FORKIT

What is FORKIT?

FORKIT is an AI based computer forensics tookit with user friendly interface to facilitate cyber crime investigations.

How it works?

FORKIT analyzes and decodes the Partition Information and recognizes File System i.e. NTFS, FAT, FAT32, EXT4 and extracts the files structure of the Evidence Image file.

It includes different analysis modules including Image recognition and analysis, AI based document analysis, Data carving and Malware detection. Interesting files are tagged along with comments for report generation.

How's it better?

While other forensics software are limited to file extraction and processing, FORKIT provides in-depth analysis such as Object Recognition and detection in picture files, saving hours of work. While also providing AI based document analysis for ease of investigation.

FORKIT also determines if a file contains malware or virus by providing detailed analysis with the help of cryptographic hash values.

Why we need Forensics Tools

With the advancement in digital technology, digital crimes are increasing exponentially. Digital crimes involve attack on digital devices in order to "expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of the asset". In order to reach the attacker, forensics tools plays essential role in digital forensics.

KEY FEATURES

Dashboard

Overall summary of the files extrated from the acquired evidence in different visual representations

Image Recognition

Extract the list of objects recognized in the images, then categorizes based on different categories such as weapon, person, and so much more

Document Analysis

AI based document analysis based on similar content clustering of text documents including pdfs and office files
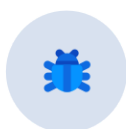
Malware Detection

Identifies if a file is infected with malware or virus based on hash analysis

System Requirements	
PC	Windows compatible PC with Intel i5 or compatible running at 1.9 GHz or higher
Operating System	Microsoft Windows 10
Memory (RAM)	Recommended: 8GB
Space Requirements	4 GB of free disk space for installa on
Functionalities	
Supported Files Systems	FAT, FAT12, FAT16, FAT32, EXFAT, NTFS, EXT2, EXT3, EXT4
Disk Image Formats	.E01, .Ex01, .L01, .Lx01, .vmdk, .vhd, .001
Browser Files	Chrome, Firefox, Internet Explorer (edge)
Email Files	PST, NSF, DBX, MBOX
Other Miscellaneous Files	.lnk, .pf, .db, .evtx, registry hives
Keyword Search	Indexed keyword search
Files Timeline	Creates timeline visualization of extracted files
Reports	PDF, Excel, Text

NCCS
NATIONAL CENTRE FOR CYBER SECURITY