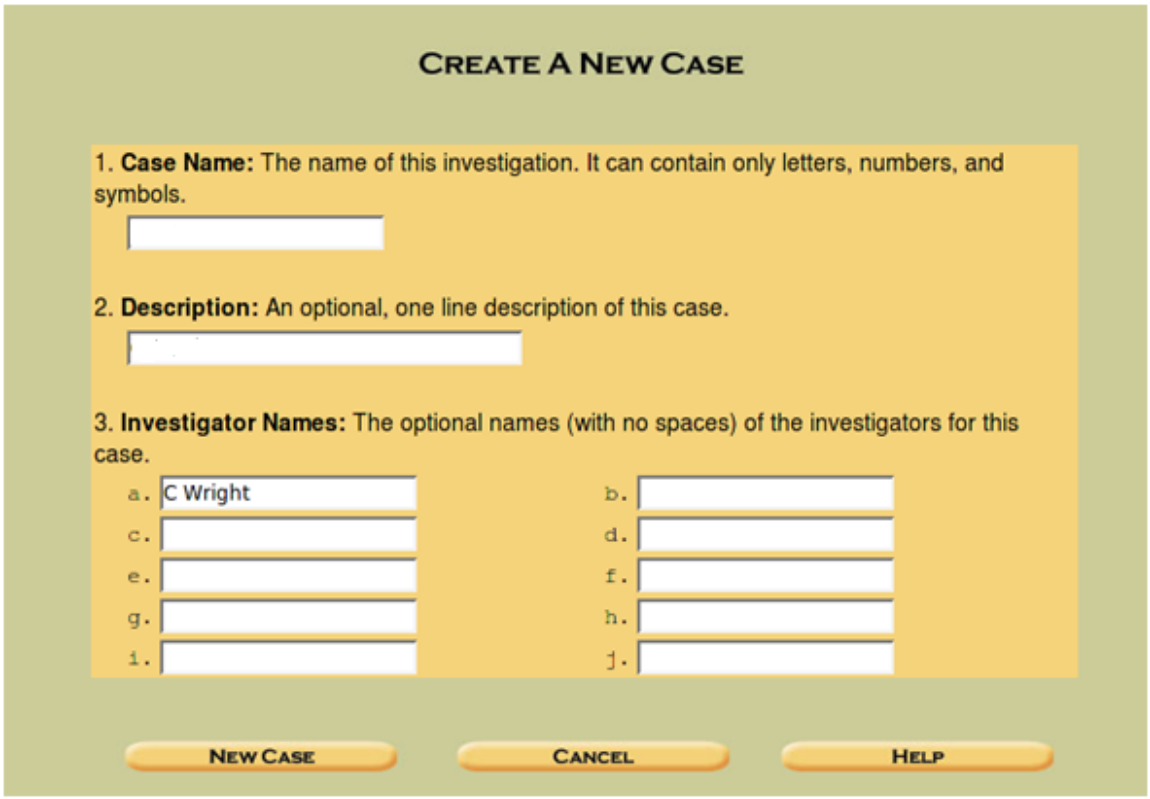
Step 1 — Start the Autopsy Forensic Browser

Autopsy is a web based front end to the FSK (Forensic Toolkit). By default, you will connect to the Autopsy service using the URL; http://localhost:9999 (http://localhost:9999). The default start page is displayed in Step 2.

Step 2 — Start a New Case

Click **New Case.** This will add a new case folder to the system and allow you to begin adding evidence. To begin, click **New Case.**

