TRACKS INSPECTOR
BY FOX IT

Digital Forensics for Non-Technical Investigators

SOLVE CRIMINAL CASES FASTER BY ENABLING DETECTIVES TO ANALYZE DIGITAL EVIDENCE ON THEIR OWN FROM ANY LOCATION

White Paper
March 2012

Executive Summary

PUTTING DIGITAL INVESTIGATION IN THE HANDS OF DETECTIVES

Detectives who are intrinsically involved in collecting and assessing evidence must depend on specialists, unfamiliar with their cases, to process digital information. Tracks Inspector offers a solution that puts most examination of digital evidence into the hands of detectives.

Law enforcement today relies on digital forensics in a greater variety of criminal investigations. With the pervasiveness of computers and mobile devices in society, the occurrences and volume of digital information in cases are exploding.

Detectives who are intrinsically involved in collecting and assessing evidence must depend on specialists, unfamiliar with their cases, to process digital information. This impedes and even prevents prosecuting cases since there are too few digital forensics specialists and labs to support caseloads.

FOX-IT, winner of the DFRWS 2011 Forensics Challenge, [1] now offers a solution that puts most examination of digital evidence into the hands of detectives. The solution, Tracks Inspector, enables detectives without a technical background to easily search, tag, analyze, link, and report digital evidence using little more than mouse clicks or touch screens in the web browser on their desktop, laptop or tablet computer.

Tracks Inspector brings simplicity, scalability and collaboration to the handling, storage, processing, management and reporting of digital evidence. It can be deployed across multiple locations and accessed from anywhere to support investigative teams, even in the earliest stages of a case. While not intended to replace laboratory-quality solutions such as FTK, EnCase, Clearwell and others, Tracks Inspector provides the complementary solution to solve more cases and solve them faster by reducing the workloads on digital specialists to only the most complex cases.

[1] Digital Forensic Research Workshop (DFRWS) is a non-profit organization that brings together leading researchers, developers, practitioners and educators in the field of digital forensics from around the world. At the annual dfrws conference, experts are invited to submit solutions to forensics challenges of varying levels of difficulty. Solutions are judged on the completeness and accuracy of findings, organization and presentation of results, and effort in developing new digital forensics techniques and tools.

Contents

The Rising Impact of Digital Forensics on Criminal Investigations

Computers and mobile devices routinely contain evidence related in some way to the planning, coordination, commission, or witnessing of crimes. The digital information from seized electronic devices must be processed by specialists in digital forensics laboratories, which often takes critical parts of investigations out of the hands of detectives.

Typically, the volume of digital information related to a case requires the detective's knowledge to determine what information may be relevant and what clearly is not. This is difficult for a detective to explain to a digital specialist, since the detective can't know exactly how the evidence will look.

This uncertainty and reliance on specialists prevents detectives from leveraging digital evidence as fast or as thoroughly as they would like for all but high-priority cases, since there are too few specialists and labs to process all cases. As a result, investigations can be impeded and cases even abandoned due to the complexity of digital forensics and the special tools and skill sets required.

WHO PERFORMS DIGITAL INVESTIGATIONS?

Reliance on digital forensics specialists prevents detectives from leveraging digital evidence as fast or as thoroughly as they would like.
Tracks Inspector provides a solution for detectives to analyze most digital evidence on their own from a web browser.

