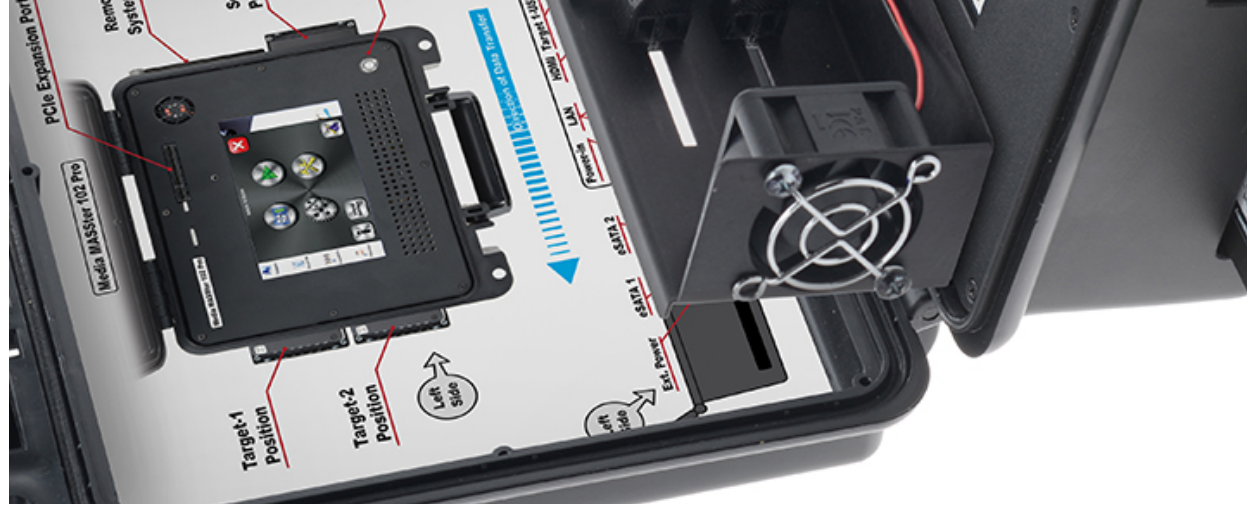




Криминалистика как бизнес процесс компаний

Ильяс Киреев





Компьютерная криминалистика



Источник: <https://ics-ic.com/media-master-102-pro-forensic/>



Криминалистика

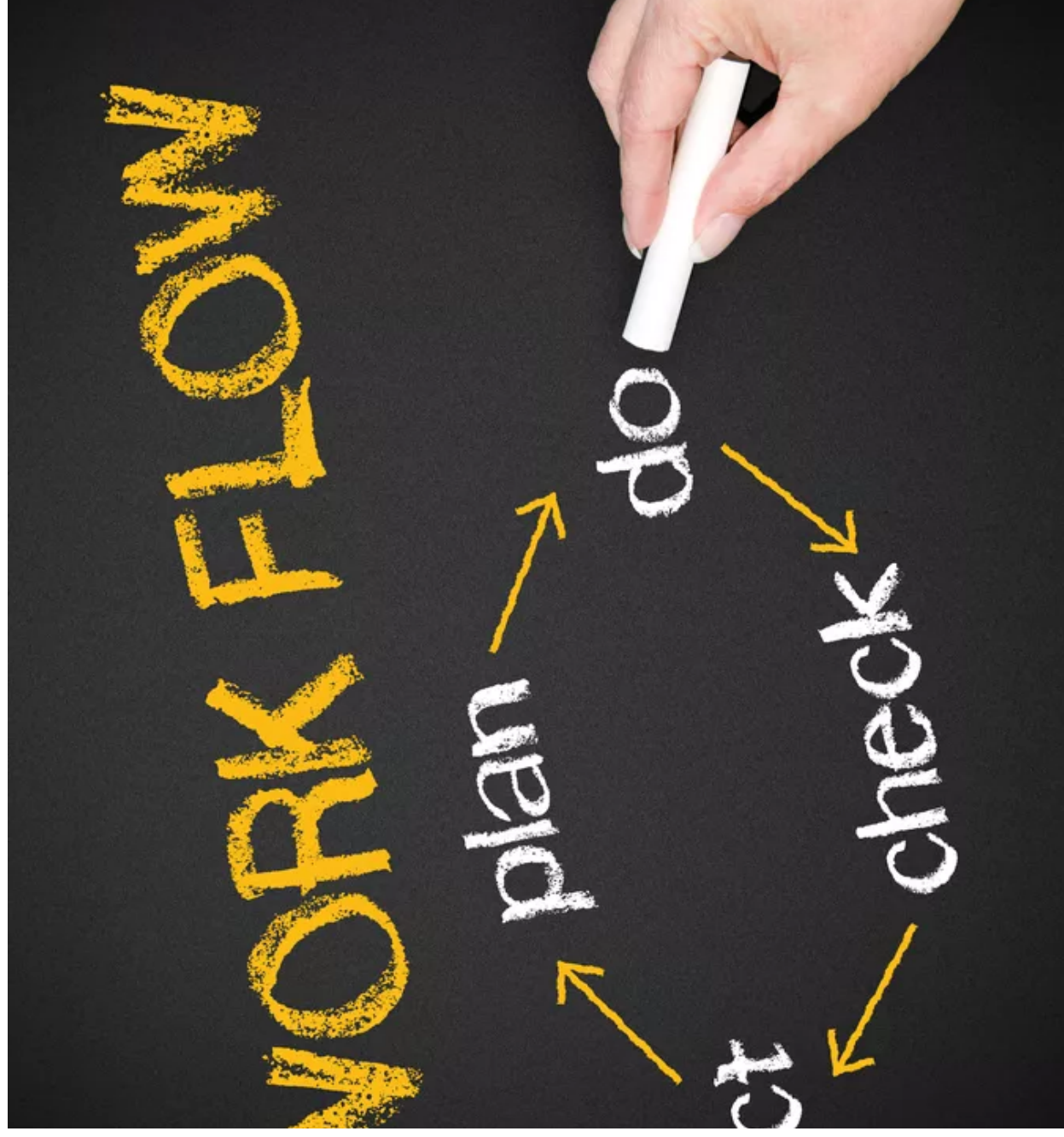
Классификация

- Computer forensics
- Network forensics
- Forensic data analysis
- Mobile device forensics
- Hardware forensic





Инцидент менеджмент



Выявление



- Активы
- События ИБ
- Инциденты ИБ
- Анализ
- Классификация

Реагирование



- Ответственные
- ГРИБ
- Контроль

Расследование



- Источники
- Причины
- Следствие

Пост анализ



- Первичный сбор
- Анализ цифровых улик
- Создание отчетов



Пост анализ

Детальные компьютерные
расследования инцидентов
информационной
безопасности





Процессы

- Сбор
- Анализ
- Рассмотрение
- Управление

Пост анализ

Кто работает в процессе?

• Служба ИБ

• Служба ИТ

• Эксперты-криминалисты





Скачать бесплатно

