CREDENCE SECURITY
DIGITAL FORENSICS

FORENSIC FUNDAMENTALS
OCTOBER WEBINAR

FASTER, COLLABORATIVE & HOLLISTIC LAB INVESTIGATIONS

ACCESSDATA

YOUR REGIONAL VALUE-ADD DISTRIBUTOR

ABOUT US

CREDENCE SECURITY

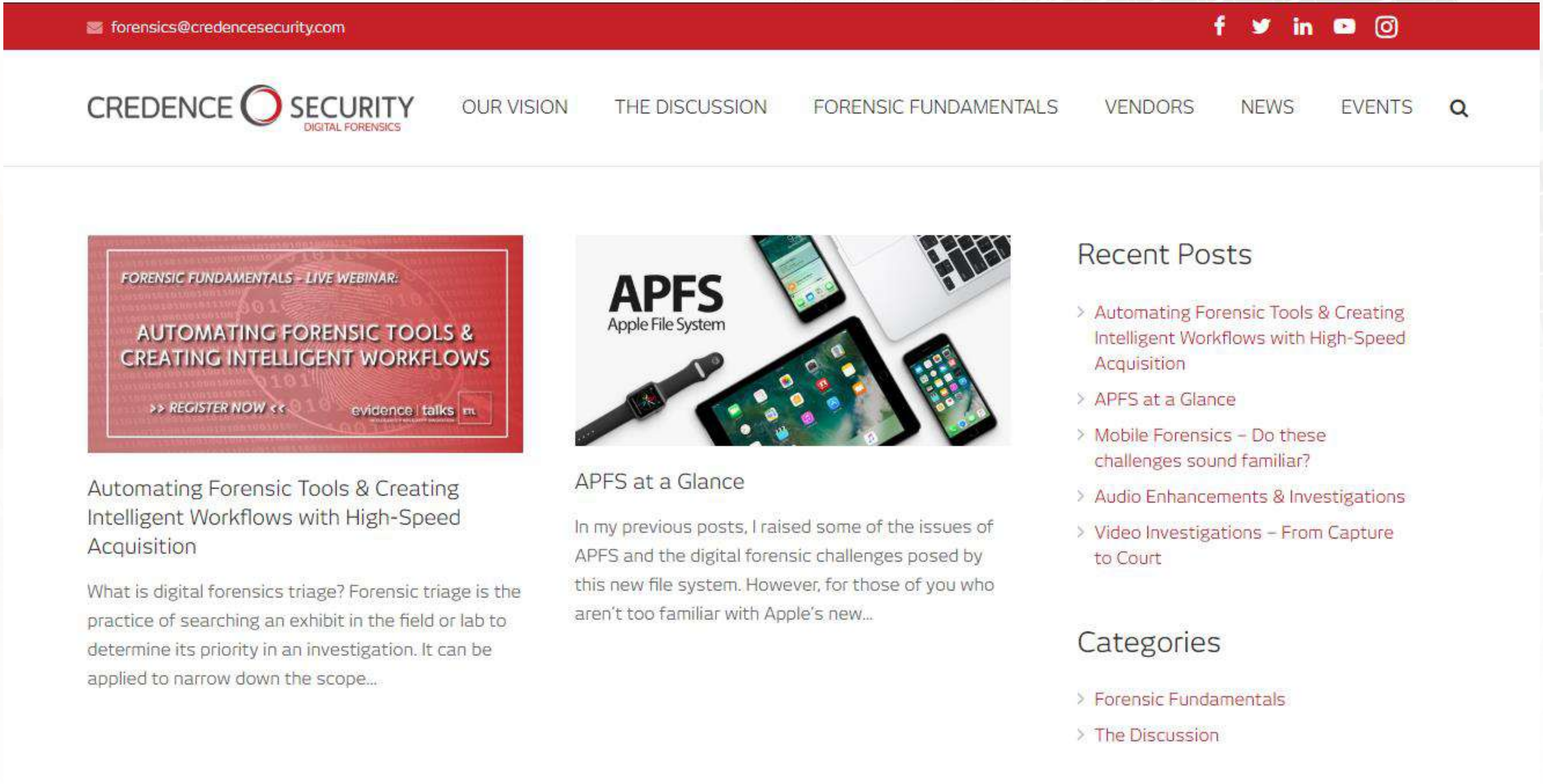
> Established in 1999, Credence Security, a PAN-EMEA specialty distributor, is a leader in cyber security, forensics, governance, risk and compliance. With headquarters in Dubai and regional offices in Johannesburg, Nairobi and London, we are a pure-play provider of security and forensics solutions, to both public and private sector enterprises across Europe, Middle East, Africa and India, through a select network of specialist resellers.

Unlike most other distributors, we take a consultative 'value-add' solution approach – we collaborate with our partners and their customers to understand their needs, both from a technology and business perspective, and then work very closely with our partners to deliver tailor made solutions. As such, our clients rely on us and trust us to deliver best in class IT security solutions that will protect their organizations from some of the most severe and malicious attacks.

With the growing sophistication of threats today, we recognize that leading technologies alone cannot safeguard an organization – organizations need to ensure that they assess risk, comply with latest security regulations and foster a 'security-first' culture.

FORENSIC FUNDAMENTALS

COMMUNITY



FORENSIC FUNDAMENTALS - LIVE WEBINAR:
AUTOMATING FORENSIC TOOLS & CREATING INTELLIGENT WORKFLOWS
>> REGISTER NOW <<
evidence | talks
APFS
Apple File System

forensics@credencesecurity.com

CREDENCE SECURITY DIGITAL FORENSICS

OUR VISION | THE DISCUSSION | FORENSIC FUNDAMENTALS | VENDORS | NEWS | EVENTS

Automating Forensic Tools & Creating Intelligent Workflows with High-Speed Acquisition

What is digital forensics triage? Forensic triage is the practice of searching an exhibit in the field or lab to determine its priority in an investigation. It can be applied to narrow down the scope...

APFS at a Glance

In my previous posts, I raised some of the issues of APFS and the digital forensic challenges posed by this new file system. However, for those of you who aren't too familiar with Apple's new...

Recent Posts

- Automating Forensic Tools & Creating Intelligent Workflows with High-Speed Acquisition
- APFS at a Glance
- Mobile Forensics – Do these challenges sound familiar?
- Audio Enhancements & Investigations
- Video Investigations – From Capture to Court

Categories

- Forensic Fundamentals
- The Discussion

http://forensics.credencesecurity.com

CREDENCE SECURITY

PRESENTER

Harsh Behl

Forensic Consultant

GCIH, GCFE, EnCE, ACE, CCE, NUIX Investigation Specialist

e: harsh.behl@credencesecurity.com

CREDENCE SECURITY

Credence Security, a PAN-EMEA specialty distributor, is a leader in cyber security, forensics, governance, risk and compliance. With headquarters in Dubai and regional offices in Johannesburg, Nairobi and London, we are a pure-play provider of security and forensics solutions, to both public and private sector enterprises across Europe, Middle East, Africa and India, through a select network of specialist resellers.

BACKGROUND

- Digital Forensic Analyst
- Technical Engineer
- Electronics & Communication Engineering Degree

SUPPORTED BY

ACCESSDATA

ACCESSDATA

PRESENTER

Keith Lockhart

Vice President - Strategic Programs

ACCESSDATA

AccessData Group has pioneered digital forensics and litigation support for more than thirty years. Over that time, the company has grown to provide both stand-alone and enterprise-class solutions that can synergistically work together to enable both criminal and civil investigations, including digital forensics, incident response, legal review, compliance, auditing and information assurance.

BACKGROUND

- Bachelor of Arts in Criminology
- 15+ years experience as AccessData VP for Global Training
- 4+ years experience as Computer Crime Specialist
- 4+ years experience as Police Officer
- 15+ years member of International Association of Computer Investigative Specialists Board of Directors

SUPPORTED BY

ACCESSDATA

TODAYS

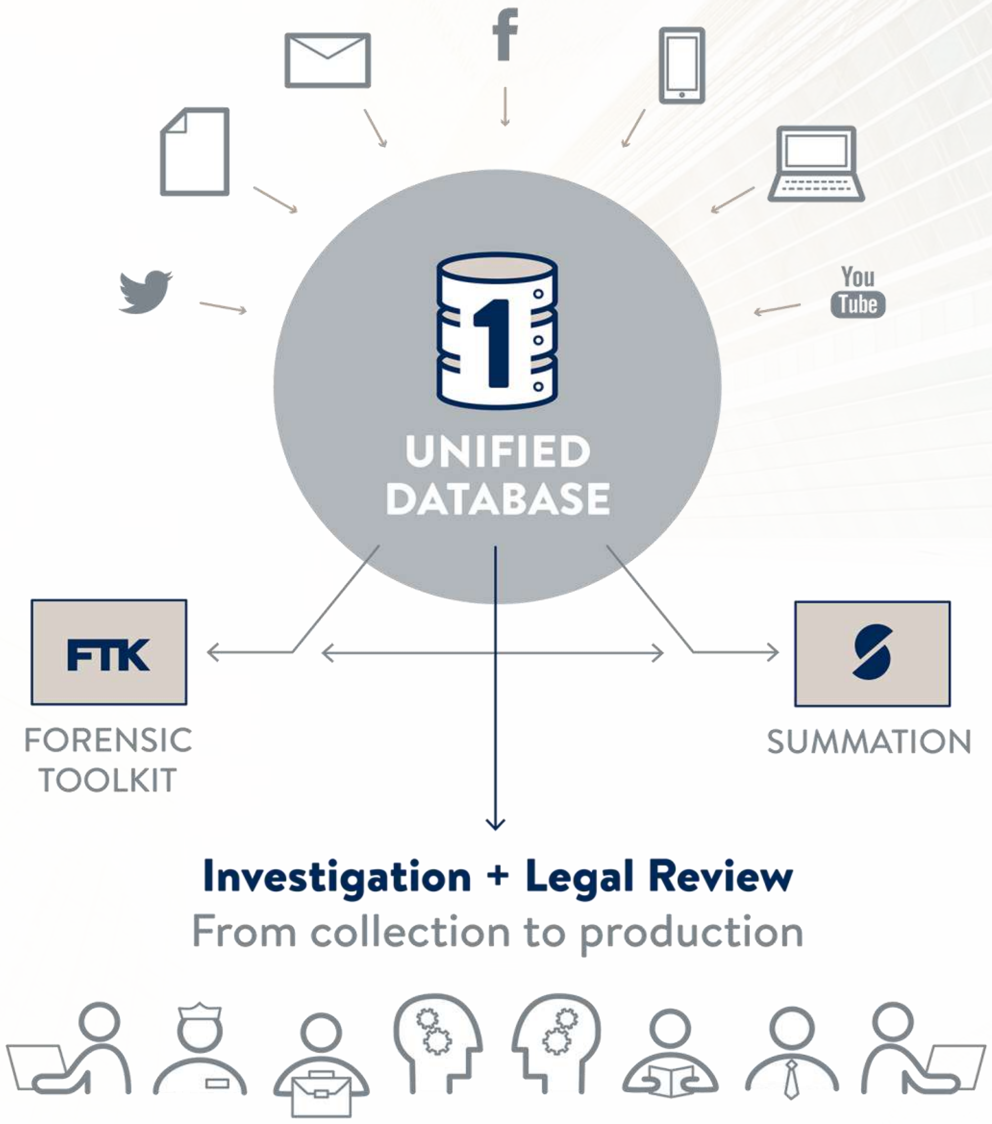
AGENDA

- ✓ What is the problem at hand ?
- ✓ How can we solve that problem with software ?
- ✓ Hardware Collaboration !
- ✓ Human Collaboration !
- ✓ Let us show you… Demonstration
- ✓ Discussion …

SUPPORTED BY

ACCESSDATA

THE ACCESSDATA APPROACH



Investigation + Legal Review

From collection to production

SUPPORTED BY

ACCESSDATA

DISTRIBUTED

DATA PROCESSING

Leaders benefiting from Distributed Data Processing…

elastic   Microsoft Azure   AMAZON EC2 amazon web services   Google App Engine   ACCESSDATA

Distributed data processing is a computer-networking method in which multiple computers across different locations share computer-processing capability.