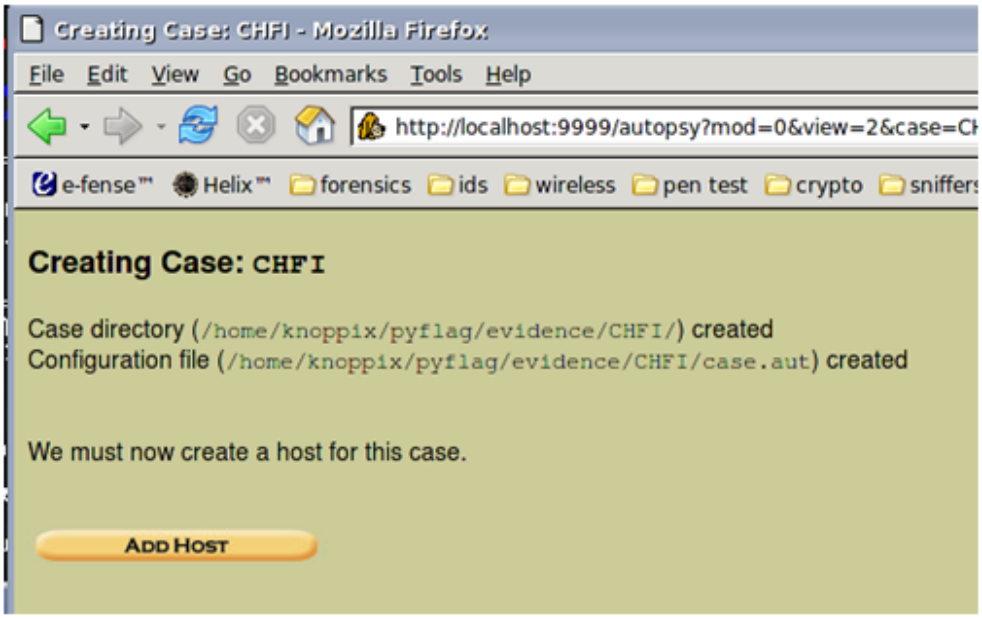
Step 3 — Enter the Case Details



Begin by entering the details about the case. This will include the name of the Case itself and a description of the case. For this, you should have a means of identifying cases. An example could be something along the lines of "<Company>.<Instance>" if you do external consulting as I do or it could be related to specific designations within a company.

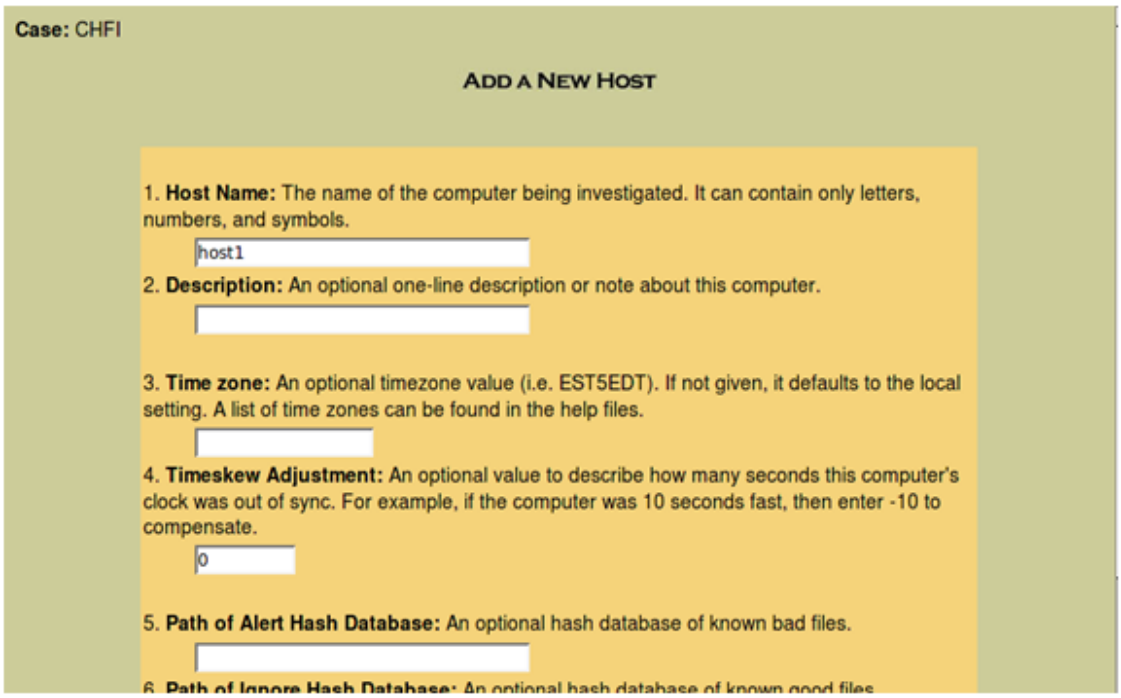
You will see the message (displayed in Step 4) when the case file is created.

Step 4 — Note where the Evidence Directory is located



In the example above, we see an example case I created for a CHFI course I created. This displays where the evidence is located on the system.