<https://accessdata.com/product-download/ftk-imager-version-4-3-0>



Size	Type
0	Folder (Placeh...
1	Directory
0	Unallocated Sp...
1	Filesystem Met...
4	Filesystem Slack

0-20	20	00	02	08	00	00	eR.NT
0-3F	00	FF	00	00	20	12	00
0-FF	D7	6D	0C	00	00	00	00
0-02	00	00	00	00	00	00	00
0-3A	21	6A	CA	62	6A	CA	B4
2-D0	BC	00	7C	FB	68	C0	07
3-0E	00	66	81	3E	03	00	4E
3-AA	55	CD	13	72	0C	81	FB
0-75	03	E9	DD	00	1E	83	EC
3-0E	00	8B	F4	16	1F	CD	13
2-E1	3B	06	0B	00	75	DB	A3
2-5A	33	DB	B9	00	20	2B	C8
F-00	8E	C2	FF	06	16	00	E8
0-BB	CD	1A	66	23	C0	75	2D
3-24	81	F9	02	01	72	1E	16



Централизованный удаленный сбор

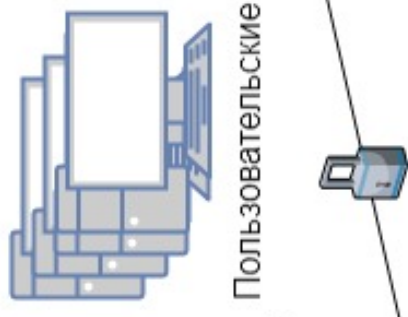
ost Case: remote project

Status

06.08.2018 17:...	06.08.2018 17:...
06.08.2018 17:...	06.08.2018 17:...
06.08.2018 17:...	06.08.2018 17:...
23.04.2018 21:...	23.04.2018 21:...
23.04.2018 21:...	23.04.2018 21:...
15.11.2018 4:5...	15.11.2018 4:5...
22.08.2013 19:...	22.08.2013 19:...
15.11.2018 4:5...	15.11.2018 4:5...
25.04.2018 4:5...	25.04.2018 4:5...