This is in contrast to a single, centralized server managing and providing processing capability to all connected systems.

Specific jobs are performed by specialized computers.

DDP provides greater scalability.

When you divide a computing function among several machines, you can fine tune each computer to suit the needs of each task.

- ✓ Improved Performance
- ✓ Reduced Processing Time
- ✓ Flexible
- ✓ Reliable
- ✓ Lower Cost
- ✓ Local Data Access

SUPPORTED BY

ACCESSDATA

DISTRIBUTED
DATA PROCESSING

Why Distributed Infrastructure is important… What the industry is saying

WIKIPEDIA
The Free Encyclopedia

There are many cases… use of a distributed system is beneficial for practical reasons. For example, it may **be more cost-efficient** to obtain the **desired level of performance** by using a cluster of several low-end computers, in comparison with a single high-end computer. A distributed system can provide **more reliability** than a non-distributed system, as there is **no single point of failure.** Moreover, a distributed system may be easier to expand and manage than a monolithic uniprocessor system. >>>

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Popular solution for big data processing to **scale and build** on distribution and **combine theoretically unlimited number of machines** in a single distributed storage. Scale out: add more nodes to a system >>>

Techno Security & Digital Forensics Conference

Distributed computing is particularly important for large cases that involve analyzing a group of hard drives. The database manages the project, automatically identifies areas of particularly keen interest (e-mail, encrypted files, items located in the My Documents directory), **and assigns the tasks based on priority**. Distributed data processing architectures **provide forensic labs with the only realistic option of handling large forensic and e-discovery cases** by harnessing the CPU power needed to deal with large data sets. >>>

ORACLE®

Distributed processing environment provides the following benefits… **exploits the multitasking and shared-memory facilities** of its underlying operating system. As a result, it delivers the highest possible degree of concurrency, data integrity, and performance to its client applications. Oracle can be **scaled as your system grows**. You can add multiple servers to distribute the database processing load throughout the network (horizontally scaled), or you can move Oracle to a minicomputer or mainframe, to take advantage of a larger system's performance (vertically scaled). In either case, all data and applications are maintained with little or no modification, since Oracle is portable between systems. >>>

SAP®

Distributed data processing has the following advantages:

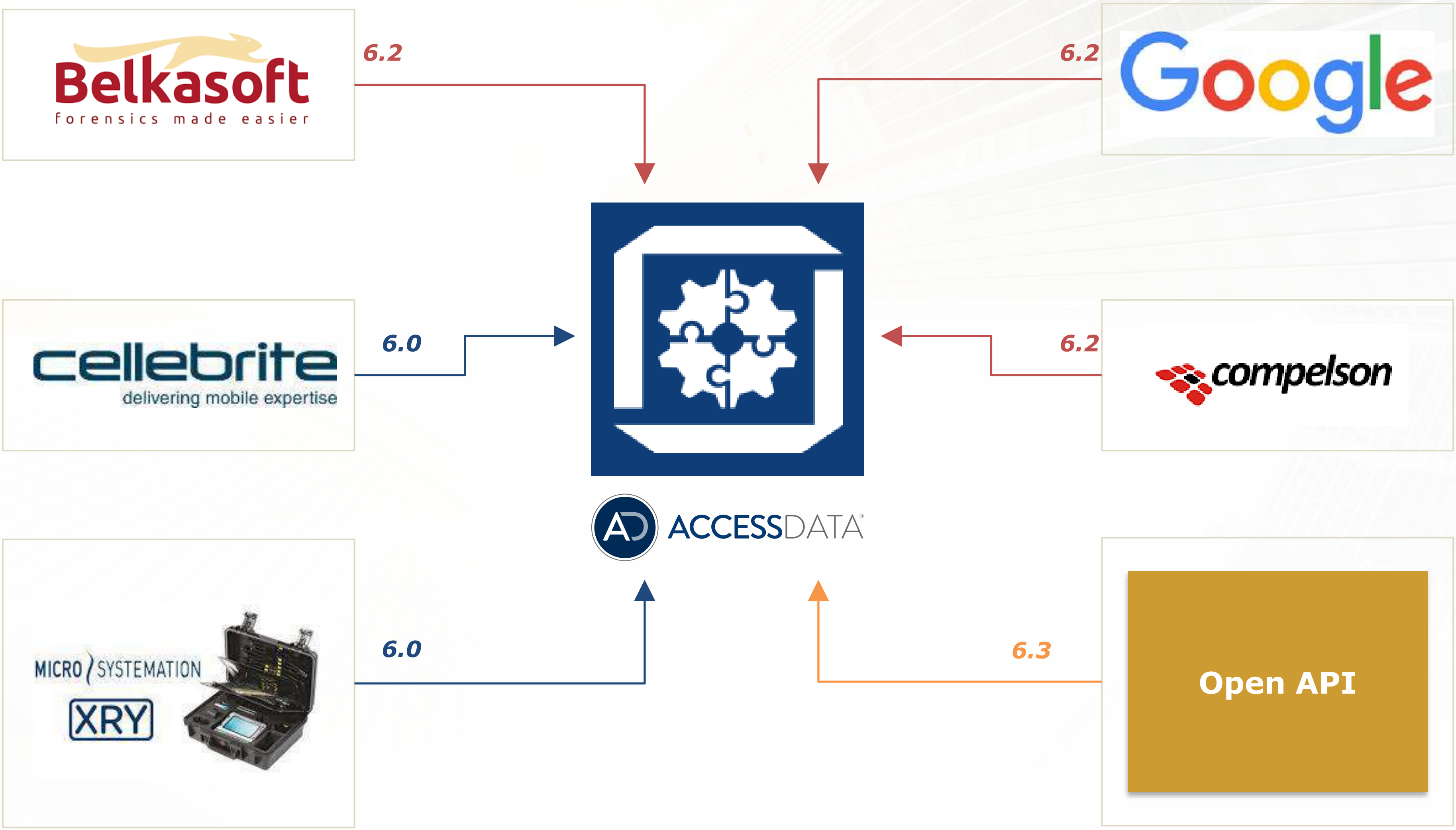
- **Improved performance**
- **Greater security**
- It promotes decentralized company policies, which provides sites with a **high degree of autonomy.** This allows whole areas of responsibility to be assigned to those organizational units at which information - on customers, vendors or goods movements - is usually gathered. >>>

SUPPORTED BY
ACCESSDATA®

ECO-SYSTEM

ENHANCEMENTS

The need for integration in the lab market has become increasingly apparent given the diverse datatypes that must now be supported. AccessData is responding with an open eco-system approach that will allow anyone to integrate seamlessly with AD LAB.



Open API

SUPPORTED BY

ACCESSDATA

ECO-SYSTEM

DETAIL

Belkasoft

forensics made easier

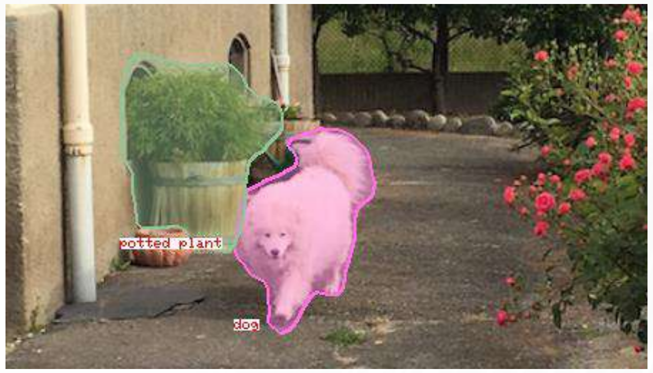
- ✓ Best chat parsing on the market
- ✓ Over 250 parsers
- ✓ Rapid data normalization
- ✓ Parsers include:
  - 155 IM formats
  - 19 Browser formats
  - 13 mail formats
  - 6 CloudFile formats
  - 4 P2P formats
  - 28 MobileApps

compelson

- ✓ Complete phone support (ability to analyze almost every phone on the market)
- ✓ Extensive phone app parsing
- ✓ Phone Support includes:
  - IOS
  - Android
  - Blackberry
  - Windows
  - Motorola
  - Huawei
  - HTC
  - Symbian
  - Nokia
  - Acer
  - Lenovo
  - Samsung
  - Sony
  - LG

