



FOREINSICS

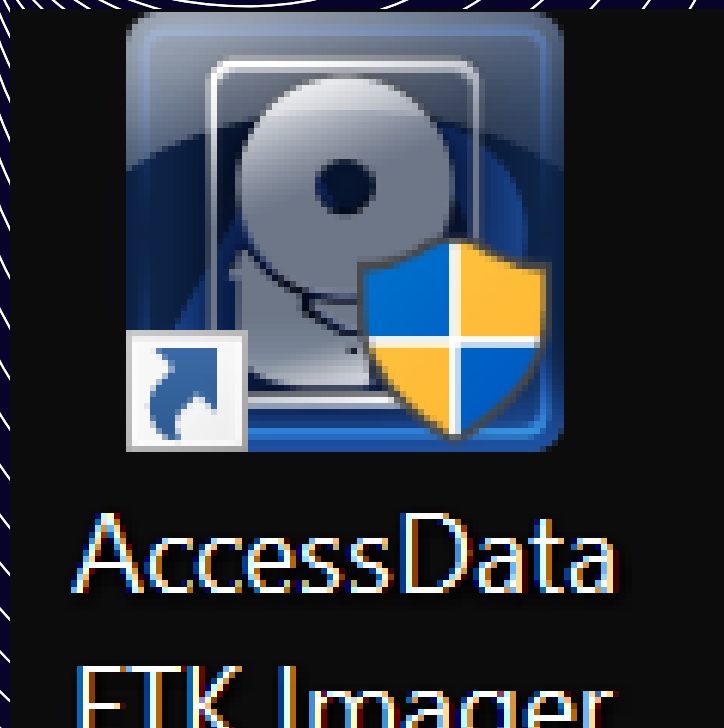
[EXPLORE NOW](#)

CHAIN OF CUSTODY



Evidence number	Description
01	USB flash drive storage <u>SanDisk</u> <u>cruzer</u> Contains evidence
02	4 E0 files, 1 CVS file <u>and</u> one README

Evidence number	date/time	Received from	Released to	Comment
01	11/0/.2024 17:00hrs 02	John Morgan	Laetitia <u>Badaro</u>	An image file was created using FTK Imager 4.3.11 on an isolated virtual machine with the software write blocking in place all USB storage device
02	10/04/2024 15:00hrs	John Morgan	Laetitia <u>Badaro</u>	We chose the easiest file to open which is 4 E0 <u>files</u> , it was opened with two different software autopsy and FDK imager that gave us the same content



FTK IMAGER

FTK Imager is primarily categorized as digital forensic software, designed to acquire and analyze digital evidence from computer systems, it allows forensic investigators to create forensic images of hard drives, partitions, and logical files

1.Acquiring data:

- FTK Imager can acquire data from various devices and media, including hard drives, memory cards, USB drives, optical disks, and mobile phones.
- It creates forensic images of the data, which are exact copies of the original data for analysis and verification.
- Supports various image formats such as E01, DD, SMART, and AFF.
- Can create logical images based on criteria like file types, dates, or keywords.

2. Previewing data:

- FTK Imager allows previewing data before acquisition, saving time and resources.
- Displays file and folder contents, metadata (file names, sizes, dates, hashes), file system structure, partitions, and unallocated space.
- Capable of previewing data from encrypted or compressed files, as well as live systems or memory dumps.

3.Analyzing data:

- After acquiring data, FTK Imager enables analysis without modifying it.
- Can mount forensic images as read-only drives for access and examination.
- Export data to formats like CSV, HTML, or XML.
- Perform basic searches and filters based on file name, extension, hash, or keyword.
- Generates reports and logs for documentation and verification.

4.Recovering data:

- FTK Imager assists in recovering hidden, deleted, or corrupted data.
- Identifies and recovers data from various file systems (FAT, NTFS, HFS, EXT, UFS), unallocated space, slack space, and bad sectors.
- Recovers data from encrypted or compressed files, as well as RAID arrays or virtual machines.

