Cross Technologies

Людмила Кошелева,
Менеджер по развитию


HOW TO CATCH THE BAD GUY:
1. Collect tons of data
2. Sort all the data
3. Analyze every last word
4. Find time to catch the bad guy

Предпосылки

Глобальная цифровизация, растущие объемы данных, множество форматов:

1996 – 10 MB

1999 – IBM the Microdrive 170 MB и 340 MB

2002 – 137 GB addressing space barrier broken

2005 – 500 GB hard drive

2007 – 1 terabyte hard drive

2009 – 2 terabyte hard drive

2011 – 4 terabyte hard drive

2013 – 5 terabyte hard drive

2015 – 10 terabyte hard drive

2018 - 16TB Samsung, 60 terabyte SSD Seagate

Предпосылки

Нехватка персонала и обучение персонала

Задержки по разбору инцидентов, криминалистическому анализу

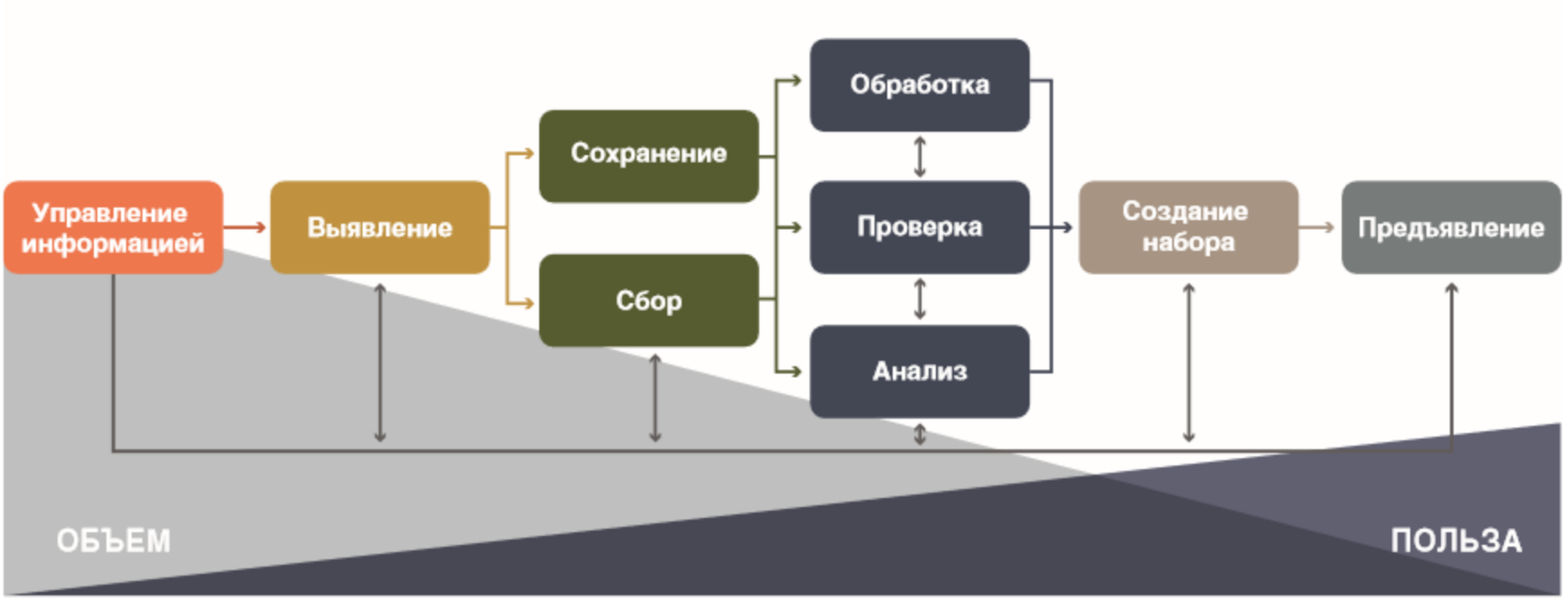
Необходимость оптимизации работы экспертов

Принципы сбора доказательств (уголовные дела)

ACPO – Association of Chief Police Officers – 4 принципа:

1. Любое действие не должно изменять собираемую с электронных носителей информации (целостность)
2. Если необходимо обеспечить доступ к ESI, то специалист должен быть компетентным для сбора релевантных доказательств
3. Процесс сбора данных должен быть зафиксирован, чтобы третья сторона могла его повторить с получением того же результата (воспроизводимость, повторяемость, протоколирование связаны с п.1)
4. Соответствие (непротиворечивость) первых трех принципов законодательным актам.