Google

- ✓ Image recognition
- ✓ Object identification
- ✓ Picture category tagging

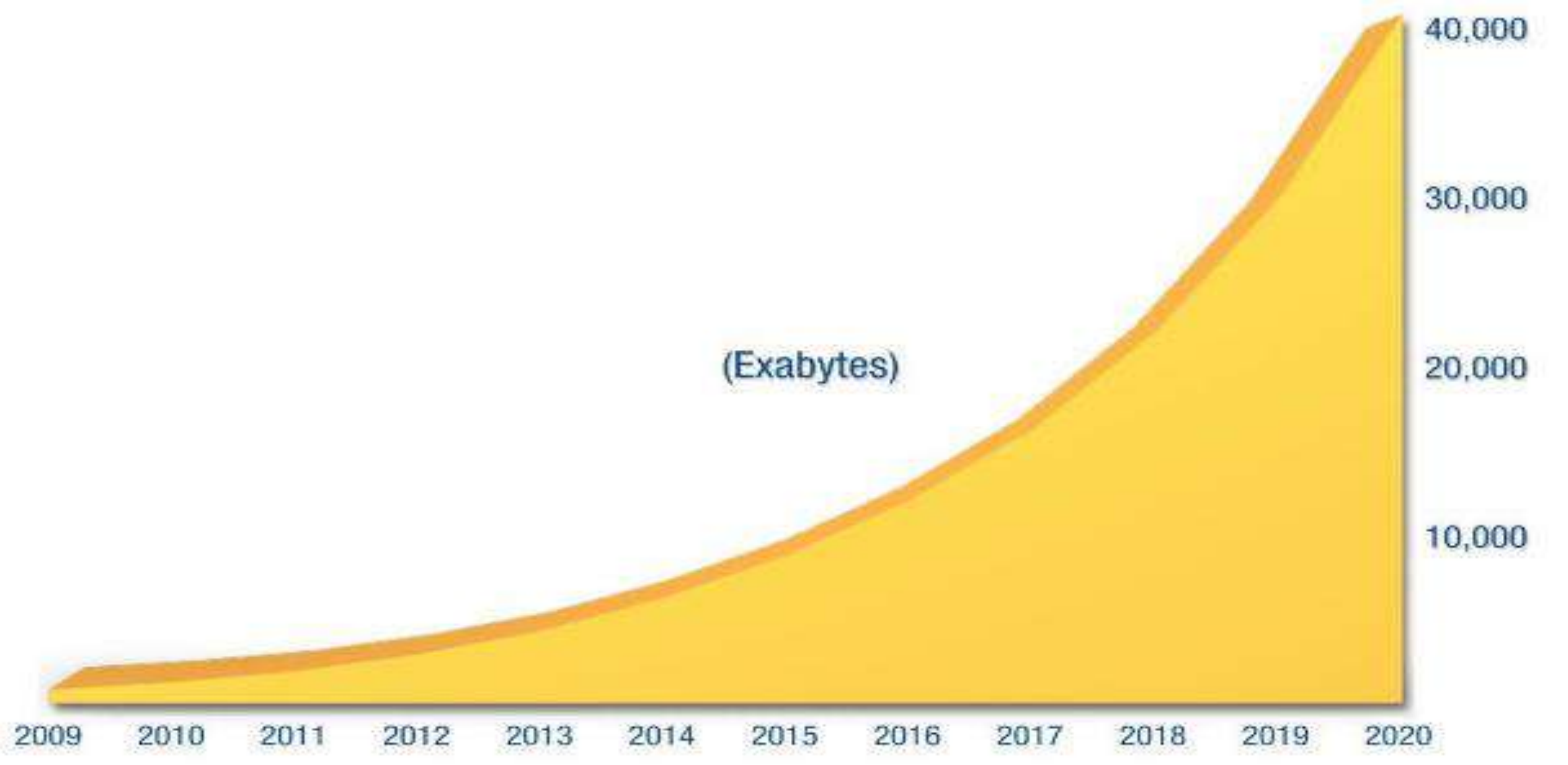


SUPPORTED BY

ACCESSDATA

FASTER

PROCESSING



More machines are better than one!!

✓ FTK (three workers)

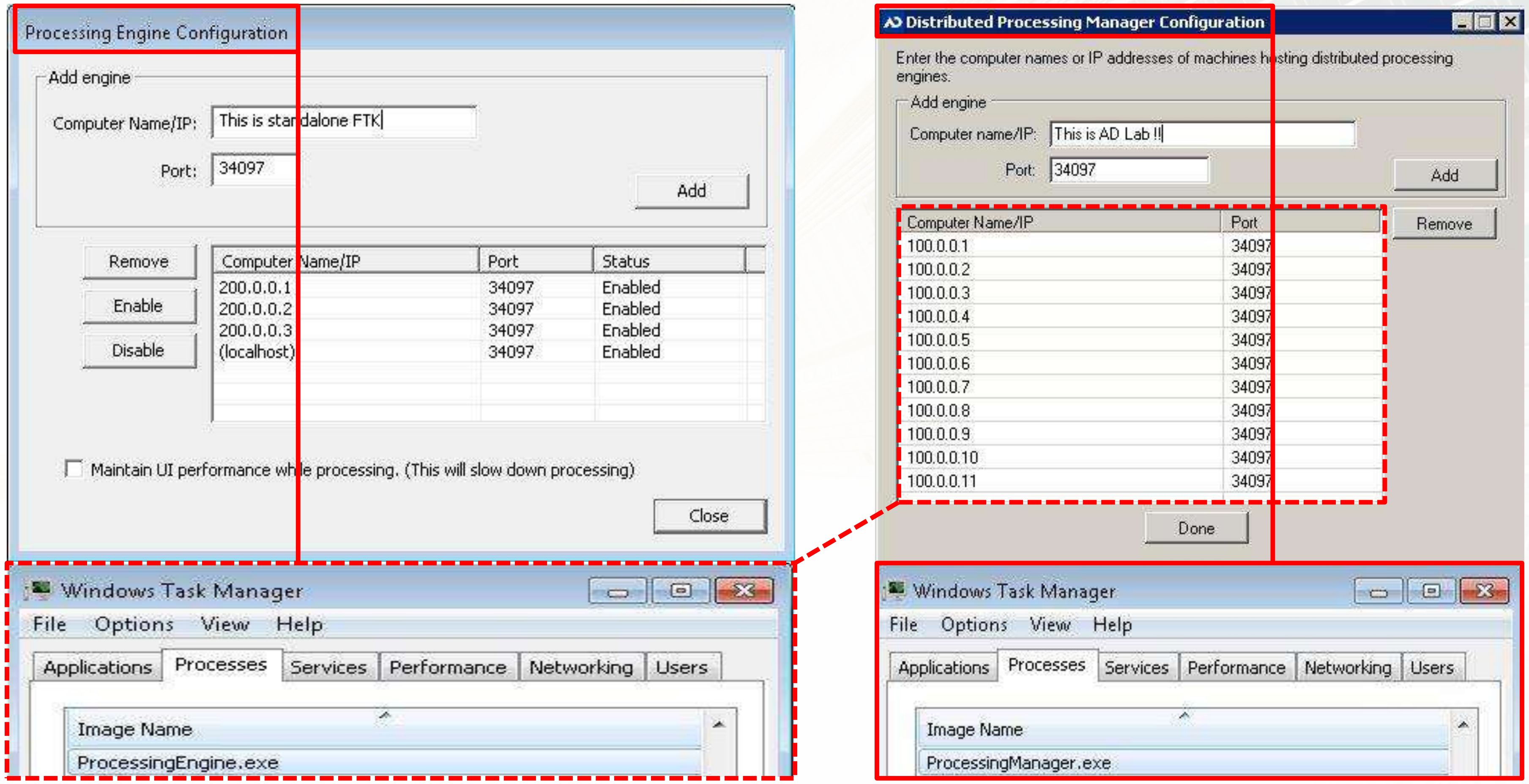
✓ AccessData Lab (managed work clusters)

SUPPORTED BY

ACCESSDATA

FASTER

PROCESSING


Processing Engine Configuration
Add engine
Add
Remove
Enable
Disable
Close
Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
Distributed Processing Manager Configuration
Add engine
Add
Remove
Done

Computer Name/IP: This is standalone FTK
Port: 34097

Computer Name/IP	Port	Status
200.0.0.1	34097	Enabled
200.0.0.2	34097	Enabled
200.0.0.3	34097	Enabled
(localhost)	34097	Enabled

☐ Maintain UI performance while processing. (This will slow down processing)

Image Name
ProcessingEngine.exe

Enter the computer names or IP addresses of machines hosting distributed processing engines.

Computer name/IP: This is AD Lab !!
Port: 34097

Computer Name/IP	Port
100.0.0.1	34097
100.0.0.2	34097
100.0.0.3	34097
100.0.0.4	34097
100.0.0.5	34097
100.0.0.6	34097
100.0.0.7	34097
100.0.0.8	34097
100.0.0.9	34097
100.0.0.10	34097
100.0.0.11	34097

Image Name
ProcessingManager.exe

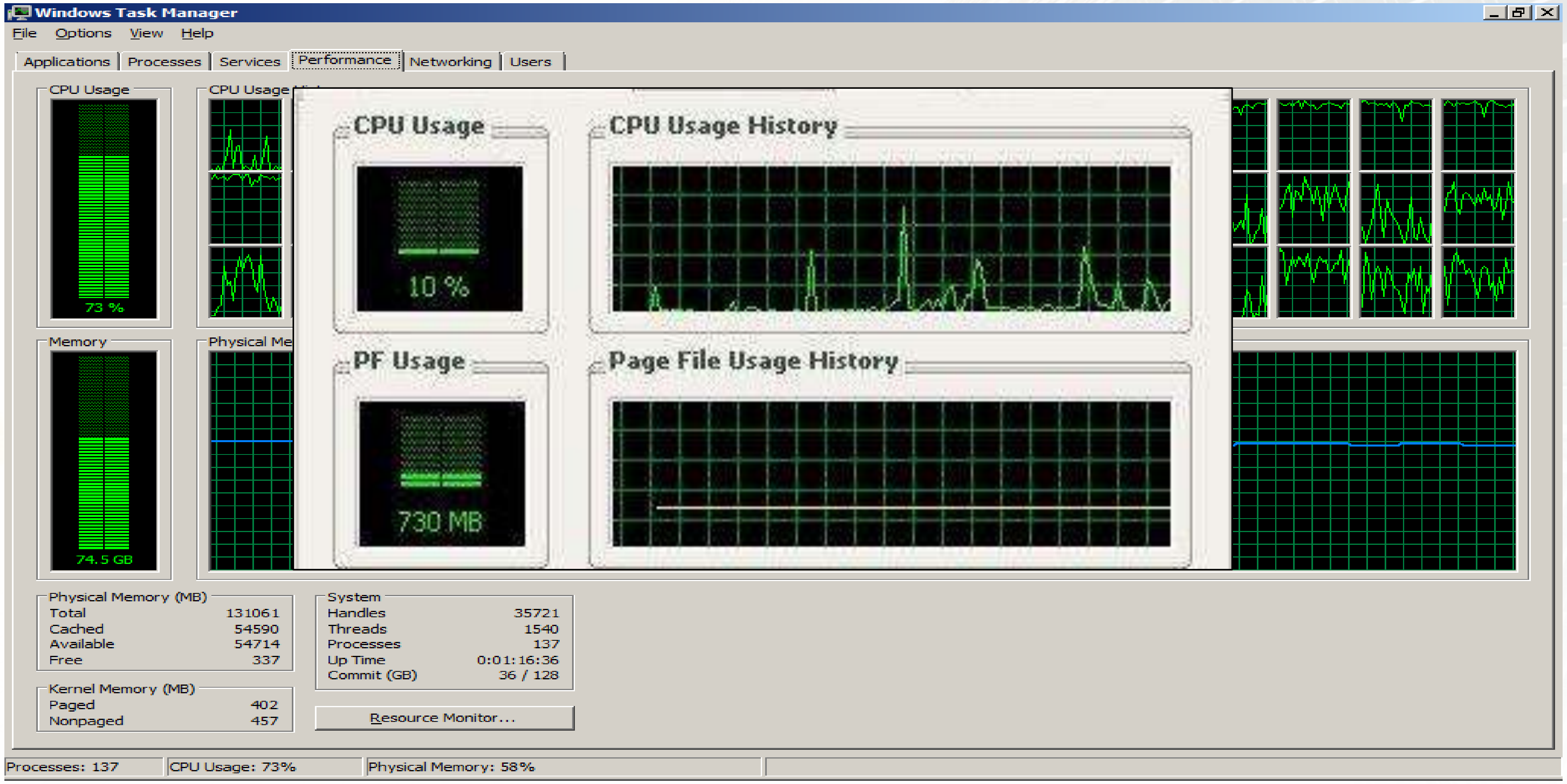
Distributed case processing:

✓ FTK (Forensic Toolkit) (three workers)
✓ AccessData Lab (managed work clusters)

SUPPORTED BY
ACCESSDATA

FASTER

PROCESSING



```
Physical Memory (MB)              System
Total          131061             Handles            35721
Cached          54590             Threads             1540
Available       54714             Processes            137
Free              337             Up Time       0:01:16:36
                                  Commit (GB)     36 / 128
Kernel Memory (MB)
Paged             402
Nonpaged          457

Processes: 137    CPU Usage: 73%    Physical Memory: 58%
```

Size Matters !!