5. Comparing data:

- Helps in comparing data from different sources or images.
- Uses hashes (MD5, SHA1, SHA256, SHA512) for unique identification.
- Generates and verifies hashes of files, folders, partitions, or images.
- Compares hashes from different sources or images to identify matches or mismatches.

6. Integrating data:

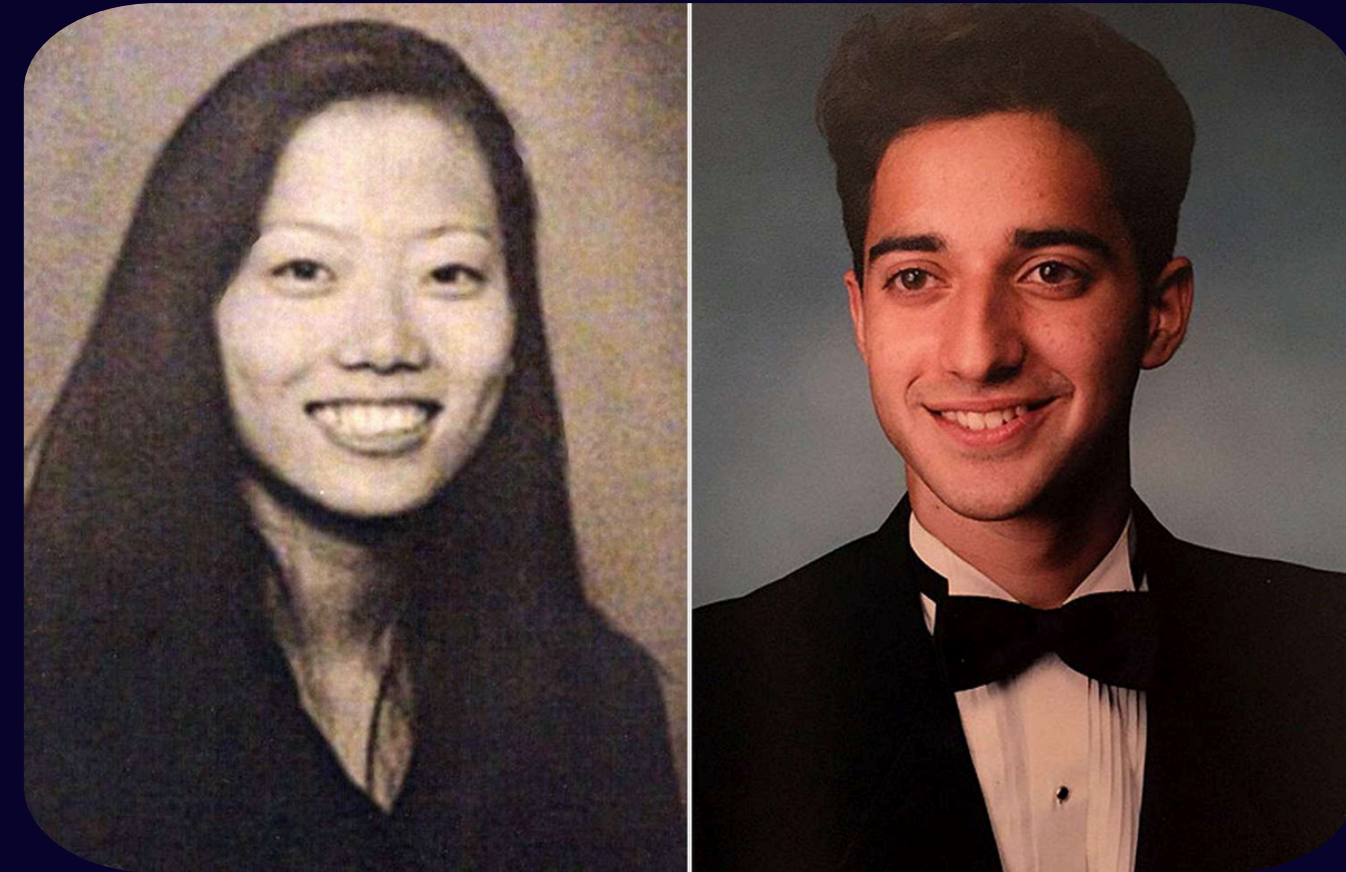
- Integrates data from different sources or images to create a comprehensive view.
- Imports and exports data from other forensic tools such as EnCase, X-Ways, Cellebrite, or Magnet.
- Adds data from different sources to a single case file for analysis by FTK.
- Creates portable case files for sharing and viewing without installing FTK Imager.