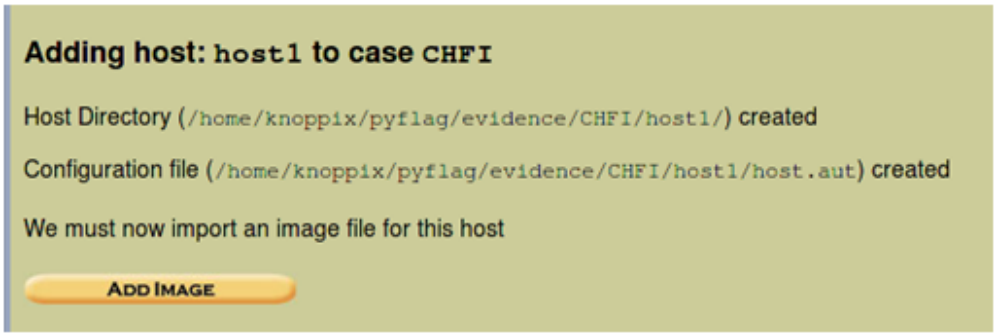
Step 5 — Add a Host to the Case



Click **"Add Host"** and you will be presented with a screen (above) that allows you to add the host and a description. As it states, the Timezone and skew can be configured. Also, you can add and use a list of known good or known bad hashes. This can be as complex as the NSRL lists or as simple as a hashed list of your own organizations "known good" files. Lists of known rootkits and other Malware can be added as a known bad list.

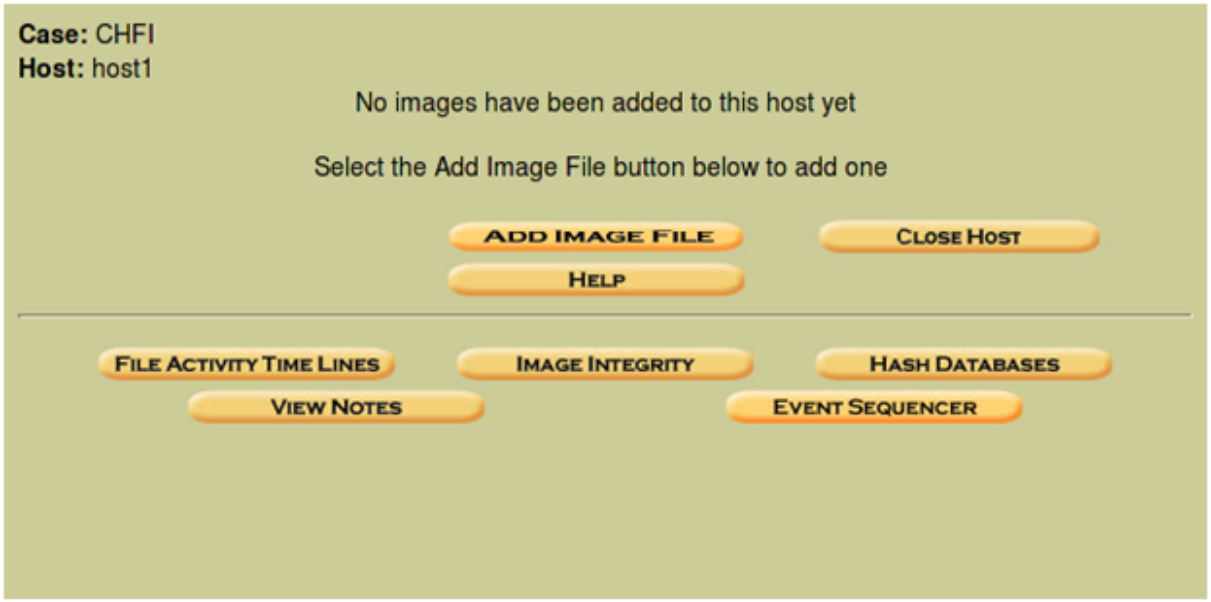
Where a time skew is known, you can also add this in advance.

Step 6 — Note whete the host is located



Next, add the disk image by pressing the **Add Image** button (Example /home/CHFI.img. Autopsy allows you to use an image that you have already captured. This can be an image of the disk using the dd command for instance). You can also use Autopsy to capture an image, but this is not covered in this post.