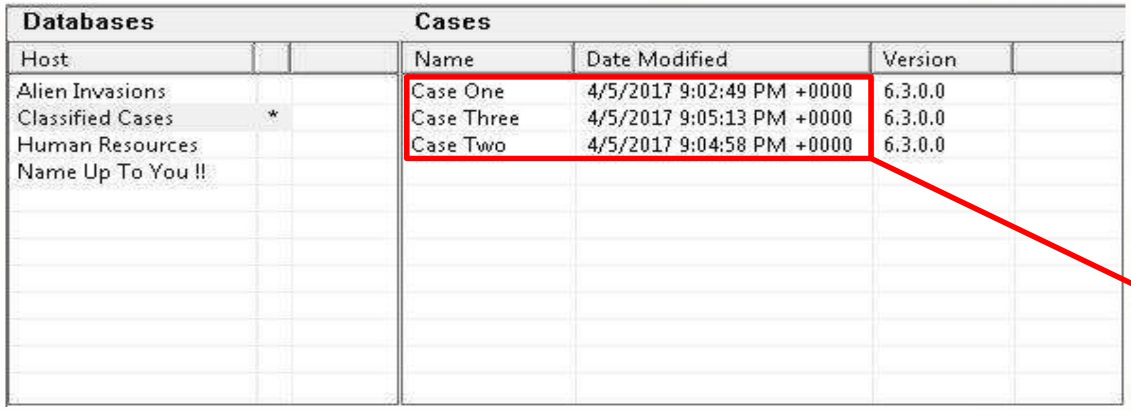
SUPPORTED BY

ACCESSDATA

CREDENCE SECURITY

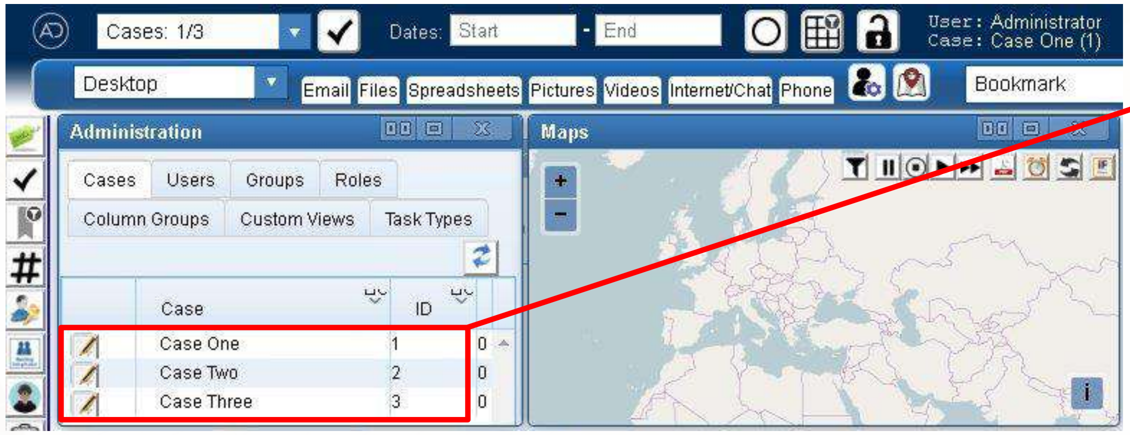
DATA IN THE

RIGHT PLACE



Databases		
Host		
Alien Invasions		
Classified Cases	*	
Human Resources		
Name Up To You !!		

Cases			
Name	Date Modified	Version	
Case One	4/5/2017 9:02:49 PM +0000	6.3.0.0	
Case Three	4/5/2017 9:05:13 PM +0000	6.3.0.0	
Case Two	4/5/2017 9:04:58 PM +0000	6.3.0.0	



Cases: 1/3 ✓ Dates: Start - End

User: Administrator
Case: Case One (1)

Desktop

Email Files Spreadsheets Pictures Videos Internet/Chat Phone

Bookmark

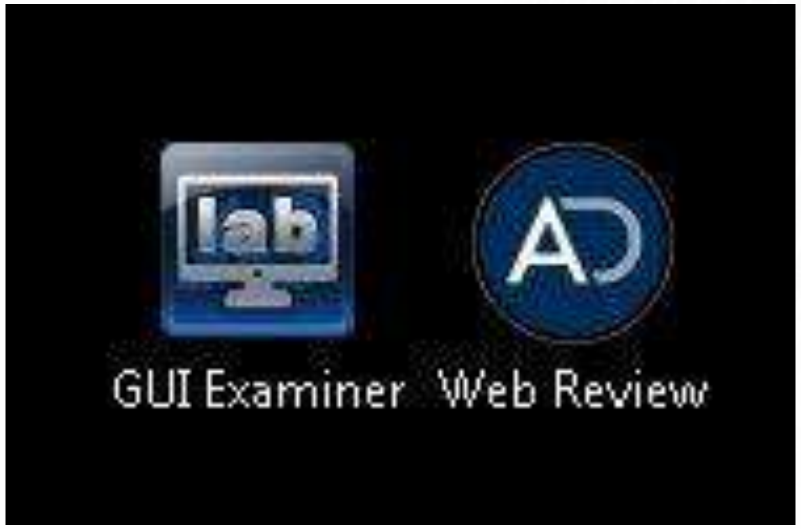
Administration

Cases Users Groups Roles

Column Groups Custom Views Task Types

Maps

Case	ID	
Case One	1	0
Case Two	2	0
Case Three	3	0



Lab provides multiple windows to case data:

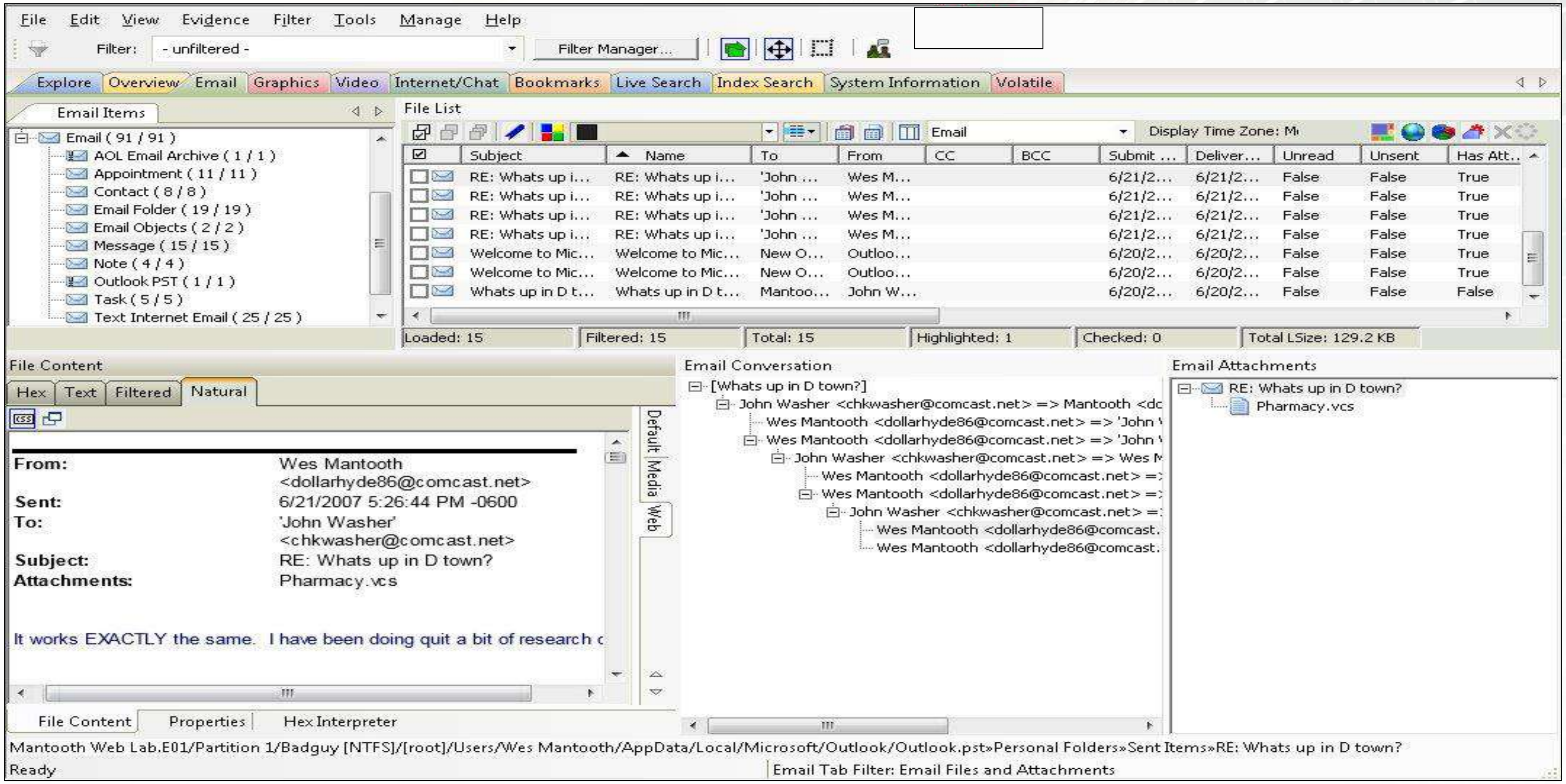
- ✓ Heavy client examiner (forensic examiner)
- ✓ HTML-based web review (case investigators)