Act Go

Объекты сбора и анализа





CROSSTECH
SOLUTIONS GROUP

- почтовые сервера
- базы данных
- файловые хранилища
- криминалистический образ

eDiscovery



Threat Hunting

Деконпозиция по хешам

C2 хакерской группировки.

портфолио группировки

хеш суммы пораженных файлов



IOCs

MD5	SHA-1	SHA-256
SkinnyD		
ec2377cbd3065b4d751a791a22bd302c	cdd78ccd274705f6c94b6640c968e90972597865	1d59968304
3ff50f9ea582848b8a5db05c88f526e	ea11d0d950481676282cee20c5eb24fc71878bcc	b5227a1218
55186de70b2d5587625749a12df8b607	858d866c5faa965fa9fbe41c8484a88fe0c612eb	d81ba465fe!
Бэқдор xDII		
9f01cb61f342f599a013c3e19d359ab4	b63bfdfb7f267e9fbf1c19be65093d857696f3b0	169c24f0ad!
a2d552ed07ad15427f36d23da0f3a5d3	1858a80c8cff38d7871286a437c502233e027ab0	59759bbdfc!
60ddb540da1ae1ee1e14f12578eafda8	8d16bc28cef6760ecf69543a14d29ba041307957	87a57f5bb9!
7a4c8e876af7d30206b851c01dbda734	4cff1af90c69cc123ecafe8081e3c486a890d500	06d20fb589!
3d760b6fc84571c928bed835863fc302	adc9ade7a4dc14b7bf656e86ea15766b843e3b6	8ac21275d0

Добавление кейса и задачи на сканирование шары по хешу

Поиск по индексу целевого хеша и название файла

Добавление списка хешей ЮС в формате CSV

Настройка профиля KFF

Настройка планировщика задач поиска

eDiscovery processing

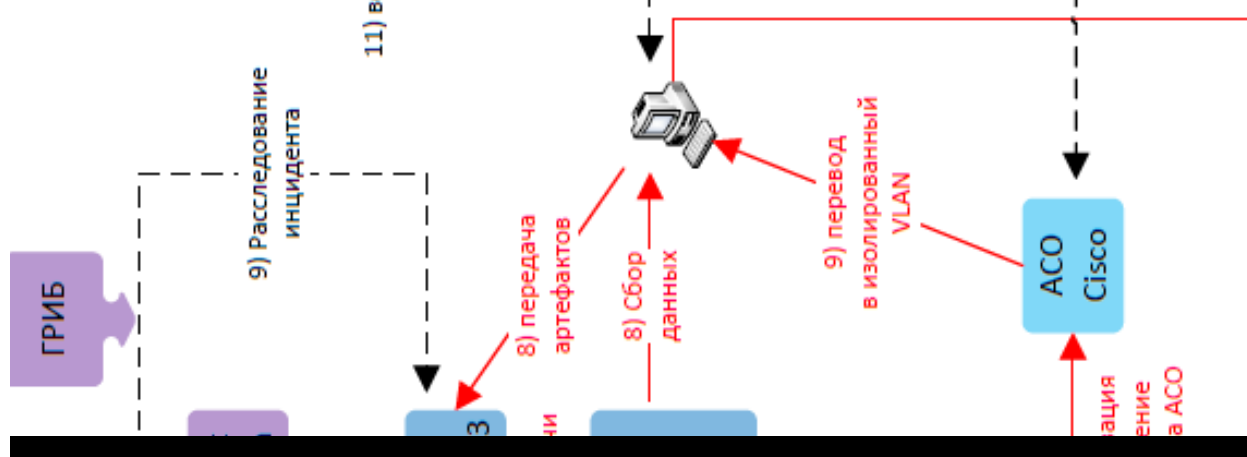
Вирусное заражение

```
ue]local.config = (245, 23, 068, 789
  name <img> = s
  # input.new(c
  # [statu
  # scri
  # kmo
  ction logged: #
  ction logged: #
  wn} m#4:80a?:
  ue]local.config
  fg#6 mn4:h6110
  tatus?] code <
  ript_src = [error]
  wn} m#4:80a?:/ status. omm
  ue]local.conf
  put false fun
  ials {logged:
  src = address
  ess:denial //
  [true] {?unk
  ction logged: #
  ction logged: #
  ction logged: # inp .[tru
  # /q.s statu
  # (245, 23, 6 8
  # name<i g> s
  # #status (m
  # #malicious code k
  # #status: commi
  ue]local.config = (245, 23, 068, 789
```




Автоматизация инцидент менеджмента

- Улучшает реакцию команды SOC **до 40 минут**
- Исключает ошибки человека
- Автоматизирует сбор цифровых артефактов
- Изоляция хоста на стадии закрепления
- Интеграция с IT платформами





Вопросы?

