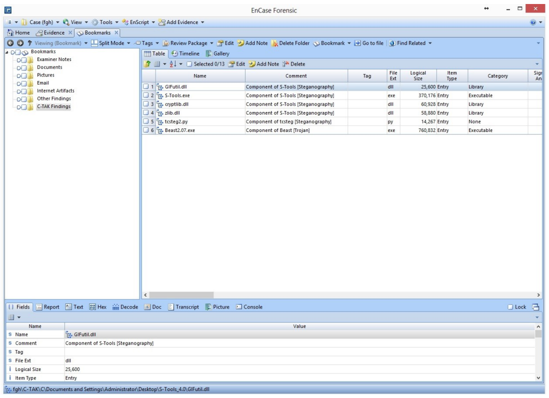
DATA SHEET

C-TAK™

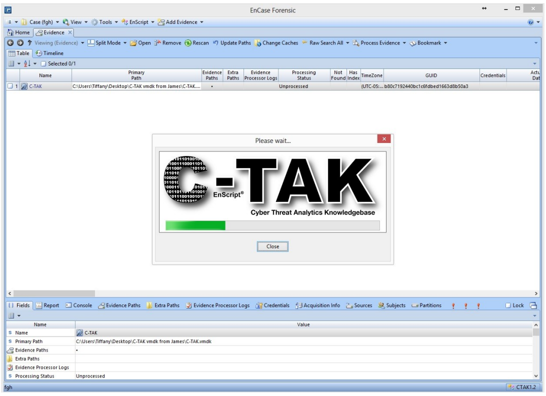
Extend your EnCase® evidence search with Cyber-Threat Analytics Knowledgebase (C-TAK). This technology provides examiners with high performance and accurate identification of cyber threats such as Trojans, Steganography, Rootkits and Anti-forensics that may directly impact investigations. Not only can the presence and classification of these programs allow examiners to view suspects from a new perspective, but paranoia level, suspect sophistication and covert behaviors can also be derived from searching for applications with a common theme. These behaviors can assist in assessing suspect capability, activities, intent, threat or "consciousness of guilt."



	Name	Comment	Tag	File Ext	Logical Size	Item Type	Category
1	GIFutil.dll	Component of S-Tools [Steganography]		dll	25,600	Entry	Library
2	S-Tools.exe	Component of S-Tools [Steganography]		exe	370,176	Entry	Executable
3	cryptlib.dll	Component of S-Tools [Steganography]		dll	60,928	Entry	Library
4	zlib.dll	Component of S-Tools [Steganography]		dll	58,880	Entry	Library
5	tcsteg2.py	Component of tcsteg [Steganography]		py	14,267	Entry	None
6	Beast2.07.exe	Component of Beast [Trojan]		exe	760,832	Entry	Executable

Name	Value
Name	GIFutil.dll
Comment	Component of S-Tools [Steganography]
Tag	
File Ext	dll
Logical Size	25,600
Item Type	Entry

fgh\C-TAK\C\Documents and Settings\Administrator\Desktop\S-Tools_4.0\GIFutil.dll



	Name	Primary Path	Evidence Paths	Extra Paths	Evidence Processor Logs	Processing Status	Not Found	Has Index	TimeZone	GUID	Credentials
1	C-TAK	C:\Users\Tiffany\Desktop\C-TAK vmdk from James\C-TAK....	•			Unprocessed			(UTC-05:...	b80c7192440bc1c6fdbed1663d8b50a3	

Name	Value
Name	C-TAK
Primary Path	C:\Users\Tiffany\Desktop\C-TAK vmdk from James\C-TAK.vmdk
Evidence Paths	•
Extra Paths	
Evidence Processor Logs	
Processing Status	Unprocessed

C-TAK FREE TRIAL:

Our 30-day free trial includes the following datasets: Trojans, Keyloggers, and Rootkits.

C-TAK VERSION 2.0:

C-TAK delivers rapid identification of a broad array of cyber threats. This full version includes the following datasets: Anti-Forensics, Botnet, Fraud Tool, Denial of Service, Encryption, Exploit Scanner, Keylogger, Password Cracking, Peer to Peer, Piracy, Remote Access, Rootkit, Scareware, Sniffer, Spyware, Steganography, Toolkit, Trojan, Web Threat, Wireless Tool, Ransomware.

C-TAK is an EnCase® Application developed specifically for EnCase® AppCentral. C-TAK Version 2.0 has been tested with EnCase Forenisc 7.1.

For more information, contact sales@wetstonetech.com

WetStone