THE MURDER OF HAE MIN LEE

hae min lee was a student from baltimore marilna she was murdered by her boyfreind andnaan sayed in january 1999 . ht e main too that was use was ftk imager

ftk imager was used during the reinvestigation of the crime to be sure of the conviction because at the time the technology wasn't advanced enough

- **Cell Phone Evidence:** FTK Imager was used to extract call logs, text messages, and location data from Hae Min Lee's cell phone, which was recovered near her burial site. This data provided a timeline of her movements on the day of her disappearance, crucial for reconstructing events.
- **Computer Forensics:** FTK Imager was employed to examine the hard drive of a computer found at Adnan Syed's home. Digital evidence retrieved from the computer, including email correspondence and search history, provided insights into the relationship between Hae and Adnan and possible motives for the crime.
- **GPS Data Analysis:** FTK Imager was used to extract GPS data from various devices. This data helped reconstruct the routes taken by Adnan Syed and others on the day of the murder, aiding in establishing their whereabouts and potential involvement in the crime.



AUTOPSY



Autopsy®
OPEN | EXTENSIBLE | FAST

Autopsy, a digital forensics platform, is characterized by its ability to analyze digital evidence from computer systems. It allows forensic investigators to examine file systems, recover deleted files, and generate comprehensive reports, aiding in the investigation of criminal activities and incidents.

1. Data Acquisition:

- Autopsy supports acquiring data from various sources including:
 - Hard drives:
 - Mobile phones:
 - Cloud storage:
 - RAM:

3. Data Carving:

- Autopsy employs data carving techniques to extract specific data types from unallocated space or fragmented files.
- It can recover files based on file signatures, allowing the extraction of images, documents, emails, and other file types even if they have been deleted or partially overwritten.

5. Timeline Generation:

- Autopsy generates timelines of events on the system, providing a chronological view of user activity, file modifications, and system changes.
- Timeline analysis helps investigators understand the sequence of events and relationships between different activities, aiding in the reconstruction of digital incidents.

2. File System Analysis:

- Autopsy reconstructs file systems from acquired disk images and analyzes them to recover deleted data and uncover hidden files and activities.
- It supports various file systems including NTFS, FAT, exFAT, HFS+, and EXT.
- The tool can identify file attributes, including timestamps, ownership, and permissions, aiding in the analysis of file usage and manipulation.

4. Registry Analysis:

- Autopsy includes features for analyzing the Windows Registry, a critical component of the Windows operating system that stores configuration settings, user activities, and system information.
- It can parse registry hives, revealing installed software, user activities, USB device history, and other relevant information.

6. Reporting and Visualization:

- Autopsy facilitates the creation of comprehensive reports and visualizations of the findings.
- It provides customizable report templates and visual representations of data, helping investigators to effectively communicate their findings in a clear and understandable manner.

HANNAH CLARKE AND HER CHILDREN MURDER

On 19 February 2020, Rowan Baxter perpetrated a quadruple murder-suicide in Camp Hill, Queensland, Australia. Baxter fatally burned his 31-year-old estranged wife Hannah Clarke and their three children before dying by suicide at the scene

1. Communication Patterns:

- Autopsy helped in recovering deleted messages, emails, and social media communications between Hannah and Rowan Baxter.
- This revealed a history of abusive behavior, threats, and controlling behavior exerted by the perpetrator, providing essential context to the investigation.