SUPPORTED BY

ACCESSDATA

THE RIGHT TOOL FOR THE JOB

EXAMINER



- Email (91 / 91)
  - AOL Email Archive (1 / 1)
  - Appointment (11 / 11)
  - Contact (8 / 8)
  - Email Folder (19 / 19)
  - Email Objects (2 / 2)
  - Message (15 / 15)
  - Note (4 / 4)
  - Outlook PST (1 / 1)
  - Task (5 / 5)
  - Text Internet Email (25 / 25)

☑	Subject	Name	To	From	CC	BCC	Submit ...	Deliver...	Unread	Unsent	Has Att..
□	RE: Whats up i...	RE: Whats up i...	'John ...	Wes M...			6/21/2...	6/21/2...	False	False	True
□	RE: Whats up i...	RE: Whats up i...	'John ...	Wes M...			6/21/2...	6/21/2...	False	False	True
□	RE: Whats up i...	RE: Whats up i...	'John ...	Wes M...			6/21/2...	6/21/2...	False	False	True
□	RE: Whats up i...	RE: Whats up i...	'John ...	Wes M...			6/21/2...	6/21/2...	False	False	True
□	Welcome to Mic...	Welcome to Mic...	New O...	Outloo...			6/20/2...	6/20/2...	False	False	True
□	Welcome to Mic...	Welcome to Mic...	New O...	Outloo...			6/20/2...	6/20/2...	False	False	True
□	Whats up in D t...	Whats up in D t...	Mantoo...	John W...			6/20/2...	6/20/2...	False	False	False

Loaded: 15 | Filtered: 15 | Total: 15 | Highlighted: 1 | Checked: 0 | Total LSize: 129.2 KB

From:	Wes Mantooth <dollarhyde86@comcast.net>
Sent:	6/21/2007 5:26:44 PM -0600
To:	'John Washer' <chkwasher@comcast.net>
Subject:	RE: Whats up in D town?
Attachments:	Pharmacy.vcs

It works EXACTLY the same. I have been doing quit a bit of research c

- [Whats up in D town?]
  - John Washer <chkwasher@comcast.net> => Mantooth <dc
    - Wes Mantooth <dollarhyde86@comcast.net> => 'John \
    - Wes Mantooth <dollarhyde86@comcast.net> => 'John \
      - John Washer <chkwasher@comcast.net> => Wes M
        - Wes Mantooth <dollarhyde86@comcast.net> =>
        - Wes Mantooth <dollarhyde86@comcast.net> =>
          - John Washer <chkwasher@comcast.net> =>
            - Wes Mantooth <dollarhyde86@comcast.
            - Wes Mantooth <dollarhyde86@comcast.

- RE: Whats up in D town?
  - Pharmacy.vcs

Mantooth Web Lab.E01/Partition 1/Badguy [NTFS]/[root]/Users/Wes Mantooth/AppData/Local/Microsoft/Outlook/Outlook.pst»Personal Folders»Sent Items»RE: Whats up in D town?

Ready | Email Tab Filter: Email Files and Attachments

Heavy Client Examiner:

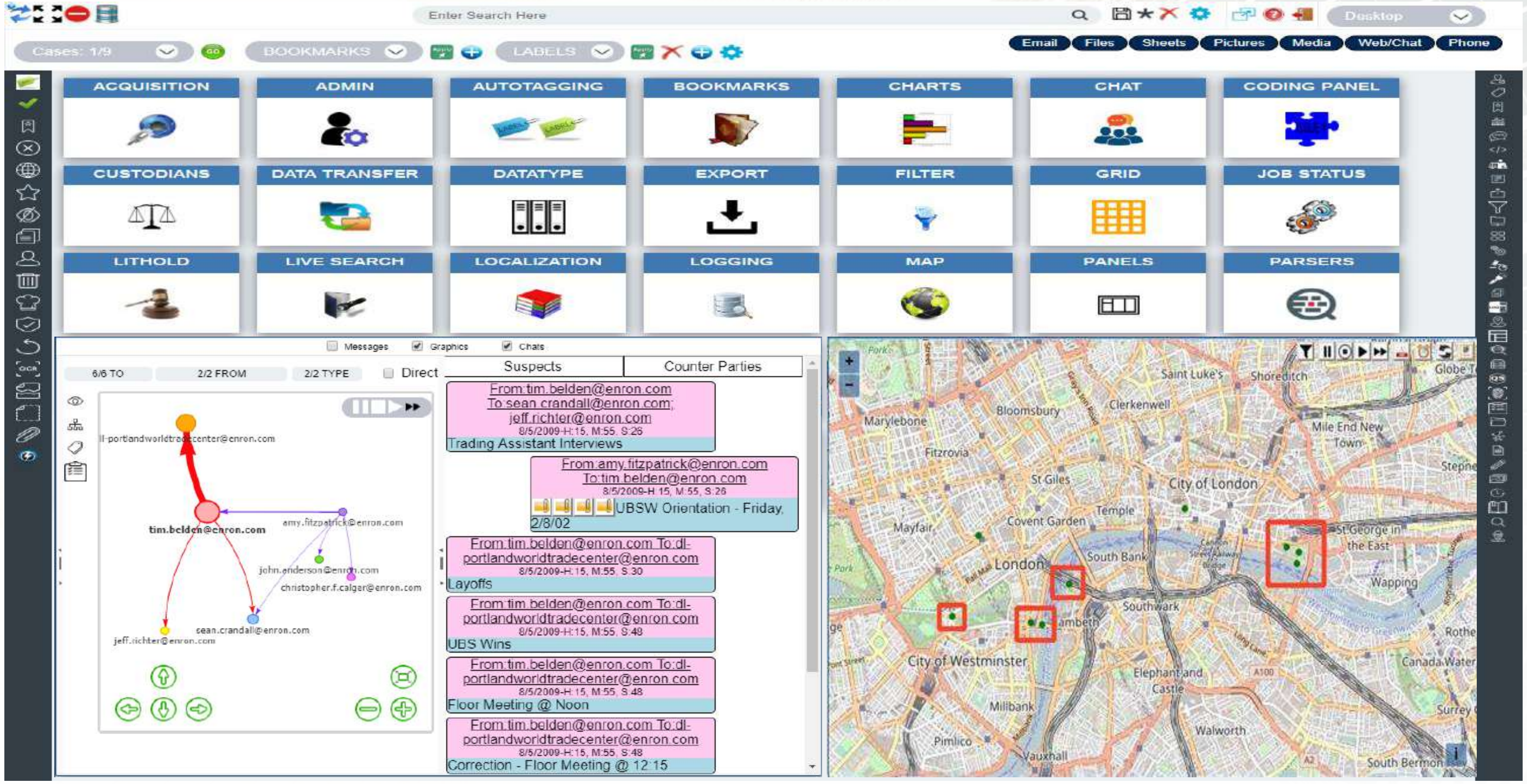
- ✓ Email threading
- ✓ Memory Analysis
- ✓ Robust file identification
- ✓ Robust data filtering
- ✓ Built-in decryption
- ✓ Full indexed search

SUPPORTED BY ACCESSDATA

CREDENCE SECURITY

THE RIGHT TOOL FOR THE JOB

REVIEWER



From:tim.belden@enron.com
To:sean.crandall@enron.com;
jeff.richter@enron.com
8/5/2009-H:15, M:55, S:26
Trading Assistant Interviews

From:amy.fitzpatrick@enron.com
To:tim.belden@enron.com
8/5/2009-H:15, M:55, S:26
UBSW Orientation - Friday, 2/8/02

From:tim.belden@enron.com To:dl-portlandworldtradecenter@enron.com
8/5/2009-H:15, M:55, S:30
Layoffs

From:tim.belden@enron.com To:dl-portlandworldtradecenter@enron.com
8/5/2009-H:15, M:55, S:48
UBS Wins

From:tim.belden@enron.com To:dl-portlandworldtradecenter@enron.com
8/5/2009-H:15, M:55, S:48
Floor Meeting @ Noon

From:tim.belden@enron.com To:dl-portlandworldtradecenter@enron.com
8/5/2009-H:15, M:55, S:48
Correction - Floor Meeting @ 12:15

Web Reviewer:

- ✓ Geo-plotting
- ✓ Timeline plotting
- ✓ Cross-case analysis
- ✓ Target profile analytics
- ✓ Data permissions
- ✓ Reviewer tasking

