eForensics VOL. 12 NO. 02

ISSN 2300-6986

DIGITAL FORENSICS TOOLS

ADVANCED DIGITAL FORENSICS WITH **FTK IMAGER**

ARTIFICIAL INTELLIGENCE AND **IMAGE MANIPULATION**

DIGITAL FORENSIC TOOLS FOR WEAPONIZED DRONE INCIDENTS

EDITOR'S WORD

Dear readers,

In this issue, you can read about digital forensics tools. Forensic tools are needed in today's digital environment. By using digital forensic tools, you can investigate many digital devices. They can be accessed, investigated, and analyzed with DFiR tools. Investigative techniques or gathering evidence for judicial use may be employed with the tools. These tools allow you to complete a comprehensive investigation. You can decrypt encrypted files, extract valuable data, preserve data integrity, and much more. Tools for digital forensics are useful for all kinds of law enforcement and incident response functions, as well as cybersecurity and maintenance.
In this issue, you read the article written by Amber Schroader. She's comparing two tools. It is a useful method in the case of any lab, and the two-tool method has real value when reviewing the comparisons. Kate Libby will present, in her article, an overview of some of the best tools in the field. Inside, you will find links to the resources, that will either feature more information about the tools or the project page itself. You will gain a more in-depth understanding of these tools.
Adam Karim presents "FTK Imager, also known as Forensic Toolkit Imager, is a software tool commonly used in the field of digital forensics. It is developed and distributed by AccessData, a company that specializes in digital investigations and forensic software. FTK Imager is a free, standalone application that provides forensic professionals, law enforcement agencies, and computer forensic examiners with the ability to create forensic images of digital storage media, such as hard drives, USB drives, memory cards, and other storage devices."
Jeff Minakata tell you about AI usage. "Given the rise of bad actors leveraging AI to generate fake images to influence people's perceptions, we will be looking at one tool (Hive AI Detector) to potentially combat this growing issue and make identifying these AI-generated images quickly and easily. Fortunately, there are some easy tools that we can employ, one being Hive AI Detector, a Chrome Web Store plugin. Given that the AI images that we are likely to view will be online anyway, this becomes an ideal tool for us to use."
You can find more information in the Table of Contents. There are many interesting articles and interviews in this issue, so I recommend reading them all.
I want to thank everyone who contributed to this issue and helped me create the magazine. A big thank you to all our readers!

Enjoy reading,
Ewa

EDITOR-IN-CHIEF
JOANNA KRETOWICZ
JOANNA.KRETOWICZ@EFORENSICSMAG.COM

ASSOCIATE EDITOR
EWA DUDZIC
EWA.DUDZIC@EFORENSICSMAG.COM

Cover Image
Wiktoria Bukowska

Advisory Board
Paulo Pereira
Alessandro Lofaro
Kharim Mchatta

Cover Design
Wiktoria Bukowska

Reviewers
David Michaud, Gabriel Carvalhaes, Ranjitha R, Davide Gabrini, Hammad Arshed, Jan-Tilo Kirchhoff, Dauda Sule, Yousuf Zubairi, Alex Gilles, David Von Vistauxx, Leighton Johnson III, Bartek Adach

PUBLISHER HAKIN9 MEDIA SP. Z O.O. 00-585 WARSZAWA UL. BAGATELA 10/30 EFORENSICSMAG.COM

ADVANCED DIGITAL FORENSICS WITH FTK IMAGER

ADAM KARIM

FTK Imager, also known as Forensic Toolkit Imager, is a software tool commonly used in the field of digital forensics. It is developed and distributed by AccessData, a company that specializes in digital investigations and forensic software. FTK Imager is a free, standalone application that provides forensic professionals, law enforcement agencies, and computer forensic examiners with the ability to create forensic images of digital storage media, such as hard drives, USB drives, memory cards, and other storage devices.