Принципы сбора доказательств (EDRM)



Документальная база

- ГОСТ 27037-2014 (Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме)
- «eDiscovery in digital forensic investigations» (Centre for Applied Science and Technology)

Подход AccessData

AD Enterprise

Расследования в сети
и пост-анализ инцидентов

- Корпоративные расследования
- Предварительный просмотр данных в конечной точке в реальном времени
- Анализ оперативной памяти
- Агентская инфраструктура
- Удаленная работа, скрытые расследования
- Восстановление удаленных файлов и т.д.

AD eDiscovery®

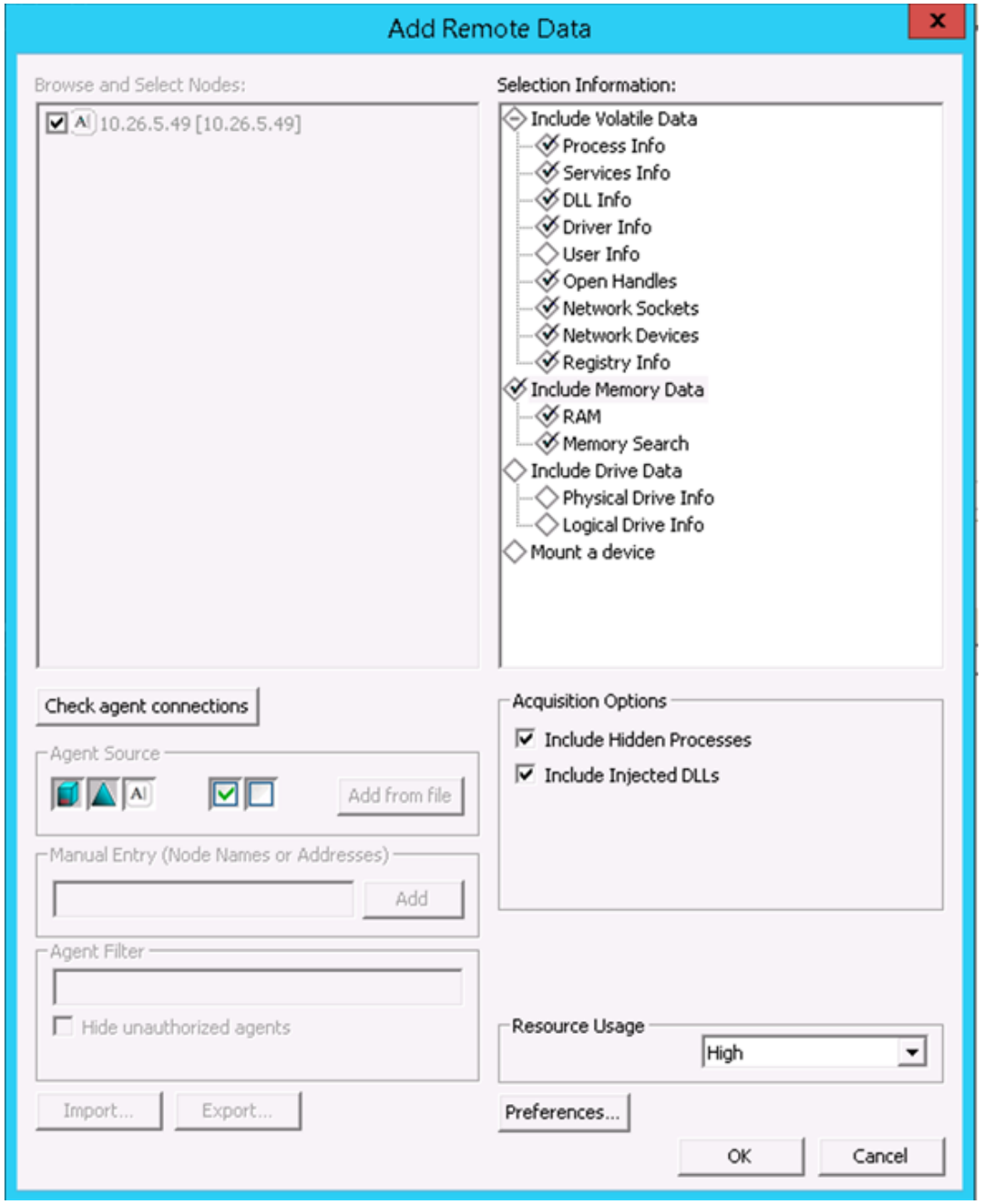
Регулярный защищенный
сбор данных

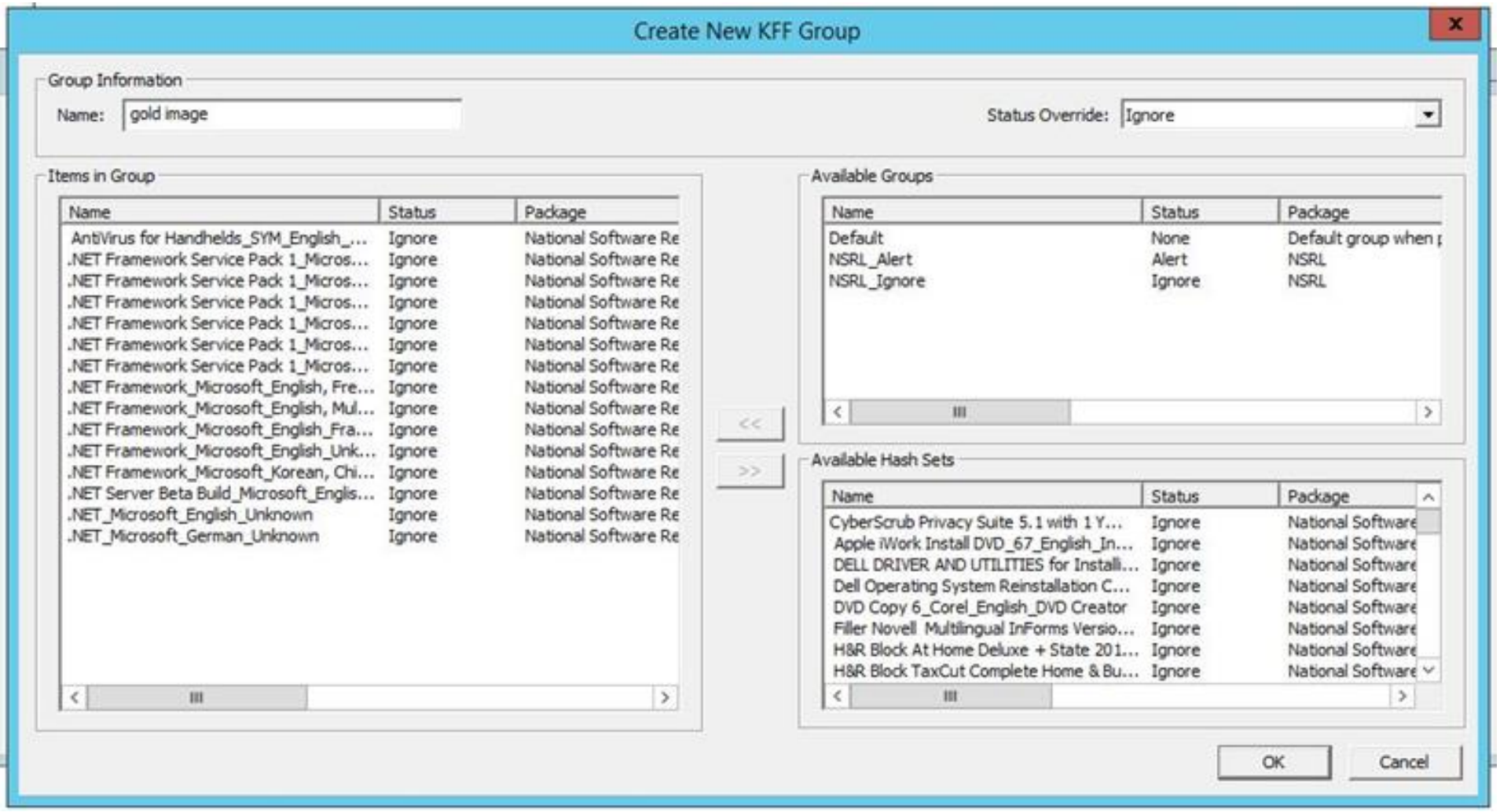
- Крупномасштабные расследования
- Сбор данных через коннекторы к наиболее используемым хранилищам
- Встраивание в EDRM
- Визуализация и аналитика для интерпретации данных