Tracks Inspector Puts Digital Investigations into the Hands of Detectives

Tracks Inspector, developed by FOX-IT, provides a digital forensics solution for non-technical detectives. Tracks Inspector enables detectives to search and analyze most digital evidence on their own using the web browser on their desktop, laptop or tablet computer. When evidence requires a specialist, Tracks Inspector notifies the user. [2]

TRACKS INSPECTOR BRINGS:

- Simplicity to investigations involving digital evidence while preserving chain of custody
- Less reliance on digital forensics experts to build and prosecute cases
- Capabilities for detectives to search, tag, analyze, link, and report on digital evidence
- Easy collaboration among investigative teams across locations and agencies
- Budget-friendly deployment of system components across locations and agencies
- A centralized "digital evidence vault" across locations and agencies
- Scalability to grow any and all system components just by adding servers

TRACKS INSPECTOR IS DESIGNED TO:

- Enable detectives to investigate seized digital information within the context of a case from its earliest stages
- Complement laboratory-quality solutions such as EnCase, FTK, Clearwell, ZyLAB, ZiuZ, Analyst's Notebook, and Nuix
- Improve utilization of digital forensics laboratories by reducing caseloads
- Feed evidence that requires the skill sets and tools of specialists to laboratory systems
- Operate with open industry standards such as Linux, MySQL, Google protocol buffers and HTML
- Enable law enforcement agencies to solve more cases faster

EASY TO USE SOLUTION

Tracks Inspector enables detectives to search and analyze most digital evidence on their own using the web browser on their desktop, laptop or tablet computer.

[2] any evidence entered into Tracks Inspector can be accessed and analyzed by laboratory-quality solutions.

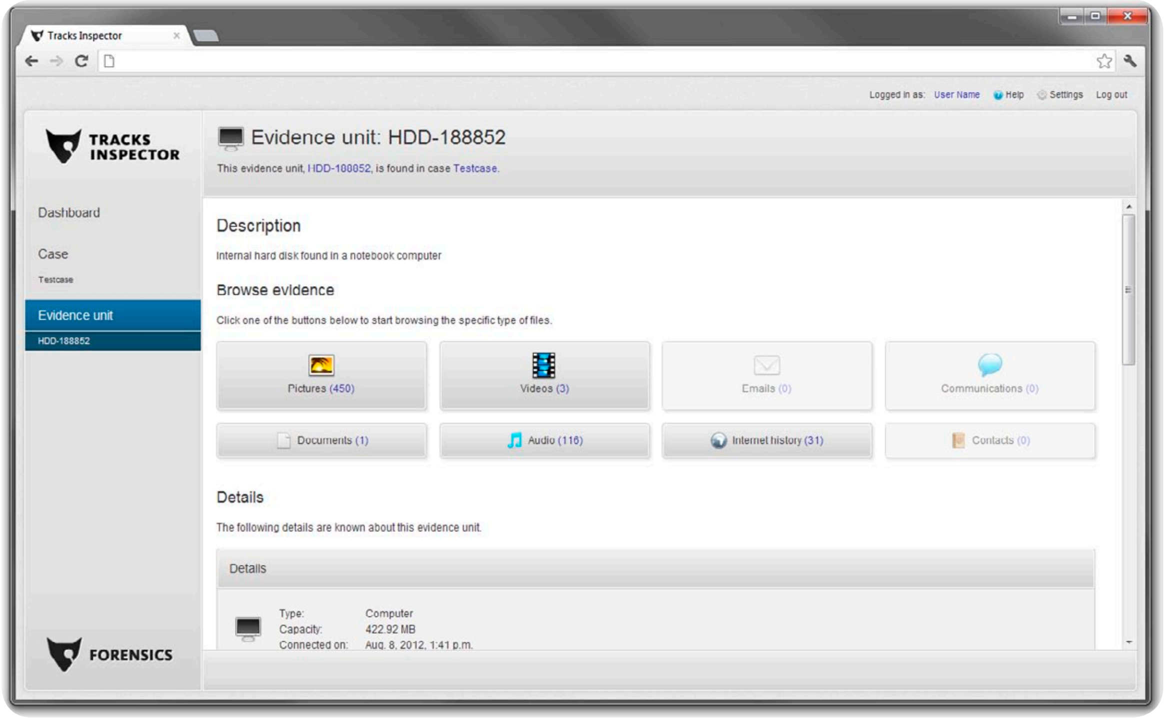
Browser-Based Operation Simplifies Evidence Search and Processing

From the web browser on a desktop, laptop or tablet computer, any detective assigned to a case can intuitively search and analyze the content of seized digital devices (Figure 1). The process is simple and quick, relying almost entirely on mouse clicks or screen touches to identify information relevant to the case, tag evidence, and generate reports. Only when entering keywords for searches or attaching comments to evidence are keypad entries required.