SUPPORTED BY

ACCESSDATA

THE RIGHT TOOL FOR THE JOB

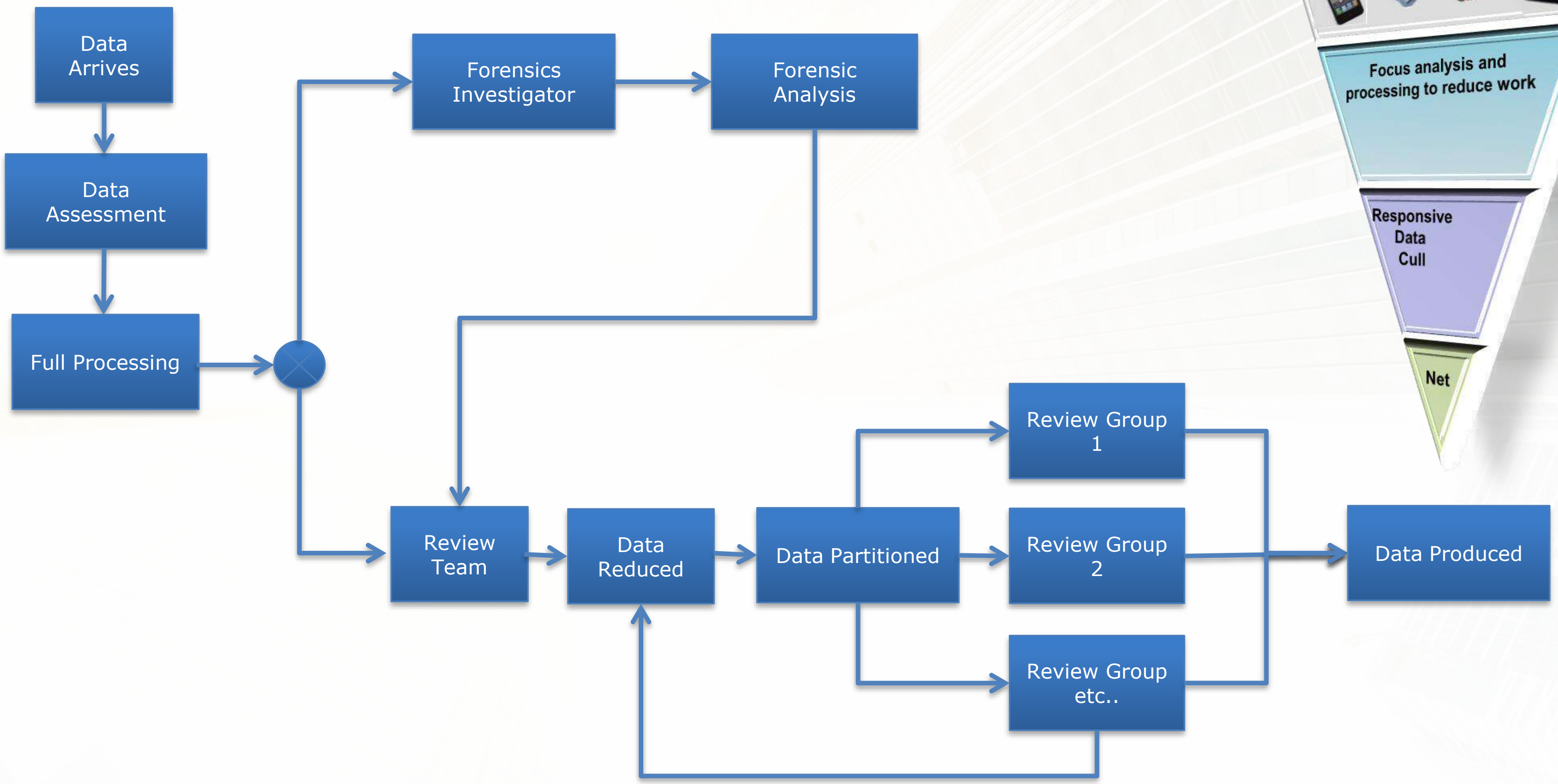
REVIEWER

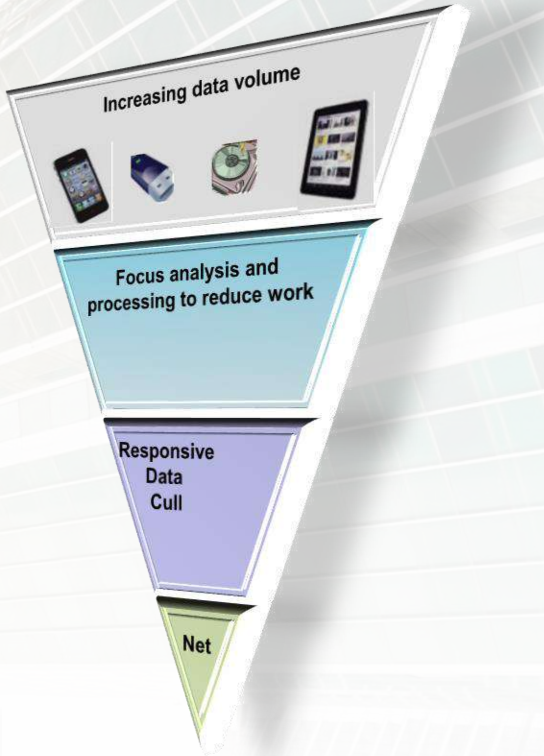
- ✓ Massive scale for collaboration
- ✓ Custom data views to focus review work
- ✓ Custom interface to match user skills
- ✓ Alternate languages available …
- ✓ Case management through review …
- ✓ User Tasking
- ✓ User Communications
- ✓ Data Analytics
- ✓ Working together with your technology

SUPPORTED BY

ACCESSDATA

LIFECYCLE OF COLLABORATION



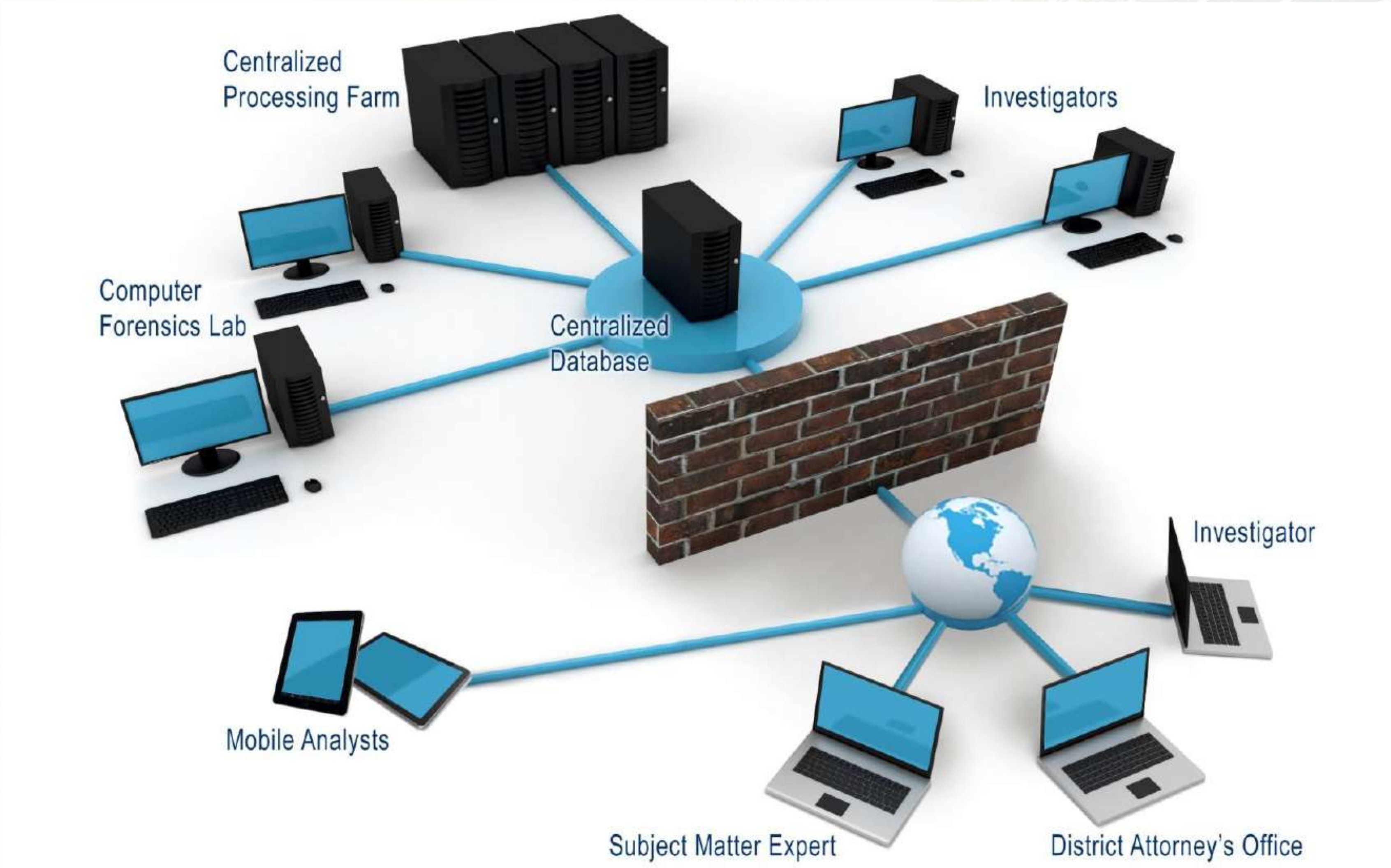


Potential Use Cases:

- ✓ Pre-trial review
- ✓ Agency collaboration
- ✓ Workload Distribution
- ✓ Data Processing Reduction

SUPPORTED BY ACCESSDATA

REAL TIME
COLLABORATION



Scalable features:

- ✓ Processing
- ✓ Examiners
- ✓ Databases
- ✓ Reviewers

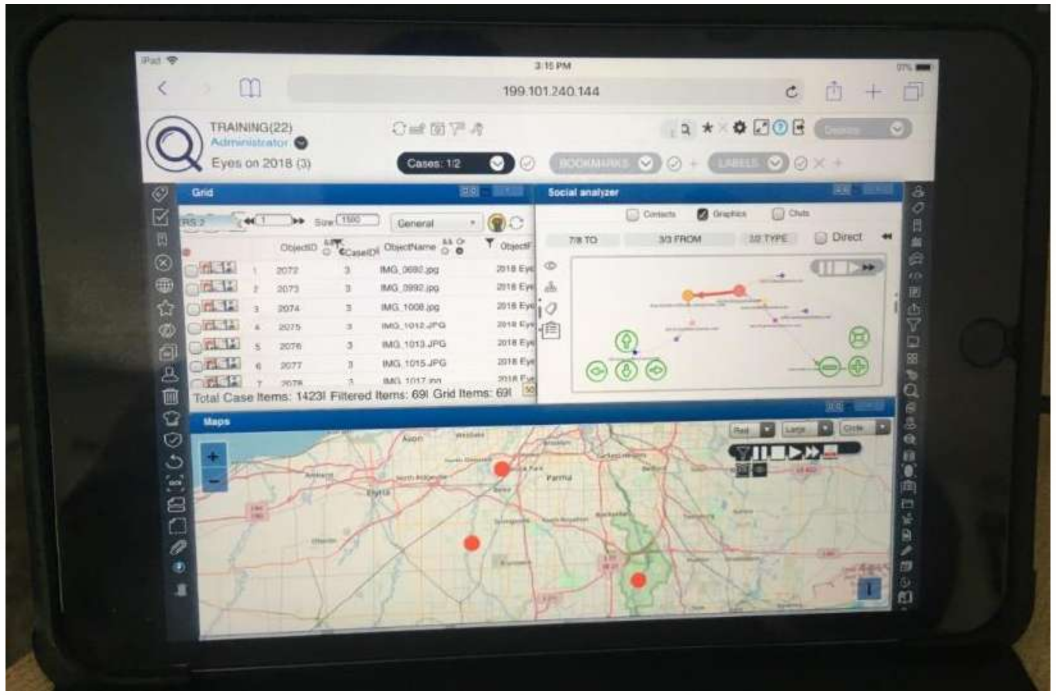
Efficient Migration:

- ✓ Minimal learning curve for FTK users
- ✓ Minimal hardware outlay for reviewers