Step 7 — Add an Image to Analyze

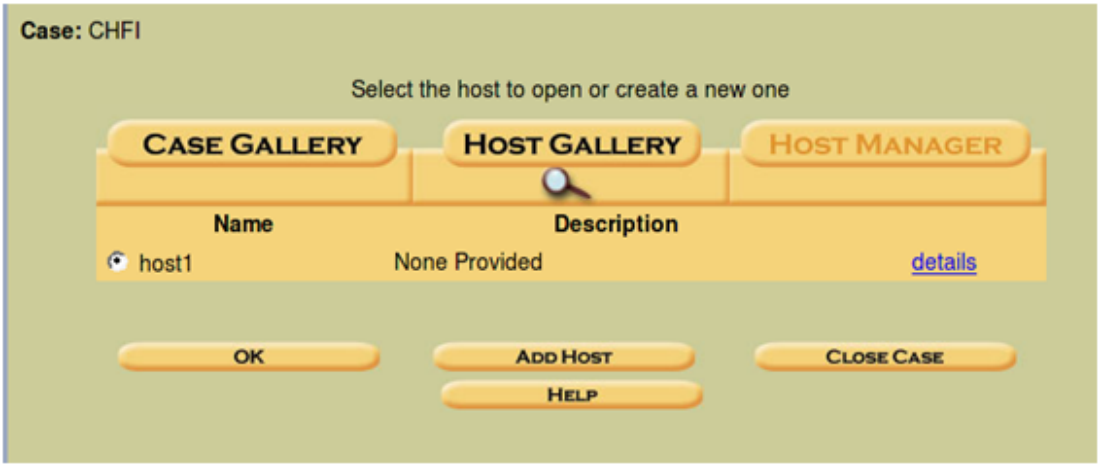


The "**Add Image**" screen allows us to import the image that we are going to analyze in Autospy.

Step 8 — Select the location of the Image to Analyze

This will allow us to import an image into our evidence locker. Rather than working on the original image, you can select the move option to copy the image to the analysis host and have a separate copy of the image for use in Autopsy.

Step 9 — the Case Gallery



As you add hosts to the case, these will be displayed in the "Case Gallery". When you now go back to the Case Gallery and view your options, you will be presented with the options displayed in Step 10.

Step 10 — Now try the other options

You should work with various features of Autopsy browser and experiment with these in order to become familiar with the options and functionality. Try the other options and analyze an image to gain experience with the tool.

The Evidence Analysis Techniques in Autopsy

The primary modes and functions of the Autopsy Forensic Browser are to act as a graphical front end to the Sleuth Kit and other related tools in order to provide the capabilities of analysis, search and case management in a simple but comprehensive package. This collection of tools creates a simple, yet powerful forensic analysis platform.

Analysis Modes in Autopsy

A **dead analysis** occurs when a dedicated analysis system is used to examine the data from a suspect system. When this occurs, Autopsy and The Sleuth Kit are run in a trusted environment, typically in a lab. Autopsy and TSK provides support for raw, Expert Witness, and AFF file formats.

A **live analysis** occurs when the suspect system is being analyzed while it is running. In this case, Autopsy and The Sleuth Kit are run from a CD in an untrusted environment. This is frequently used during incident response while the incident is being confirmed. Following confirmation, the system is acquired and a dead analysis performed.

Evidence Search Techniques

The Autopsy Browser provides the following evidence search functionality:

- File Listing: Analyze the files and directories, including the names of deleted files and files with Unicode-based names.
- File Content: The contents of files can be viewed in raw, hex, or the ASCII strings can be extracted. When data is interpreted, Autopsy sanitizes it to prevent damage to the local analysis system. Autopsy does not use any client-side scripting languages.
- Hash Databases: Lookup unknown files in a hash database to quickly identify it as good or bad. Autopsy uses the NIST National Software Reference Library (NSRL) and user created databases of known good and known bad files.
- File Type Sorting: Sort the files based on their internal signatures to identify files of a known type. Autopsy can also extract only graphic images (including thumbnails). The extension of the

file will also be compared to the file type to identify files that may have had their extension changed to hide them.

- Timeline of File Activity: A timeline of file activity can help identify areas of a file system that may contain evidence. Autopsy can create timelines that contain entries for the Modified, Access, and Change (MAC) times of both allocated and unallocated files.
- Keyword Search: Keyword searches of the file system image can be performed using ASCII strings and grep regular expressions. Searches can be performed on either the full file system image or just the unallocated space. An index file can be created for faster searches. Strings that are frequently searched for can be easily configured into Autopsy for automated searching.
- Meta Data Analysis: Meta Data structures contain the details about files and directories. Autopsy allows you to view the details of any meta data structure in the file system. This is useful for recovering deleted content. Autopsy will search the directories to identify the full path of the file that has allocated the structure.
- Data Unit Analysis: Data Units are where the file content is stored. Autopsy allows you to view the contents of any data unit in a variety of formats including ASCII, hexdump, and strings. The file type is also given and Autopsy will search the meta data structures to identify which has allocated the data unit.
- Image Details: File system details can be viewed, including on-disk layout and times of activity. This mode provides information that is useful during data recovery.