From the Evidence Unit Dashboard, users can select, search and filter digital information to find evidence relevant to the case (Figure 2). Filtering is done by using facets, selecting evidence with specific properties. All files can be viewed, tagged, annotated and reported on through the web browser. If a detective wants to download a file, and has the permission from the Case Administrator who assigns roles and evidence access, he can do so.

Operation is analogous to visiting an online store, where a shopper views and clicks through information to narrow choices of merchandise. The investigator can quickly drill down to that smoking gun he or she is looking for. ›

FIGURE 1 END USER'S EVIDENCE UNIT DASHBOARD



Evidence unit: HDD-188852

This evidence unit, HDD-188852, is found in case Testcase.

Description

Internal hard disk found in a notebook computer

Browse evidence

Click one of the buttons below to start browsing the specific type of files.

Details

The following details are known about this evidence unit.

Details

Type: Computer
Capacity: 422.92 MB
Connected on: Aug. 8, 2012, 1:41 p.m.

FIGURE 2 CLICK OR TOUCH SCREEN DRILLDOWNS FROM EVIDENCE UNIT DASHBOARD

EVIDENCE TYPE	FACETS	OTHER CAPABILITIES
Pictures	Date Camera Make & Model Picture Size Users[1] Origin (e.g., from a document or a compressed file) Tags[2]	Attach text comment to evidence
Videos All major video formats	Date Duration Users Origin Tags[2]	View screenshots of video Run video Attach text comment to evidence
Documents • Word • PDF • Presentations • Spreadsheets	Date Document Type Language Keywords & Phrases Users Origin Tags[2]	View documents[3] View documents with all occurrences of keywords or phrases highlighted[3] Download documents[3] Attach text comment to evidence
Audio	Date Duration Users Origin Tags[2]	Attach text comment to evidence
Email MS Outlook (PST) databases, mbox and more (not webmail)	Language Date Keywords & Phrases Users Origin (IP address) Contact Tags[2]	Open and view email attachments[3] Download attachments[3] Attach text comment to evidence
Internet History	Date URLs Keywords used with Search Engines Cookies and details	Attach text comment to evidence Copy and send links to other investigative team members
Contacts	Keywords & Phrases	
Communication	Date Type Keywords & Phrases	

[1] Tracks Inspector determines user values based on the location of a file in the file system.

[2] Evidence can be tagged by the user or another member of the investigative team with a click/touch—at any time, not just when filtering information. A text box is also available to type comments about tagged or untagged evidence.

[3] Dependent on role in investigation as assigned by Tracks Inspector Case Administrator

‹ in continuation of page 7

FIGURE 3 TRACKS INSPECTOR SMART DASHBOARDS[1]

	PURPOSE
Case Dashboard	• Provide an overview of evidence units in a case • Link evidence units by finding traces of evidence connected to a suspect or common environment[2] • Prioritize evidence units
Evidence Unit Dashboard	• Identify the evidence unit, file types, and how many of each file type were encountered while processing the evidence unit
Operating System Dashboard	• Show when an operating system was used, the suspect's accounts, if it was part of a network or domain, if any USB devices were connected, etc.
User Account Dashboard	• Go beyond the standard user dashboard currently available to investigate system file artifacts in a suspect's user folder which cannot be browsed
Identities Dashboard	• Collect possible suspect identities from author information, email addresses, user registry, phone details, Internet URLs and cookies • Automatically derive a restricted list of main identities • Resolve duplicate identities • Show occurrences of identity in evidence

In addition to investigating digital pictures, videos, documents, audio, email and Internet history, Tracks Inspector users can view computer screen displays as previously viewed by suspects and search operating systems, such as for all who used a seized device.