2. Tracking :

- Autopsy's analysis of GPS data from smartphones provided valuable insights into Rowan Baxter's movements leading up to the crime.
- It helped establish Baxter's whereabouts, identifying his proximity to the crime scene, and tracking his movements before and after the murders.

3. pictures:

- Autopsy assisted in identifying digital artifacts such as photos, videos, and browsing history that provided additional evidence supporting the case.
- These artifacts helped establish Baxter's state of mind, his intentions leading up to the crime, and his actions afterward.





VISUAL STUDIO

1. Software Development:

- **Code Editor:** Visual Studio offers a powerful code editor with features like syntax highlighting, code completion, and code refactoring tools.
- **Debugging:** Debugging tools allow developers to find and fix issues in their code efficiently. Visual Studio provides features like breakpoints, watch windows, and step-through debugging.
- **Version Control:** Visual Studio integrates with version control systems such as Git, allowing developers to manage source code repositories directly within the IDE.
- **Code Analysis:** It includes tools for static code analysis, which help identify potential bugs, security vulnerabilities, and code quality issues.
- **Unit Testing:** Visual Studio supports unit testing frameworks, allowing developers to write and run tests directly within the IDE.
- **Performance Profiling:** Developers can analyze the performance of their applications using built-in profiling tools, helping to optimize performance and identify bottlenecks.

2. Web Development:

- **Web Development Tools:** Visual Studio includes features tailored for web development, such as support for HTML, CSS, JavaScript, and popular web frameworks like ASP.NET and Node.js.
- **Web Server Integration:** It includes a built-in web server for testing web applications locally.
- **Client-side Debugging:** Visual Studio supports debugging JavaScript code running in web browsers.

5. Cloud Development:

- **Cloud Services Integration:** Visual Studio integrates with cloud platforms like Azure, allowing developers to build, deploy, and manage cloud-based applications directly from the IDE.
- **Serverless Development:** It supports the development of serverless applications using Azure Functions.

3. Mobile Development:

- **Mobile App Development:** Visual Studio supports the development of mobile applications for iOS, Android, and Windows platforms using frameworks like Xamarin.
- **Emulators and Simulators:** It provides emulators and simulators for testing mobile applications on various devices and platforms.

6. Data Science and AI:

- **Data Analysis Tools:** Visual Studio provides tools for data analysis and visualization, including integration with libraries like NumPy and Pandas.
- **Machine Learning Tools:** It includes tools for building and training machine learning models using frameworks like TensorFlow and PyTorch.

4. Desktop Development:

- **Desktop App Development:** Visual Studio supports the development of desktop applications for Windows using frameworks like WPF (Windows Presentation Foundation) and WinForms.
- **UI Design Tools:** It includes tools for designing user interfaces for desktop applications.

7. Game Development:

- **Game Development:** Visual Studio supports game development with tools like Unity3D integration for developing games using the Unity engine.