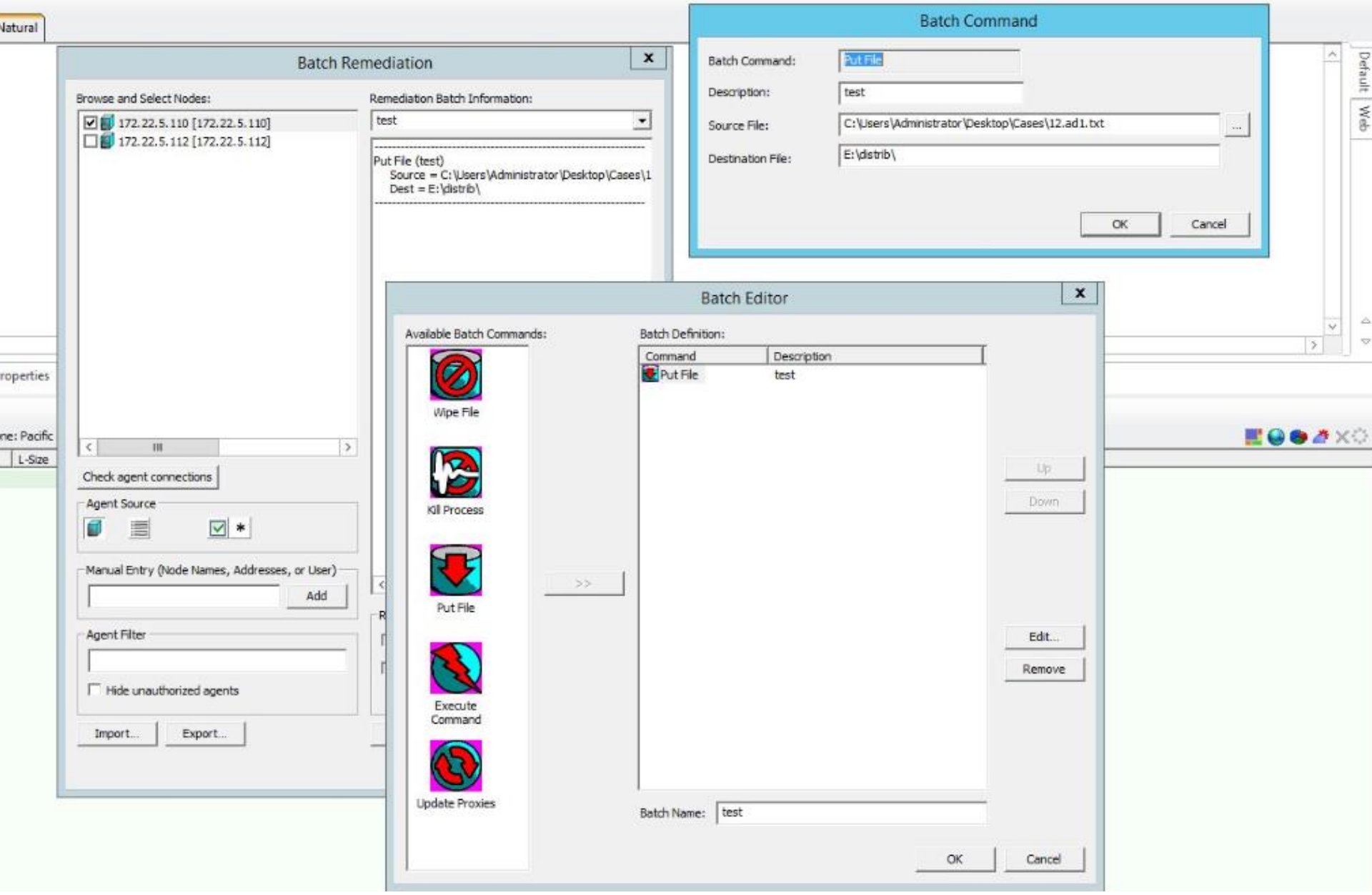
AD Lab

Крупномаштабные
расследования

- Расследования криминалистических лабораторий
- Распределение рабочей нагрузки в рамках единой масштабируемой среды (ролевая модель)
- Обработка и хранение данных, в том числе в облаке AWS
- Интеграция с Belkasoft для мобильных платформ