Tracks Inspector facilitates collaboration across investigative teams working from different locations from anywhere at any time. Team members can access the same data, share links and print reports through their web browsers. Investigations once delayed by caseloads in digital forensics laboratories move faster. More cases can be handled in less time, improving the effectiveness of law enforcement agencies.

Tracks Inspector utilizes open source software to extract text and metadata from digital files, and for converting and rendering text, image, video and audio content. For user or data issues, Tracks Inspector provides online help screens and notifications when investigations need to be escalated to digital forensics specialists.

SMART DASHBOARDS

Currently, Tracks Inspector offers standard dashboards at case and evidence unit levels. By late 2012, "smart dashboards" as described in Figure 3 will be included to further leverage information extracted by Tracks Inspector's Evidence Monitor. This information can be used to more quickly discover related evidence units and reveal information about user behavior that would not be reflected in standard investigations of images, videos, documents, emails and Internet history.

[1] Planned for release in the fall of 2012

[2] Examples of linking evidence units would be identifying laptops used on the same WiFi LAN, or different file systems showing traces of the same user ID, or a USB stick (one evidence unit) that was connected to an operating system (another evidence unit).

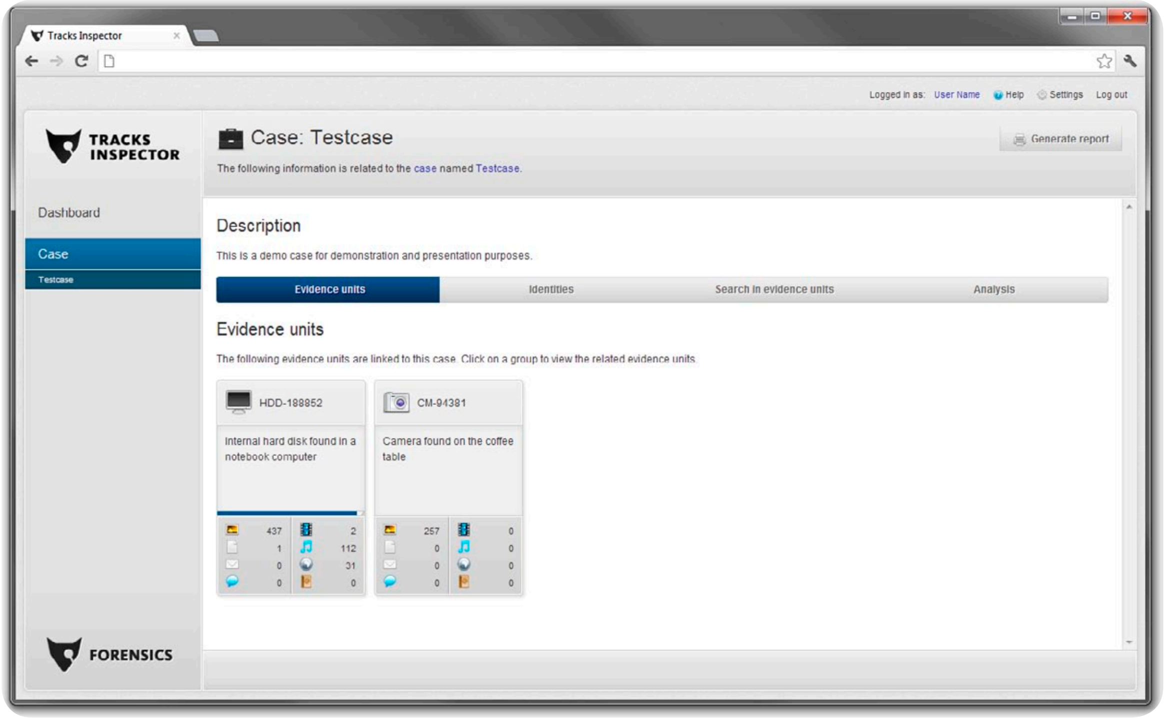
Case administrator Controls Evidence and System Access by Role-Based Investigative Teams