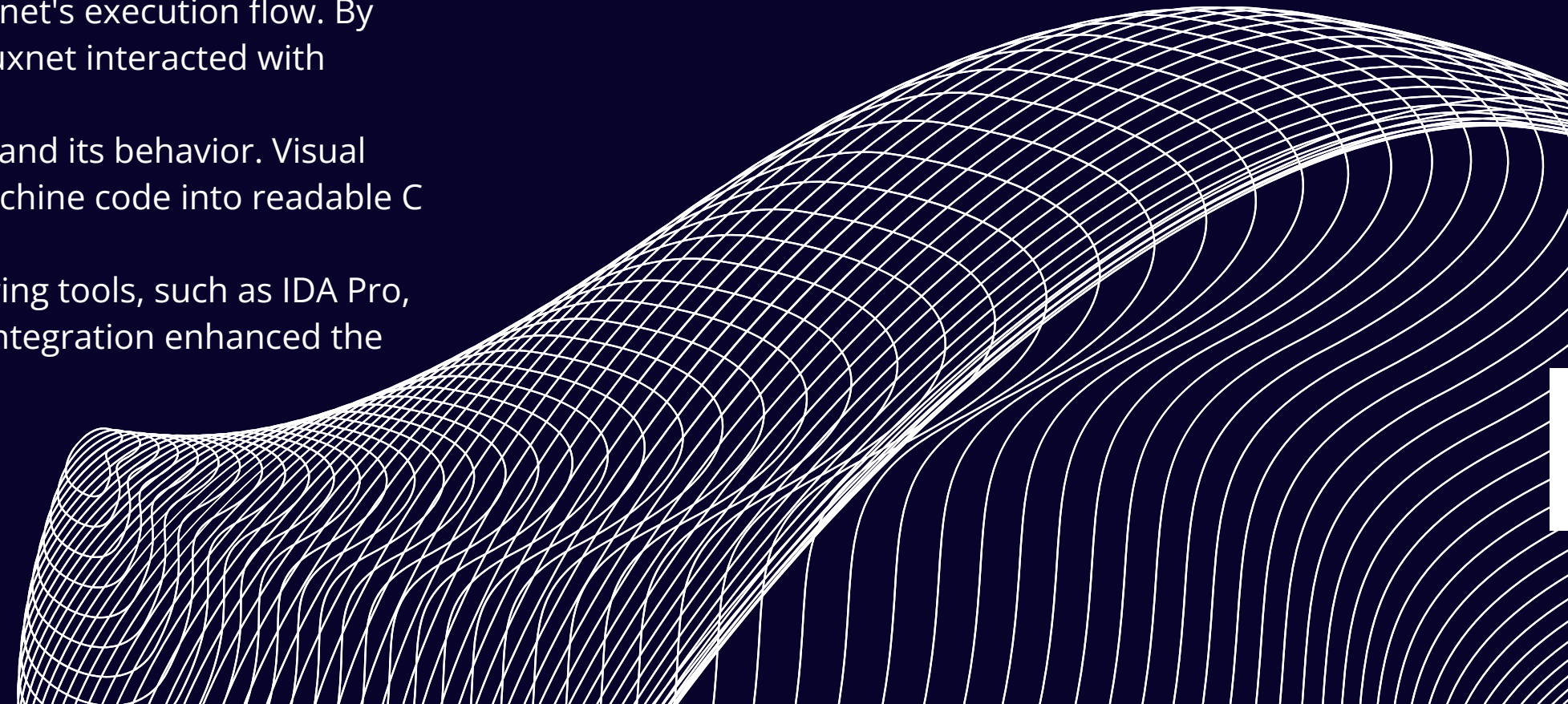
STUXNET WORM



Stuxnet is a malicious computer worm first uncovered in 2010 ,it targets supervisory control and data acquisition (SCADA) systems and is believed to be responsible for causing substantial damage to the nuclear program of Iran.

the problem with resolvinthe stunext case is that it was highly encrypted, making it challenging to understand its functionality. Stuxnet utilized custom communication protocols to interact with industrial control systems, requiring detailed analysis to decipher and exploited multiple zero-day vulnerabilities, which were previously unknown and not patched, adding to the difficulty of analysis.