SUPPORTED BY
ACCESSDATA

MOBILITY & FREEDOM

FROM HARDWARE



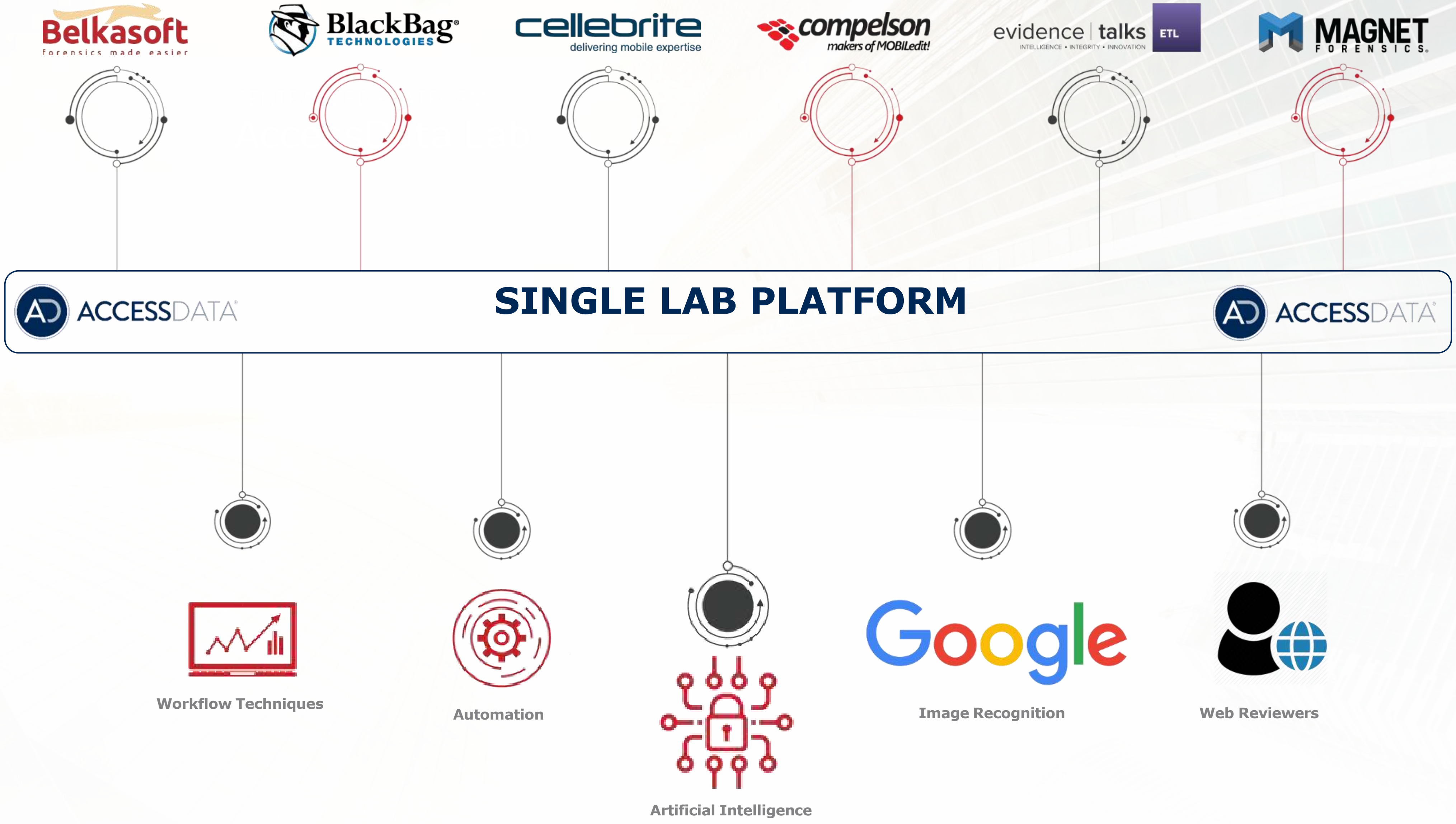
- ✓ AWS
- ✓ Bring your licensing …
- ✓ Use ours when you need

- ✓ HTML 5…
- ✓ Mobility with scale
- ✓ Holidays are over !!

SUPPORTED BY

ACCESSDATA

CENTRALISED
PLATFORM



SINGLE LAB PLATFORM

Workflow Techniques

Automation

Artificial Intelligence

Image Recognition

Web Reviewers

SUPPORTED BY
ACCESSDATA

ACCESSDATA

WHAT IS QUIN-C?

SUPPORTED BY

ACCESSDATA

QUIN-C

CURIOUS ABOUT THE NAME?

JACK KLUGMAN is
QUINCY, M.E.
The Original Crime Scene Investigator
M
Moderate Themes, Mild Violence
DVD VIDEO
UNIVERSAL

Quin-C is named in tribute to *Quincy, M.E.,* the popular television series about forensic pathology that aired from 1976 to 1983.

While many detective series at the time portrayed rudimentary physical evidence analysis such as fingerprints and bullet comparisons, *Quincy, M.E.* was the first series to regularly present in-depth forensic investigations – **it was ahead of its time.**

So is Quin-C.

THE NOW...