With primarily the same click/touch operation (Figure 4), a Case Administrator in charge of an investigation(s) involving digital evidence can:

- Create the case(s) in Tracks Inspector
- Acquire the digital information source(s) suspected of containing evidence
- Assign the case(s) to detectives based on their roles in the investigation
- Allow or deny access to evidence according to investigative roles

Tracks Inspector preserves chain of custody with the same evidence handling procedures and best practices used by digital forensics laboratories. Industry-standard write blockers secure digital information in Tracks Inspector's forensically sound write-protected environment. Access to information is controlled by the Case Administrator on a per-user basis. Legally privileged information can be hidden from any type of search. (There is a separate role in the system to assign users who are authorized to view privileged data.)

FIGURE 4 CASE ADMINISTRATOR'S MANAGEMENT DASHBOARD



Case: Testcase

The following information is related to the case named Testcase.

Description

This is a demo case for demonstration and presentation purposes.

Evidence units

The following evidence units are linked to this case. Click on a group to view the related evidence units.

Internal hard disk found in a notebook computer

Camera found on the coffee table

How Tracks Inspector Works

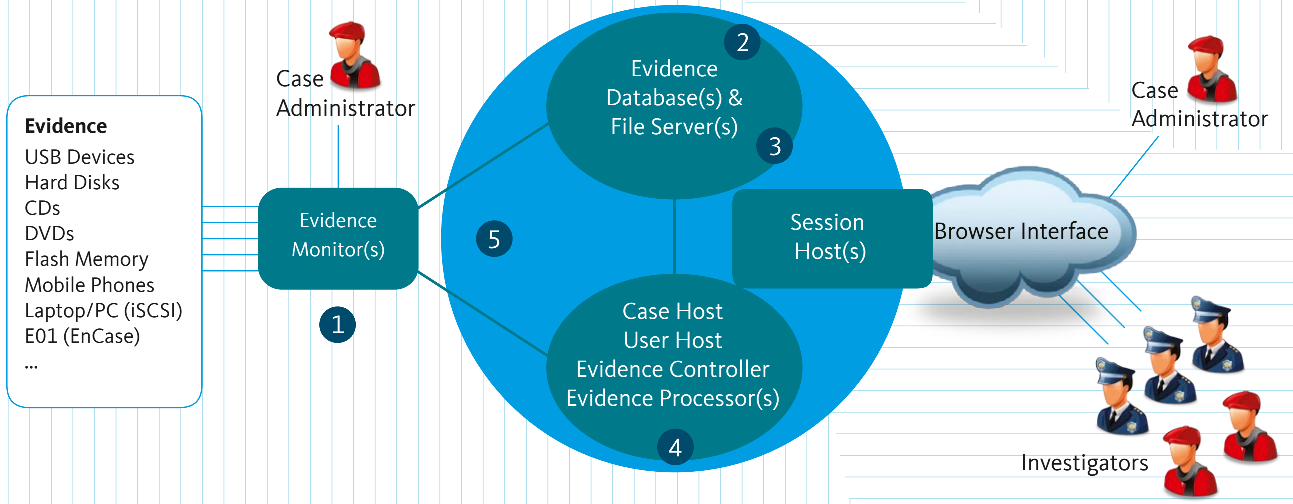
A basic knowledge of Tracks Inspector's architecture (Figure 5) helps to explain the system's power of simplicity and how it can be leveraged across multiple locations and law enforcement agencies.