Key features of FTK Imager include:

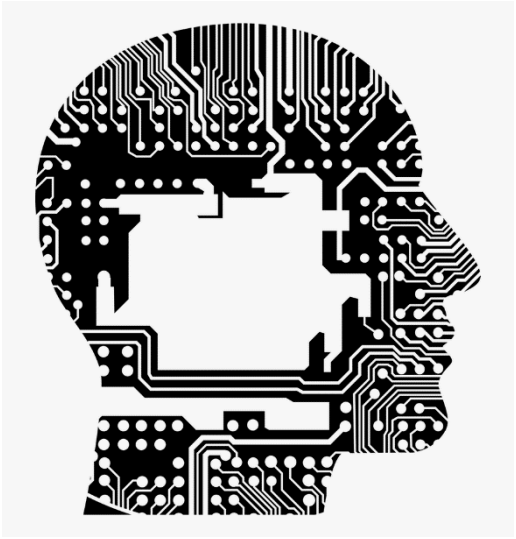
1. Disk Imaging: FTK Imager allows users to create forensic images of digital storage media. These images are bit-by-bit copies of the original media, preserving all data, file structures, and metadata for forensic analysis.

2. File Examination: It provides the capability to examine files within a forensic image without altering the original data. This includes viewing file attributes, directory structures, and file content.

Artificial Intelligence and Image Manipulation

Jeff Minakata

During the last couple of years, we have seen an explosive growth in both AI technology development and its mainstream use, both good and bad. Given the rise of bad actors leveraging AI to generate fake images to influence people's perceptions we will be looking at one tool (*Hive AI Detector*) to potentially combat this growing issue and make identifying these AI generated images quickly and easily.



Fortunately, there are some easy tools that we can employ, one being *Hive AI Detector*, a Chrome Web Store plugin. Given that the AI images that we are likely to view will be online anyways this becomes an ideal tool for us to use. The installation is the same as any other Chrome app and there is no configuration needed so we are going to skip the setup process.

BEST DIGITAL FORENSIC TOOLS

KATE LIBBY

Digital forensic investigators rely on a variety of tools that are crucial in various aspects of digital forensics like data recovery, analysis, and reporting. This article is an overview of some of the best tools in the field, there are links in the resources that will either feature more information about the tools or the project page itself. Please visit the resources to gain a more in-depth understanding of these tools.

I include licensed software and hardware to open-source platforms to showcase a variety of choices in selection of products. As the science of digital forensics is growing and becomes more advanced, the barrier of entry has become lower as well. We are now seeing an increase in individuals learning this speciality because of the widely accessible tools and resources available, which is why you will find a variety of tools, for the most capable experienced investigator to tools for the absolute beginner.

Autopsy

This free, open-source tool is popular in the digital forensics community for conducting digital investigations. It is capable of analyzing hard drives, smartphones, and media cards, and is designed to be user-friendly with a graphical interface, suitable for both beginners and experienced investigators. Autopsy has a very low barrier to learning as it literally walks you through the process of data acquisition to analysis step by step. It also features a few built in modules to handle a variety of data types. Basis Technologies also offers a training and certification track if you wish to take your experience to the next level. I have included a very brief walk-through video of installing Autopsy within a Windows environment.

Navigating the Skies of Justice: Digital Forensic Tools for Weaponized Drone Incidents

Rhonda Johnson

As technology advances, so do the threats that law enforcement agencies face. The emergence of weaponized drones poses a unique challenge, demanding innovative approaches to investigation and evidence collection. In this context, digital forensic tools play a pivotal role in aiding law enforcement agencies to unravel the complexities of weaponized drone incidents. This article delves into the significance of digital forensic tools tailored for such incidents, providing detailed insights and a comprehensive summary in the form of a table.

1. The Challenge of Weaponized Drones

Weaponized drones present a multifaceted challenge for law enforcement agencies (Elliott, 2018). From identifying the operators to analyzing flight patterns and payload delivery mechanisms, investigations into weaponized drone incidents require a specialized set of digital forensic tools.