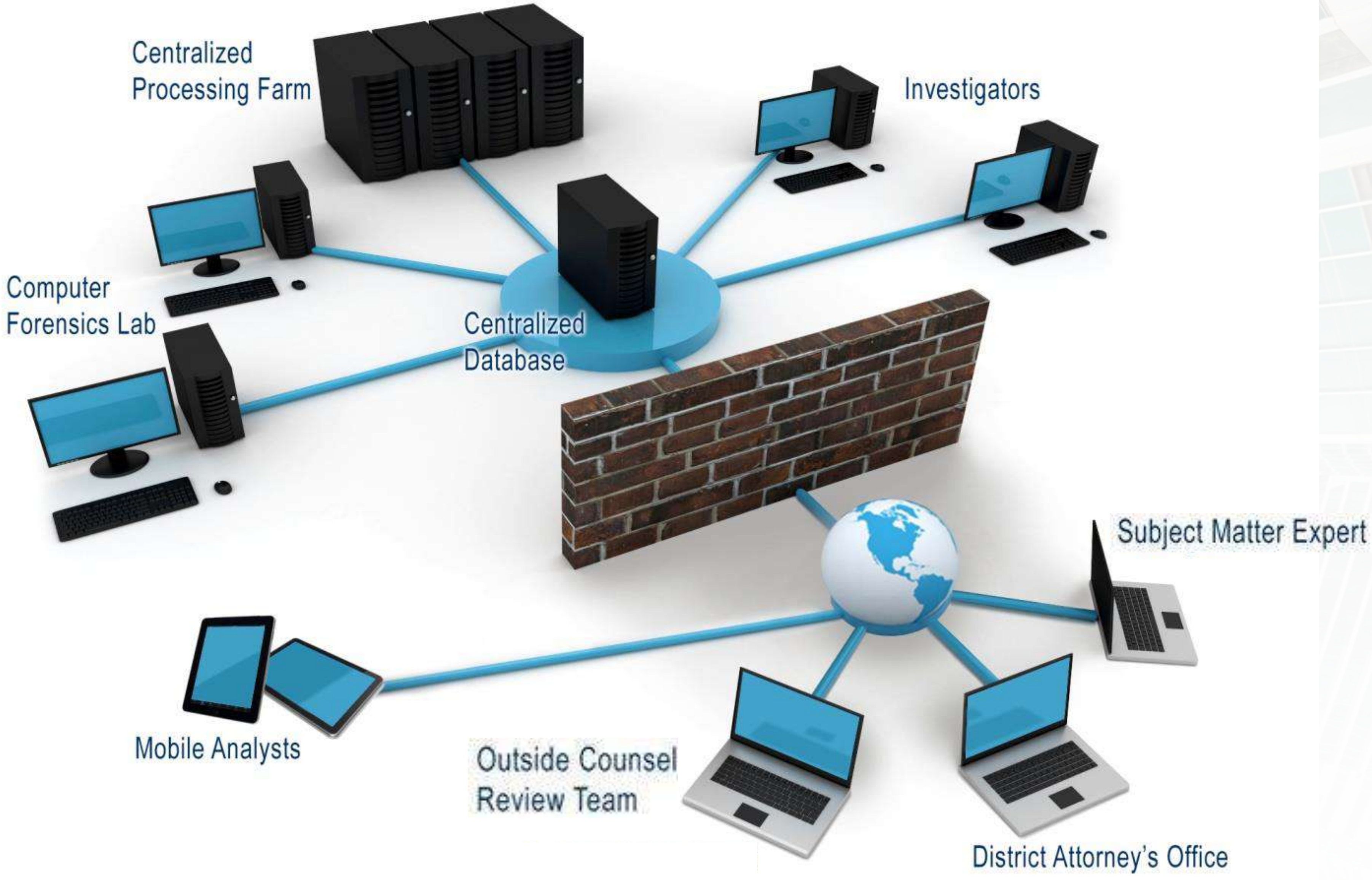
THE FUTURE

The Now

- Basic
- Investigator
- Legal
- Collaboration

The Future

- Response tool
- Compliance tool
- Mobile analysis
- You dream it …

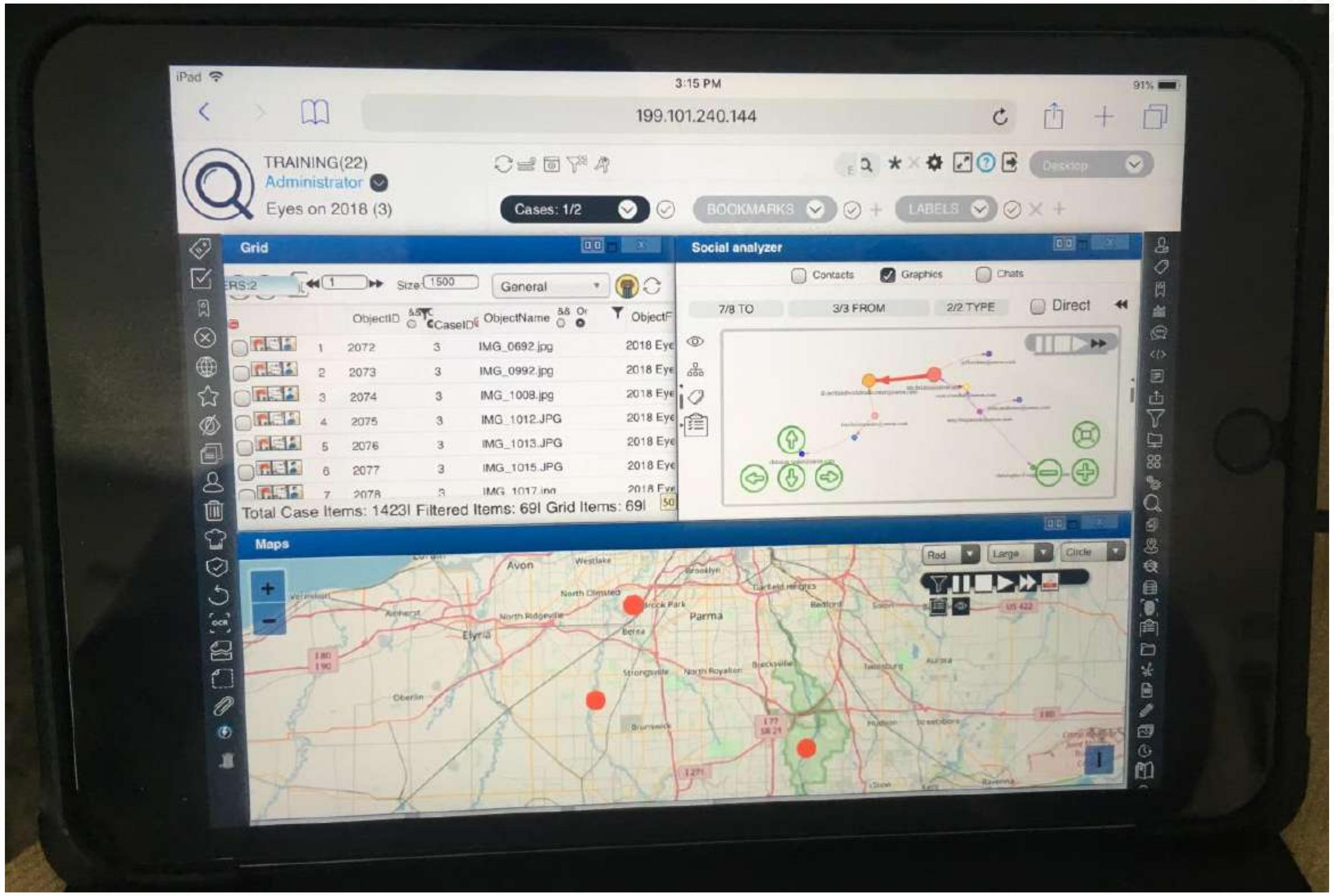


SUPPORTED BY

ACCESSDATA

QUIN-C

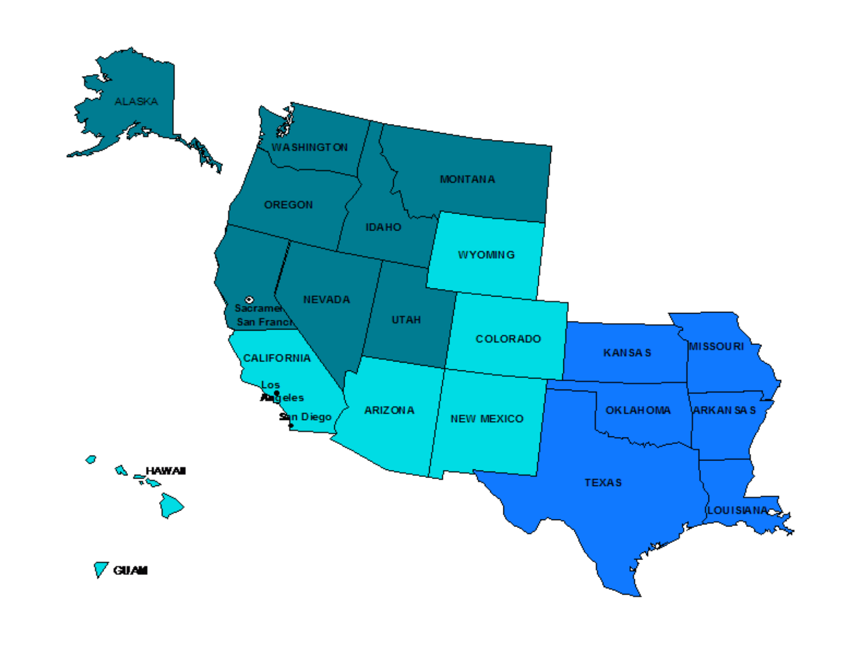
IT REALLY DOES THIS…



Size: 1500 General

	ObjectID	CaseID	ObjectName	ObjectF
1	2072	3	IMG_0692.jpg	2018 Eye
2	2073	3	IMG_0992.jpg	2018 Eye
3	2074	3	IMG_1008.jpg	2018 Eye
4	2075	3	IMG_1012.JPG	2018 Eye
5	2076	3	IMG_1013.JPG	2018 Eye
6	2077	3	IMG_1015.JPG	2018 Eye
7	2078	3	IMG_1017.jpg	2018 Eye

Total Case Items: 1423| Filtered Items: 69| Grid Items: 69|



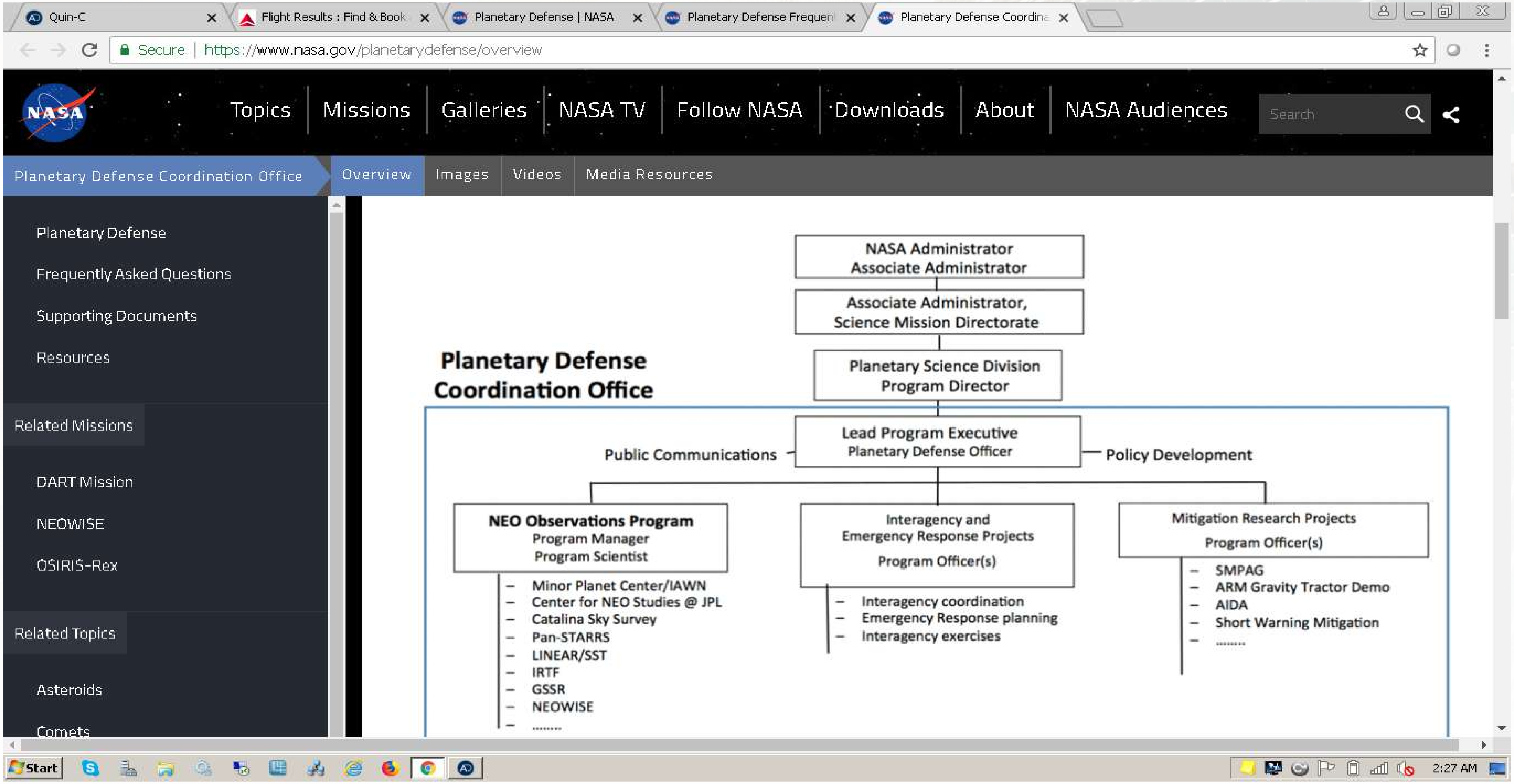
- HTML 5 …
- Mobility with scale
- Holidays are over !!

SUPPORTED BY

ACCESSDATA

CREDENCE SECURITY

ACCESSDATA
QUIN-C



Planetary Defense Coordination Office

NASA Administrator
Associate Administrator

Associate Administrator,
Science Mission Directorate

Planetary Science Division
Program Director

Lead Program Executive
Planetary Defense Officer

Public Communications

Policy Development

NEO Observations Program
Program Manager
Program Scientist

- Minor Planet Center/IAWN
- Center for NEO Studies @ JPL
- Catalina Sky Survey
- Pan-STARRS
- LINEAR/SST
- IRTF
- GSSR
- NEOWISE
- ....

Interagency and
Emergency Response Projects
Program Officer(s)

- Interagency coordination
- Emergency Response planning
- Interagency exercises

Mitigation Research Projects
Program Officer(s)

- SMPAG
- ARM Gravity Tractor Demo
- AIDA
- Short Warning Mitigation
- ....

SUPPORTED BY
ACCESSDATA

QUIN-C

THE LIST

Introduction

- What is QC
- Desktop Tour
- Talking Scale
- Turn ▲ , ▼

CR1 - Maps

- Scale down
- Case Access
- Custom Data View
- User Tasking
- Map Plotting

CR2 - Email

- Scale Up
- Index Search
- Social Analyzer
- Document Mark-up

CR3 - Parsers

- Ecosystem
- Belkasoft Data
- Image Recognition (1st A/I)
- Wash / Rinse / Repeat !!

Freelance …

- Panel Views
- Localization
- Process Data / Import
- Export Widget
- Report Widget
- Auto-tagging
- Spreadsheets
- Bread sheets
- Thumbnails
- Video Thumbs

SUPPORTED BY
ACCESSDATA

QUIN-C

THE LIST

Freelance …

- 4 facets of speed
  - Grid Page Size
  - Lazy Load
  - Speed Columns
  - Database Lock
- Let’s plot a drone
  - Lat / Long
  - Elevation
  - Path
  - Rotor speeds

Admin …

- Configurations (*.*)
  - JSONs
  - Setup Configuration
  - Processing
  - Crime Types
  - Column Groups
  - Label Matrix
  - Viewer Configuration

Watson

- Predictive Coding
- Document Clustering
- Cross Case Images
- Cross Case Geo-Location
- Cross Case Contacts
- Entities
- Watson Investigations
  - Investigations
  - Who / What / When
  - Where / Why / Learning ??

SUPPORTED BY ACCESSDATA

QUIN-C

THE LIST

Admin …

- System Values
  - Cases
  - Export
  - Transfer
  - Evidence
  - Using another DB
  - Distributed Processing
- Top Level Functions
  - Cases
  - Users
  - Roles

Admin …

- Configurations (*.*)
  - JSONs
  - Setup Configuration
  - Processing
  - Crime Types
  - Column Groups
  - Label Matrix
  - Viewer Configuration

Watson

- Predictive Coding
- Document Clustering
- Cross Case Images
- Cross Case Geo-Location
- Cross Case Contacts
- Entities
- Watson Investigations
  - Investigations
  - Who / What / When
  - Where / Why / Learning ??

ACCESSDATA

LIVE DEMO

LIVE DEMO

SUPPORTED BY

ACCESSDATA

QUESTION &

ANSWER

QUESTIONS?

SUPPORTED BY

ACCESSDATA

CREDENCE
SECURITY

THANK YOU

FORENSIC FUNDAMENTALS

NEXT WEBINAR

MAGNET
FORENSICS®

13th November 2018
2PM GST (GMT +4)