SYSTEM COMPONENTS INCLUDE:

- Evidence Monitor for device imaging that inputs digital information into Tracks Inspector
- Evidence Controller to track information and where each evidence unit is connected in the system
- Evidence Database which stores information and metadata to accelerate information retrieval
- Evidence Processor which processes information and extracts metadata for use by Case, User, and Session hosts
- Session Host to manage system components and communications for browser sessions
- User Host which provides user functionality and user activity audit trail
- Case Host to register cases and track case information, such as assigned investigators, roles in investigations and evidence access permissions

Tracks Inspector's Evidence Monitor, Evidence Database, Evidence Processing, and Session Host can be deployed across servers at different locations. This enables multiple law enforcement agencies to pool resources and share system implementation, minimizing each agency's costs. Every system component is scalable, simply by adding servers. For example, there can be multiple Evidence Monitors to support Case Administrators in different jurisdictions, or Evidence Processing can be implemented across multiple nodes to support the volume of digital evidence from cases across jurisdictions. Volume is not an issue with Tracks Inspector, since analysis of each evidence unit is stored in its own MySQL database. Even with hundreds and thousands of evidence units, Tracks Inspector easily distributes processing, archives evidence units, and splits or merges cases when necessary.

FIGURE 5 Tracks Inspector architecture



1 Evidence imaging can be performed by the Tracks Inspector Evidence Monitor Appliance (evidence processed during imaging) or by a third-party appliance or imaging software (evidence processed after imaging). Tracks Inspector Evidence Monitor(s) is iSCSI-ready for remote imaging.

2 Meta-information, as used in Tracks Inspector, simplifies evidence search and investigative team collaboration.

3 Evidence stored in Tracks Inspector is available to digital forensics specialists with laboratory-quality tools such as EnCase and FTK to solve complex issues beyond the scope of Tracks Inspector. (Tracks Inspector tells end users when investigation requires a specialist.)

4 Evidence Processor(s) extracts files and metadata from evidence and identifies patterns that link evidence units.

5 Tracks Inspector deployment is not site-specific. Servers and Tracks Inspector components can be located across different locations. Any and all system functionality is scalable by adding servers. End users can access, investigate and print Tracks Inspector data from any location.

Meeting the Challenge of Today's Digital World

The occurrences and volume of digital evidence in criminal cases can no longer be managed by digital forensics laboratories alone. Tracks Inspector provides an innovative and pragmatic solution to harvest most digital evidence in the field by detectives on their own, enabling faster investigations and reduced caseloads for digital specialists whose skill sets and tools can focus on the most complex cases.

As a complement to laboratory tools and interoperable with them, Tracks Inspector's simplicity, distributed architecture, and scalability for storing, processing, and managing digital evidence increases opportunities for collaboration, creating a centralized "digital evidence vault" and sharing budget-friendly deployment across locations and agencies.

Computers and mobile devices change how today's world operates, including the criminal element. With Tracks Inspector, law enforcement can better adapt to "digital change" and more effectively carry out their mission to deter crime and bring perpetrators to justice.

COLLABORATION AND INTEROPERABILITY

As a complement to laboratory-quality tools and interoperable with them, Tracks Inspector increases opportunities for collaboration, creating a centralized "digital evidence vault" and sharing budget-friendly deployment across locations and agencies.

FOX-IT prevents, solves and mitigates the most serious cyber threats with innovative solutions for government, defense, law enforcement, critical infrastructure, banking, and commercial enterprise clients worldwide. Our approach combines human intelligence and technology into innovative solutions that ensure a more secure society. We develop custom and packaged solutions that maintain the security of sensitive government systems, protect industrial control networks, defend online banking systems, and secure highly confidential data and networks.

for a more secure society

FOX IT

FOX-IT
Olof Palmestraat 6, Delft
PO BOX 638, 2600 AP Delft
The Netherlands

T +31 (0)15 284 79 99
F +31 (0)15 284 79 90
E fox@fox-it.com

TRACKSINSPECTOR.COM
FOX-IT.COM