USING TWO TOOLS FOR SMARTPHONE FORENSICS ACQUISITIONS

AMBER SCHROADER

There is no greater area in digital forensics that changes more frequently than smartphones. The many differences between manufacturers, regions, and devices can cause a wide range of problems when looking at the smartphone from an acquisition perspective. Keeping this in mind, the landscape of available tools has also changed dramatically over the past few years. With the development of more and more private tools vs open-source tools, there are a variety of options to select from. The following will review the different acquisition options between an open-source solution vs a private solution, and how the use of both tools can benefit an organization.

Open-source Tool

Autopsy with iLeap

https://www.autopsy.com/

https://github.com/abrignoni

Autopsy® is the premier end-to-end open-source digital forensics platform built by Basis Technology. With core features one would expect to see in commercial forensic tools, Autopsy is a fast, thorough, and efficient hard drive investigation solution that evolves with your needs.

iLeap: iOS Logs, Events, And Plist Parser

Aleap: Android Logs Events And Protobuf Parser

Private Tool: Paraben's E3 Forensic Platform (E3:UNIVERSAL License)

https://paraben.com/ - Trials are available for five days after signing up on the website.

DFIR Labs in the Cloud: The Future of Digital Forensics

Belkasoft

Introduction

The surge in data volumes stored by digital devices has created a headache for forensic examiners—too many devices are piling up in digital forensics labs due to limited resources (O'Reilly, 2022). What causes this problem is a shortage of space to store evidence and insufficient computing resources to process it efficiently. However, there is a smart solution already making waves in other sectors. It involves moving a Digital Forensics and Incident Response (DFIR) lab to the cloud.

This shift simplifies the management of hardware resources and offers potential benefits such as improved scalability, cost-efficiency, and accessibility. But is it feasible? The sensitivity of data handled by DFIR labs introduces a number of complexities to this equation. Another question is whether digital forensics tools are ready for this change. Can they integrate with cloud environments and keep providing the same level of efficiency and security?

In this article, we will cover the ins and outs of adopting cloud solutions in digital forensics and explore how DFIR tools can accommodate this change. As an example, we will look into Belkasoft digital forensics software, known for its innovative solutions, and explore the features that enable it to embrace the cloud approach.

CELLEBRITE PHYSICAL ANALYZER ULTRA

Designed to make mobile forensics accessible to all.

CHRISTOPHER COLLINS

With technology evolving and new apps released daily, crime is ever changing on the digital front. As a result Cellibrate released an ultimate solution; PA Ultra (PAU).

PAU allowsthe examiner to use a full dashboard of data discovery, with commonly sought evidence on devices. The PAU dashboard gives the user a breakdown of apps and device locations, breaking the selection down to a summary of how often other apps are used and how often locations are visited.

PAU allows the user to choose the type of evidence they wish to discover such as pictures, videos, and notes, as well as internal log files. The evidence is presented in a report using PAU Cellebrite Reader, which is used by investigators in civil prosecution proceedings. One notable improvement by PAU is the generation of a database file as a mobile device extraction.

This database file allows a mobile device extraction to be reopened in PAU in a fraction of the time related to older versions of PAU as the evidence does not need to be reprocessed again, 5 to 10 minutes compared to several hours.I had the opportunity with fellow researchers to investigate PAU during the 2023 “Cellebrite Capture the Flag (CTF)” event, where we (the Revo-lutionaries) took home first place.

In this CTF, Cellebrite provided the contestants with 4 mobile device extractions, along with a free trial of PAU. During the CTF, we utilized multiple tools but mainly focussed on using PAU.

Since the competition, I have been using PAU for most of my forensic analysis and reports. The prosecution find the analysis reports easy to use and navigate, since a new format and dashboard is used.

The backbone of PAU is almost the same as older versions when searching for evidence within log files, and database tables are conducted. I have always had an affinity for PA's ability to search through these artifacts, as it has a user friendly interface. PAU maintains the custom database tool, SQLite Wizard, and other tools such as App Genie.

