Капинус О.В. Михайлов И.Ю. Marat (forensic[sobachka]bk[tochka]ru)

ILook Investigator.

ILook Investigator (http://www.ilook-forensics.org) — программа для судебных исследований, используемая для анализа образов компьютерных жестких дисков. Данный продукт предоставляется по программе Electronic Crimes Program of the Internal Revenue Service. Лицензионное соглашение конечного пользователя ILook (End User License Agreement) и регистрация программы ограничивает использование ILook только сотрудниками правоохранительных органов. Исключений нет.

ILook создан для исследования образов компьютерных жестких дисков, полученных любой предназначенной для этого судебной программой (также называемых: побитовая копия, посекторная копия, битовый образ) - множество судебных и коммерческих утилит производят создания образов в данных форматах. Это свойство программы может также использоваться, чтобы исследовать файлы образов, созданных такими программными продуктами, как Safeback, Encase. ILook позволяет исследовать ISO - и CIF - образы компактдисков, виртуальные диски VMWare.

lLook инструмент, использоваться только который должен теми которые прошли соответствующее обучение исследователями, имеют определенную квалификацию в области судебного восстановления данных. Это не инструмент, который может использоваться неопытными пользователями в области судебной экспертизы на любом уровне. Без соответствующих знаний и квалификации, результаты, полученные при использовании Ilook для анализа цифровых данных, могут быть ненадежны так как не могут быть, в дальнейшем, подвергнуты проверке.

ILook использует базу данных Hashkeeper, разработанную и поддержанную Brian Deering и U.S. DOJ National Drug Intelligence Center. Кроме того, также поддерживаются базы данных хэшей от рабочей группы NIST NSRL. Пользователь может использовать любые базы данных хэшей, имеющие форму, которая выполняет критерии проекта ILook.

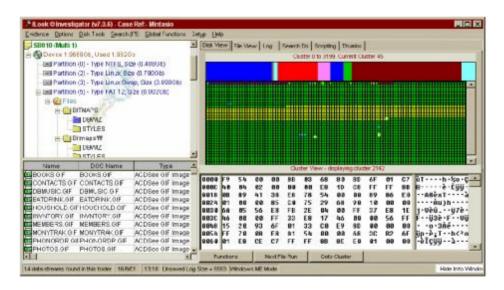


Рис.1.Рабочее окно программы ILook Investigator.

Oved	Location	Printer a Found	Type	Stre	Office of fact.	Ader	Correct	Last cores
Prod Social	•••••	F100/Ep000	South	512				
Tree Sector		Tree Space	Sector	512				
District Society		District Speece	Sector	512				
hused Sector Drawed Social		Inused Space	Renthre Skripton	512 512				
hused Sector		Introd Space	Sector	512		_		
James Scote		Annothing to	sketor	512				
hused Sector		Inused Space	Sector	512				
Drawed Society		District Speece	Soutur	512				
Unused Sector		Unused Space	Sector	512				
Unused Sector		Unused Space	Sector	512				
VARIOUS 10	MMLSOCATE NEED	le Data	Applications	191333			021.5 99 55 400.	020.569
VM MODZELL G	SINLEGOTO SOC	le Data	Application.	294733			021.569 55 400.5	021.599
YAMUUL 10	954.50°(T) 50°C	le Data	Applications	494333			021.599 55 400.	021.599
JOURNAMPER THA	MPLES/SCEVEN.	le Data	Vici eset.	101072			02139933400	27.169
290,8W RLT	VILLE.	le Data	AWC le 1	135233			021299324003	021,599.11
PART MARK DULL TALA	TORSC	le Data	Application (100424			021.599 55 407 .	021.569
_2159/1PC1 08	LATORIA	le Data	7.0 le	J24J93			020399334614	021.569
אַבּצו בעיעאמיו בעניבן[MLES.	le L'ata	Vici discreti	120000			021.599 55 4431.	27.169
SOUTHOUT DE LISAN	MLES.	le L'ata	lei> le .	247573			021.599 55 4431.	021.569
]ตหวนจระของ - เรษต	MLS:	le L'ata	Vici discreti:	3 JJ13J			021.599 55 440.0	27.1599
∳rkatouu, LP – tSAki	MLS:	le Data	lei> le	49100			021.599 55 440.0	021.599
ן בטעעטיזואין	AMPLESC	le Data	Viciosoft 1	154324			021.599 55 440.5	27.1699
TRYAGGII IM SAM	MLES:	le Data	1.64	3331			021.599 55 440.5	27.199
EXAMPLE OF THE		le Data	TLU le :	504704			UZ1.599 55 4044	021.599
ARCILLAR 1 C		(x)) ne bata	Application:	559950			021399334004	021.599
4°EERUAW 1		le Data	AWC 16	105203			021399334003	021,599.11
[<u></u>					***			