Case Management

Autopsy provides a number of functions that aid in case management. In particular, investigations started within autopsy are organized by cases, which can contain one or more hosts. Each host is configured to have its own time zone setting and clock skew so that the times shown are the same as the original user would have seen. Each host can contain one or more file system images to analyze. The following functions within Autopsy are specifically designed aid in case management:

- Event Sequencer: Time-based events can be added from file activity or IDS and firewall logs. Autopsy sorts the events so that the sequence of incident associated with an event can be easily determined.
- Notes: Notes can be saved on a per-host and per-investigator basis. These allow the investigator to make quick notes about files and structures. The original location can be easily recalled with the click of a button when the notes are later reviewed. All notes are stored in an ASCII file.
- Image Integrity: Being that one of the most crucial aspects of a forensics investigation involves ensuring that data is not modified during analysis; Autopsy will generate an MD5 value for all files that are imported or created by default. The integrity of any file that Autopsy uses can be validated at any time.
- Reports: Autopsy can create ASCII reports for files and other file system structures. This enables investigator to promptly make consistent data sheets during the course of the investigation.
- Logging: Audit logs are created on a case, host, and investigator level so that all actions can be easily retrieved. The entire Sleuth Kit commands are logged exactly as they are executed on the system.

Autopsy is available from http://www.sleuthkit.org/autopsy (http://www.sleuthkit.org/autopsy).

Craig Wright is a Director with Information Defense (http://www.information-defense.com/) in Australia. He holds both the GSE-Malware (http://www.giac.org/certifications/gse-malware.php) and GSE-Compliance (http://www.giac.org/certifications/gse-compliance.php) certifications from GIAC. He is a perpetual student with numerous post graduate degrees including an LLM specializing in international commercial law and ecommerce law

as well as working on his 4th IT focused Masters degree (Masters in System Development) from Charles Stuart University (http://www.csu.edu.au/) where he is helping to launch a Masters degree in digital forensics. He starts his second doctorate, a PhD on the quantification of information system risk at CSU in April this year.

Permalink (/blog/2009/05/11/a-step-by-step-introduction-to-using-the-autopsy-forensic-browser) | Comments RSS Feed (/blog/2009/05/11/a-step-by-step-introduction-to-using-the-autopsy-forensic-browser/feed) - Post a comment | Trackback URL (/blog/2009/05/11/a-step-by-step-introduction-to-using-the-autopsy-forensic-browser)

4 Comments

Posted April 23, 2013 at 10:02 AM | Permalink (blog/2009/05/11/a-step-by-step-introduction-to-using-the-autopsy-forensic-browser#comment-15268) | Reply (?reply-to-comment=15268#respond)

Navdeep sharma

is it accept only .img files?
i m trying to add .iso file and .jpg it is not accepting please help me
thanks in advance

Posted May 2, 2013 at 10:30 AM | Permalink (blog/2009/05/11/a-step-by-step-introduction-to-using-the-autopsy-forensic-browser#comment-15348) | Reply (?reply-to-comment=15348#respond)

Pankaj

is it accept only .img files?
i m trying to add .iso file and .jpg it is not accepting please help me
thanks in advance
Reply Admin

Posted September 7, 2013 at 2:38 PM | Permalink (blog/2009/05/11/a-step-by-step-introduction-to-using-the-autopsy-forensic-browser#comment-16733) | Reply (?reply-to-comment=16733#respond)

Arist0v

an image file it's would mean an hard drive image file not a cd or dvd image(iso) or a picture image(jpg bmp etc") if you make some search on google you will easily find how to make image from hdd. CloneZilla can help you making image file from hdd or the dd commande can also help you.
Arist0v

Posted April 25, 2014 at 11:05 AM | Permalink (blog/2009/05/11/a-step-by-step-introduction-to-using-the-autopsy-forensic-browser#comment-17423) | Reply (?reply-to-comment=17423#respond)

Nicola

I have a raw image file (.dd) which I created from CloneZilla. However Autopsy won't allow me to add it as a data file "" it is just stuck saying it is currently adding "NO_INFO'.
Has anybody ever had that before?