Add Remote Data
Browse and Select Nodes:
10.26.5.49 [10.26.5.49]
Selection Information:
Include Volatile Data
Process Info
Services Info
DLL Info
Driver Info
User Info
Open Handles
Network Sockets
Network Devices
Registry Info
Include Memory Data
RAM
Memory Search
Include Drive Data
Physical Drive Info
Logical Drive Info
Mount a device
Check agent connections
Agent Source
Add from file
Manual Entry (Node Names or Addresses)
Add
Agent Filter
Hide unauthorized agents
Import...
Export...
Acquisition Options
Include Hidden Processes
Include Injected DLLs
Resource Usage
High
Preferences...
OK
Cancel


Create New KFF Group
Group Information
Name:
gold image
Status Override:
Ignore
Items in Group
Name
Status
Package
AntiVirus for Handhelds_SYM_English_...
Ignore
National Software Re
.NET Framework Service Pack 1_Micros...
.NET Framework Service Pack 1_Micros...
.NET Framework Service Pack 1_Micros...
.NET Framework Service Pack 1_Micros...
.NET Framework Service Pack 1_Micros...
.NET Framework_Microsoft_English, Fre...
.NET Framework_Microsoft_English, Mul...
.NET Framework_Microsoft_English_Fra...
.NET Framework_Microsoft_English_Unk...
.NET Framework_Microsoft_Korean, Chi...
.NET Server Beta Build_Microsoft_Englis...
.NET_Microsoft_English_Unknown
.NET_Microsoft_German_Unknown
<<
>>
Available Groups
Name
Status
Package
Default
None
Default group when
NSRL_Alert
Alert
NSRL
NSRL_Ignore
Ignore
NSRL
Available Hash Sets
Name
Status
Package
CyberScrub Privacy Suite 5.1 with 1 Y...
Apple iWork Install DVD_67_English_In...
DELL DRIVER AND UTILITIES for Installi...
Dell Operating System Reinstallation C...
DVD Copy 6_Corel_English_DVD Creator
Filler Novell Multilingual InForms Versio...
H&R Block At Home Deluxe + State 201...
H&R Block TaxCut Complete Home & Bu...
National Software
OK
Cancel


Batch Remediation
Browse and Select Nodes:
172.22.5.110 [172.22.5.110]
172.22.5.112 [172.22.5.112]
Remediation Batch Information:
test
Put File (test)
Source = C:\Users\Administrator\Desktop\Cases\1
Dest = E:\distrib\
Check agent connections
Agent Source
Manual Entry (Node Names, Addresses, or User)
Add
Agent Filter
Hide unauthorized agents
Import...
Export...
Batch Command
Batch Command:
Put File
Description:
test
Source File:
C:\Users\Administrator\Desktop\Cases\12.ad1.txt
Destination File:
E:\distrib\
OK
Cancel
Batch Editor
Available Batch Commands:
Wipe File
Kill Process
Put File
Execute Command
Update Proxies
>>
Batch Definition:
Command
Description
Put File
test
Up
Down
Edit...
Remove
Batch Name:
test
OK
Cancel