1. **Code Analysis:** Visual Studio was used to examine the Stuxnet code thoroughly. Its integrated development environment allowed researchers to review the code's structure, identify functions, and understand its logic.
2. **Debugging Capabilities:** Visual Studio's debugging features were crucial in tracing Stuxnet's execution flow. By setting breakpoints and stepping through the code, researchers could observe how Stuxnet interacted with system components and manipulated processes.
3. **Reverse Engineering:** Stuxnet's complex code required reverse engineering to understand its behavior. Visual Studio's decompiler and disassembly features enabled researchers to translate the machine code into readable C or C++ code, providing insights into Stuxnet's operations.
4. **Integration with Other Tools:** Visual Studio's compatibility with other reverse engineering tools, such as IDA Pro, allowed researchers to seamlessly switch between different analysis techniques. This integration enhanced the efficiency of the analysis process.



NEW INNOVATIONS

Artificial Intelligence and Machine Learning (AI/ML)

- Automated data categorization and anomaly detection
- Recognition of previously unknown digital artifacts
- Sentiment analysis and keyword detection in text data such as chat logs and emails
- Analysis of images, audio, and behavior

Cloud Forensics

- Improved data collection from cloud platforms
- Enhanced capabilities in decrypting and analyzing cloud services
- Reconstruction of events and uncovering digital evidence from cloud-based environments

Forensic Readiness

- Establishment of policies, tools, and procedures for rapid evidence collection and analysis
- Training of personnel to respond swiftly to security incidents
- Reduction of time and costs associated with digital forensic investigations

Internet of Things (IoT) Forensics

- Improved data extraction and analysis from interconnected devices
- Integration of IoT-related data with other pieces of evidence
- Development of tools for IoT artifact analysis

Peer-to-Peer (P2P) Networks

- Development of methods to detect threats within P2P networks
- Enhancement of security and privacy measures within distributed systems
- Tools for analyzing and monitoring P2P network activity

ADAPTATION

	Autopsy	FTK	Visual Studio
Cloud Computing	integrating with cloud storage services like Amazon S3, Google Cloud Storage, and Microsoft Azure. This allows investigators to analyze data stored in the cloud directly, either by accessing it through APIs or by downloading it for offline analysis.	it has adapted to cloud computing by offering support for processing and analyzing data stored in cloud environments. It allows to connect to various cloud storage services, including Amazon S3, Google Cloud Storage, and Microsoft Azure, to collect and analyze digital evidence directly from the cloud.	it has adapted to cloud computing by providing integrations with cloud platforms such as Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP). Developers can easily deploy, manage, and debug applications directly in the cloud using Visual Studio, leveraging cloud services for various tasks such as hosting, storage, and data processing.
IoT Devices:	Autopst can extract and do analysis of data from IoT devices like smart home assistants, wearable devices, and connected appliances.	it has expanded its support for IoT device analysis. It includes built-in capabilities to extract data from a wide range of IoT devices, such as smart home devices, wearables, and automotive systems. This enables investigators to analyze digital evidence collected from IoT devices as part of their forensic investigations.	Visual Studio supports IoT development through its IoT development tools and integrations. Developers can use Visual Studio to build, deploy, and debug applications for IoT devices, including those running on platforms like Raspberry Pi, Arduino, and Azure IoT Edge. Visual Studio's IoT development tools provide templates, emulators, and debugging capabilities tailored to IoT development.
Encrypted Communications	it cannot directly decrypt encrypted data, it can still extract metadata, communication patterns, and other relevant information from encrypted sources. Additionally, Autopsy integrates with third-party tools that specialize in cryptographic analysis to assist in decrypting communication data where possible.	it offers features to analyze encrypted communications within the limits of legality and ethical guidelines. While it cannot decrypt encrypted data without proper authorization, FTK assists investigators in extracting metadata and other relevant information from encrypted communications. Additionally, it integrates with third-party tools for cryptographic analysis to aid in decryption efforts.	Visual Studio facilitates the development of applications that utilize encrypted communications. Developers can use libraries and frameworks within Visual Studio to implement encryption and decryption algorithms, secure communication protocols, and authentication mechanisms to ensure the security of data transmitted over networks. Visual Studio also supports the integration of third-party encryption libraries and tools for enhanced security features.

EVIDENCE