Enter country...

Subscribe

Share

(https://www.addtoany.com/share#url=https%3A%2F%2Fdigital-forensics.sans.org%2Fblog%2F2009%2F05%2F11%2Fa-step-by-step-introduction-to-using-the-autopsy-forensic-browser&title=SANS%20Digital%20Forensics%20and%20Incident%20Response%20Blog%20%7C%20A%20Step-by-Step%20introduction%20to%20using%20the%20AUTOPSY%20Forensic%20Browser%20%7C%20SANS%20Institute) (/#facebook) (/#twitter) (/#google_plus) (/#linkedin) (/#email)

Categories

- Advanced Persistent Threat (/blog/category/advanced-persistent-threat) (50)
- apt (/blog/category/apt-advanced-persistent-threat) (26)
- artifact analysis (/blog/category/artifact-analysis) (82)
- Book Reviews (/blog/category/book-reviews) (5)
- Browser Forensics (/blog/category/browser-forensics) (34)
- Call for speakers (/blog/category/call-for-speakers) (4)
- Career (/blog/category/career) (1)
- Case Leads (/blog/category/case-leads) (123)
- Certification and License (/blog/category/certification-and-license) (9)
- Challenge (/blog/category/challenge) (9)
- Cloud Forensics (/blog/category/cloud-forensics-computer-forensics) (2)
- Community SANS Events (/blog/category/community-sans-events) (4)
- Computer Forensic Hero (/blog/category/computer-forensic-hero) (2)
- Computer Forensics (/blog/category/computer-forensics) (673)
- Computer Forensics and IR Summit (/blog/category/computer-forensics-and-ir-summit) (50)
- Cyber Kill Chain (/blog/category/cyber-kill-chain) (7)
- Cyber Threat Intelligence (/blog/category/cyber-threat-intelligence-2) (24)
- DFIR Scholarship (/blog/category/dfir-scholarship) (2)
- DFIR Summit (/blog/category/dfir-summit) (18)
- DFIR Summit 2019 (/blog/category/dfir-summit-2019) (2)
- DFIR Summit Vans Contest (/blog/category/dfir-summit-vans-contest) (1)
- DFIRCON (/blog/category/dfircon) (2)
- Digital Forensic Law (/blog/category/digital-forensic-law) (50)
- Drive Encryption (/blog/category/drive-encryption) (20)
- eDiscovery (/blog/category/ediscovery) (51)
- Email Investigations (/blog/category/email-investigations) (19)
- Ethics (/blog/category/ethics) (9)
- Evidence Acquisition (/blog/category/evidence-acquisition) (124)
- Evidence Analysis (/blog/category/evidence-analysis) (202)
- FOR408 course renumbering (/blog/category/for408-course-renumbering) (1)
- FOR498: Battlefield Forensics & Data Acquisition (/blog/category/for498-battlefield-forensics-data-acquisition) (2)
- FOR500: Windows Forensics Analysis (/blog/category/for500-windows-forensics-analysis) (3)