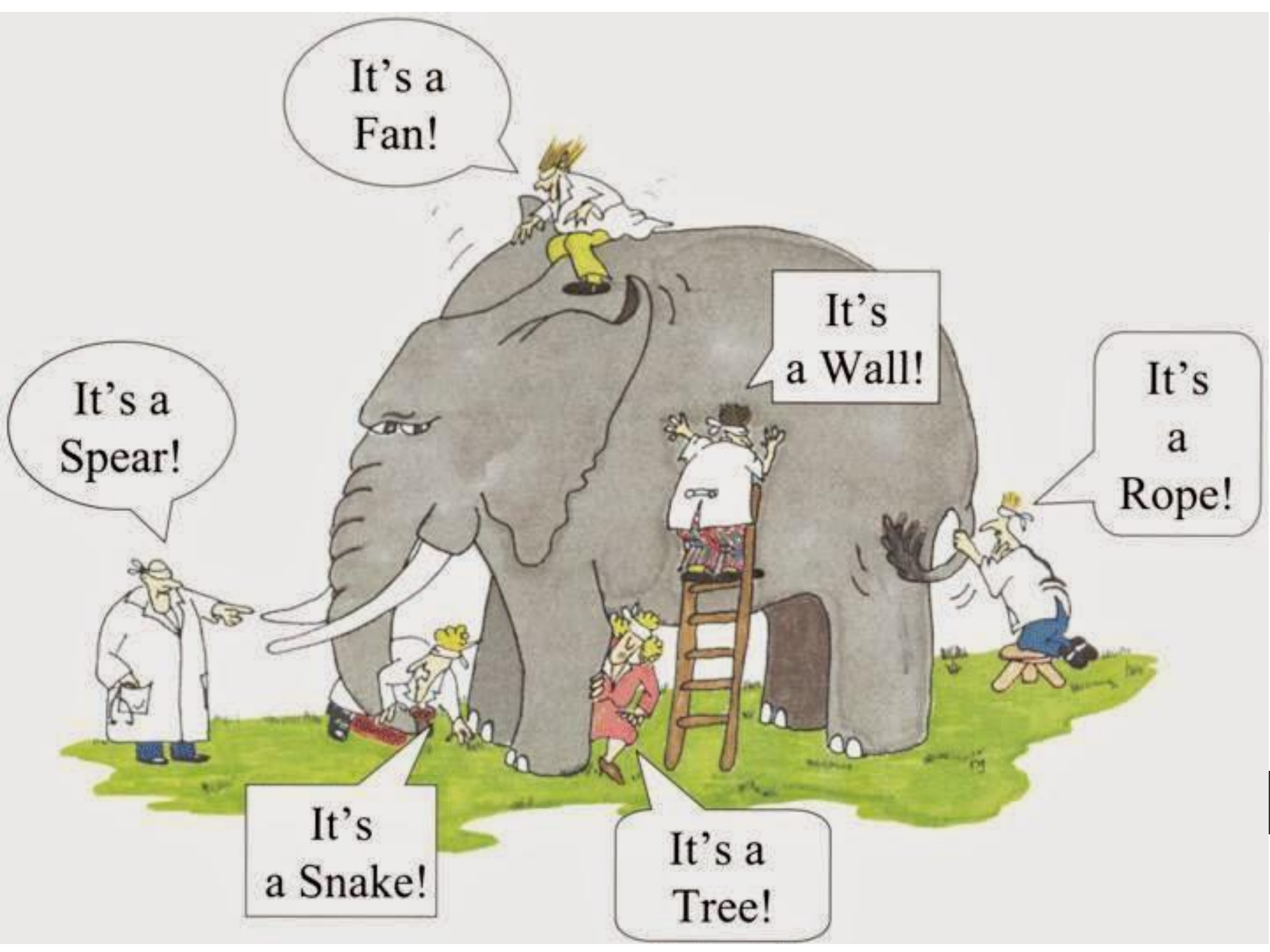
Best practice

- Автоматизация процесса сбора данных – скорость сбора, корректность, отсутствие зависимости от квалификации IT-специалиста
- Унификация форматов и процессов сбора, хранения и обработки данных
- Подтвержденная целостность собранных данных (включая трекинг процесса сбора)
- Придание юридической значимости собранным доказательствам
- Использование следственными органами инструментов, которые работают с форматами AD1, EO1

Что дает AD?

Never touch your data again!

- Отсутствие влияния на бизнес-процессы (удаленный сбор, разделение задач: безопасности свое – аналитикам и юристам свое)
- Снижение рисков
- Снижение издержек на сбор и анализ доказательств


It's a Fan!
It's a Spear!
It's a Wall!
It's a Rope!
It's a Snake!
It's a Tree!


ACCESSDATA
Cross Technologies
Благодарим за внимание
Kosheleva.l@crossteh.su