PAU is a great, as it builds on PA's already great suite.

PAU use improved mobile device forensics making mobile forensics accessible to everyone such as detectives or investigators working cases, or attorneys prosecuting these cases. Evidence is presented in an easy to read format, with breakdowns and in app analysis. With Cellebrite's commitment to continually improve digital forensic investigation and reporting, they are upholding their mission to accelerate justice for the community and victims.

About the Author

Christopher Collins is a Detective Sergeant with the Lake Jackson Police Department, in Lake Jackson, Texas. One of the roles he holds is as a Digital Forensic Examiner focusing on mobile device forensics. Detective Sergeant Collins has been in Law Enforcement for over 14 years in Texas and has obtained his Master Peace Officer, Master Telecommunicator, and Advanced Instructor Certificates through the Texas Commission on Law Enforcement (TCOLE). Detective Sergeant Collins has earned an Associate's Degree in Computer Technology for Network Management, and is in the process of finishing another Associate's Degree in Computer Technology for Cybersecurity. Detective Sergeant Collins has achieved multiple training certificates in the mobile device forensics field to include Cellebrite Mobile Forensic Fundamentals (CMFF), Certified Operator (CCO), Certified Physical Analyst (CCPA), Advanced Smartphone Analyst (CASA), and Certified Mobile Examiner (CCME), he also holds a certificate through Grayshift as a certified GrayKey Operator (GKO). Detective Sergeant Collins has developed a training course on the basics of mobile device evidence and device collection that

has been deployed and adopted by his local area and shared with Law Enforcement Agencies in Colorado, Alabama, Newfoundland (Canada), and U.S. Army Criminal Investigations (Germany). Detective Sergeant Collins has also provided expert witness testimony in criminal court for mobile device forensics.

INTERVIEW WITH DAUDA SULE

eFORENSICS TEAM

Could you please introduce yourself to our readers?

I am Dauda Sule, currently an academic at the Air Force Institute of Technology, Kaduna, Nigeria.

Can you describe your job and what you do in a few words?

I create curriculum, conduct research, and give lectures to undergraduate students who want to earn a bachelor's degree in cyber security.

When it comes to your work week, how would you describe it?

Hectic! I give lectures, administer and grade assessments, offer student counseling, and handle a variety of departmental administrative responsibilities.

INTERVIEW WITH KUNAL DUTT

eFORENSICS TEAM

Please let our readers know about yourself.

My name is Kunal Dutt. I live in India. I completed my Bachelor of Engineering in computer science and later on, I opted for a master's of engineering with a specialisation in cybersecurity with all due respect to my interest and passion. After spending six long years with theories and practicals, I joined a company as a Security analyst and I have been doing my job for the last four years. So technically I have been in this industry for a decade and along with my industrial experience, I have been a certified cybersecurity mentor in myriad domains like cyber forensics, ethical hacking, Governance-Risk-Compliance and many more. I have been a security researcher where I worked in the innovative arena of vehicle cyber security and published research work in a reputed journal. I love to learn and share my knowledge in the best practical approach to this fraternity by carrying real-time incident case studies with all due respect to my nature of work.

eFORENSICS

MAGAZINE

CURRENTLY OPEN FOR SUBMISSION

WRITERS WHO ARE LOOKING TO SEND OUT THEIR WORKS ON DIGITAL FORENSICS TOPICS ARE INVITED TO SUBMIT THEIR ARTICLES TO US.

OUR CATEGORIES INCLUDE MALWARE FORENSCIS, INCIDENT RESPONCE, SATELLITE FORENSICS, AUTOPSY 4.21, DIGITAL FORENSICS WITH KALI LINUX, COMPUTER FORENSICS AND INVESTIGATIONS, CISSP EXAM STUDY GUIDE, MEMORY FORENSICS, DRONE FORENSICS.

ANY QUESTIONS OR CONCERNS CAN BE DIRECTED TO OUR EMAIL:
EWA.DUDZIC@EFORENSICSMAG.COM