- FOR585 Smartphone Forensics course Q&A (/blog/category/for585-smartphone-forensics-course-qa) (1)
- Forensic4Cast Awards (/blog/category/forensic4cast-awards) (2)
- Getting Started (/blog/category/getting-started) (25)
- Ghidra (/blog/category/ghidra) (5)
- HeartBleed (/blog/category/heartbleed) (1)
- Incident Response (/blog/category/incident-response) (213)
- Incident Response Survey (/blog/category/incident-response-survey) (1)
- iOS (/blog/category/ios) (5)
- Lethal Forensicator Coins (/blog/category/lethal-forensicator-coins) (2)
- Linux IR (/blog/category/linux-ir) (29)
- Malicious Scripts (/blog/category/malicious-scripts) (3)
- Malware Analysis (/blog/category/malware-analysis) (121)
- Meltdown & Spectre (/blog/category/meltdown-spectre) (1)
- Memory Analysis (/blog/category/memory-analysis) (68)
- Mobile Device Forensics (/blog/category/mobile-device-forensics) (64)
- Network Forensics (/blog/category/network-forensics) (59)
- Network Forensics (/blog/category/network-forensics-computer-forensics) (10)
- Registry Analysis (/blog/category/registry-analysis) (30)
- REMnux (/blog/category/remnux) (6)
- Reporting (/blog/category/reporting-computer-forensics) (23)
- Reverse Engineering (/blog/category/reverse-engineering) (56)
- SANS Institute (/blog/category/sans-institute) (54)
- SANS Survey (/blog/category/sans-survey) (1)
- SIFT Workstation (/blog/category/sift-workstation) (18)
- smartphone (/blog/category/smartphone) (7)
- SOF_ELK (/blog/category/sof_elk) (1)
- Specials (/blog/category/specials) (23)
- Threat Hunting (/blog/category/threat-hunting) (23)
- Threat Hunting & Incident Response Summit (/blog/category/threat-hunting-incident-response-summit) (12)
- Threat Hunting and Digital Forensics (/blog/category/threat-hunting-and-digital-forensics) (1)
- Timeline Analysis (/blog/category/timeline-analysis-computer-forensics) (24)
- Training (/blog/category/training) (38)
- USB Device Analysis (/blog/category/usb-device-analysis) (15)
- Volatility (/blog/category/volatility) (3)
- WannaCry Ransomware (/blog/category/wannacry-ransomware) (1)
- Windows IR (/blog/category/windows-ir) (88)
- Windows Memory Forensics (/blog/category/windows-memory-forensics) (13)
- Write Blockers (/blog/category/write-blockers) (13)

Recent Posts

- The State of Malware Analysis: Advice from the Trenches (/blog/2019/09/26/state-of-malware-analysis)
- Mass Triage Part 5: Processing Returned Files - Amcache (/blog/2019/09/25/mass-triage-part-5-processing-returned-files-amcache)
- Mass Triage Part 4: Processing Returned Files - AppCache/Shimcache (/blog/2019/09/25/mass-triage-part-4-processing-returned-files-appcacheshimcache)
- Parsing Sysmon Events for IR Indicators (/blog/2019/09/25/parsing-sysmon-events-for-ir-indicators)
- Strengthen Your Investigatory Powers by Taking the New FOR498: Battlefield Forensics & Data Acquisition Course from SANS (/blog/2019/09/16/strengthen-your-investigatory-powers-for498)

Archives

Select Month

Links

- Log in (https://blogs.sans.org/computer-forensics/login.php)
- Entries RSS (/blog/feed/)
- Comments RSS (/blog/feed/comments/)

Latest Blog Posts

The State of Malware Analysis: Advice from the Trenches (/blog/2019/09/26/state-of-malware-analysis)
September 26, 2019 - 2:02 PM

Mass Triage Part 5: Processing Returned Files – Amcache (/blog/2019/09/25/mass-triage-part-5-processing-returned-files-amcache)
September 25, 2019 - 3:28 PM

Mass Triage Part 4: Processing Returned Files – AppCache/Shimcache (/blog/2019/09/25/mass-triage-part-4-processing-returned-files-appcacheshimcache)
September 25, 2019 - 3:28 PM

Latest Tweets @sansforensics

Just a few more days to save $200 when you register for #DFI [...]
(https://twitter.com/sansforensics/statuses/1177986350240485376)
September 28, 2019 - 4:40 PM

This poster covers the essentials you need to know while hig [...]
(https://twitter.com/sansforensics/statuses/1177980063373053952)
September 28, 2019 - 4:15 PM

KAPE is a true game-changer, no other tool is even close. L [...]
(https://twitter.com/sansforensics/statuses/1177952373257506817)
September 28, 2019 - 2:25 PM

Latest Papers

ATT&CKing Threat Management: A Structured Methodology for Cyber Threat Analysis (/community/papers/gcfa/att-cking-threat-management-structured-methodology-cyber-threat-analysis_15277)
By Andy Piazza

Leveraging the PE Rich Header for Static M alware D etection and Linking (/community/papers/grem/leveraging-pe-rich-header-static-alware-etection-linking_6321)
By Maksim Dubyk

Analysis of a Multi-Architecture SSH Linux Backdoor (/community/papers/grem/analysis-multi-architecture-ssh-linux-backdoor_3623)
By Angel Alonso-Parrizas

"This is awesome! We're seeing details that most people don't even know exist."
- John Wright, Info Tech, Inc.

"This course is filling in the blanks in my knowledge of how some things work. It is nice to know what the tools are doing."
- Douglas Couch, Purdue University

"Good, detailed information. This class has exceeded my expectations, as usual."
- Fahey Owens, Discover Financial Services