Рис.2. Окно опции: Search Result.

ILook обеспечивает следующие особенности:

- 1. Идентификация и поддержка следующих файловых систем и их вариантов:
- o FAT12;
- o FAT16,
- o FAT32.
- o FAT32x,
- o VFAT,
- o NTFS 4.
- o NTFS 5,
- о Сжатая NTFS 4,
- о Сжатая NTFS 5.
- o Mac HFS.
- o Mac HFS +.
- o Linux Ext2FS,
- o Linux Ext3FS- журналируемый вариант Ext2FS,
- o SCO Sys V AFS.
- o SCO Sys V EAFS,
- o SCO Sys V HTFS,
- o CDFS.
- o Novell Netware NWFS.
- 2. Интерфейс, аналогичный Explorer, позволяет исследователю просматривать и осуществлять навигацию по исследуемой файловой системе, как это было бы при проведении анализа на подозреваемом компьютере.
- 3. Встроенные средства позволяют извлечь все данные или часть файловой системы из исследуемого образа.
- 4. Механизм поиска может функционировать в трех режимах: стандартный, расширенный, режим индексации данных.
- 5. Имеет автономные программы поиска и индексации данных.
- 6. Имеет встроенный перекодировщик текстов.
- 7. Использует заголовки файлов для определения технологии их просмотра исследователем.
- 8. Имеет встроенный просмотрщик мультиформатных файлов.

- 9. Поддержка длинных имен файлов.
- 10. Автоматическая массовая обработка образов.
- 11. Автоматическая массовая обработка мультиобразов (образов, разделенных на части) и извлечения данных.
- 12. Имеет программы генерации словарей для подбора пароля и ключевого слова.
- 13. Имеет встроенный hex-редактор со средствами поиска.
- 14. Имеет средства восстановления удаленных файлов.
- 15. Осуществляет рутинную проверку сигнатур файлов.
- 16. Восстанавливает FAT директории.
- 17. Поддерживает хэш-анализ по алгоритмам CRC32, MD5 и SHA1.
- 18. Генерирует значения контрольных сумм для образов и данных, находящихся на диске, по алгоритмам CRC32, MD5 и SHA1.
- 19. Маркирует исследованные файлы и документирует произведенные действия.
- 20. Управление процессом исследования таково, что делает понятным проведение каждого его шага.
- 21. Имеет инструменты для исследования данных Интернет кэша и почтовой программы (с функцией восстановления и документации произведенных действий).
- 22. Декодирует сообщения электронной почты имеющие форматы UUE и Base64.
- 23. Может обеспечивать доступ к данным исследуемого носителя в обход средств BIOS.
- 24. Создание образа осуществляется через BIOS средствами, имеющими механизмы проверки подлинности по алгоритмам MD5 / SHA1 и сжатия создаваемого образа.
- 25. Производит фильтрование файлов по разным признакам.
- 26. Производит одновременный глобальный поиск.
- 27. База данных результатов поиска содержит результаты всех осуществленных поисков в рамках проводимого исследования.
- 28. Просмотр карты раздела позволяет детально просмотреть физическое расположение любого выбранного тома.
- 29. Имеет встроенный script-язык, его компилятор и отладчик.
- 30. Сортирует файлы по виртуальным папкам.
- 31. Имеет интегрированный многофункциональный просмотрщик.

Используемая литература:

1.ILook Investigator v.7.016. Help Manual

Благодарим:

Dmitry, за помощь, оказанную в написании статьи.