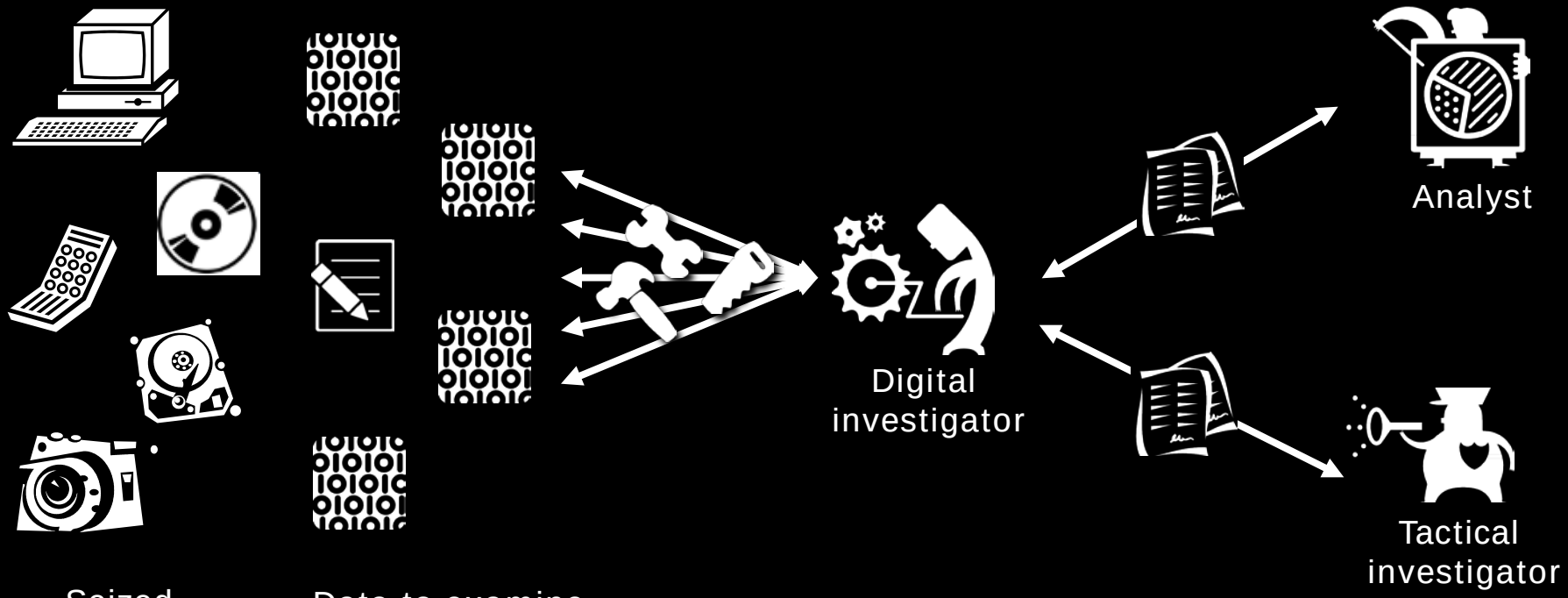
Netherlands Forensic Institute
Ministry of Security and Justice

Digital Forensics as a Service:

an update

Harm van Beek PhD
harm.van.beek@nfi.minvenj.nl

Traditional digital investigation



right information

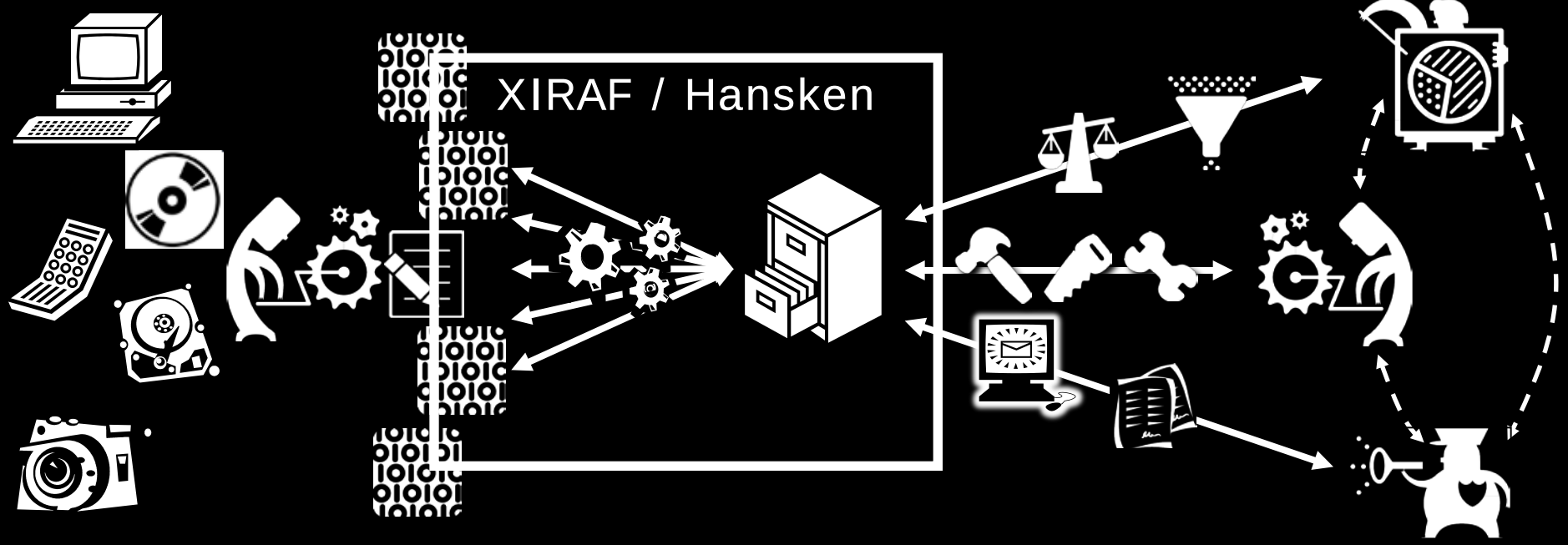
at the

right time

to the

right people

Digital Forensics as a Service (since Q4 2010)



> 600 cases

> 10,000 devices

> 1.5 PB data

> 2,500 investigators

all (regional) Dutch police forces

National High Tech Crime Unit

RST Former Dutch Antilles

Toronto Police

...

The six main lessons learned

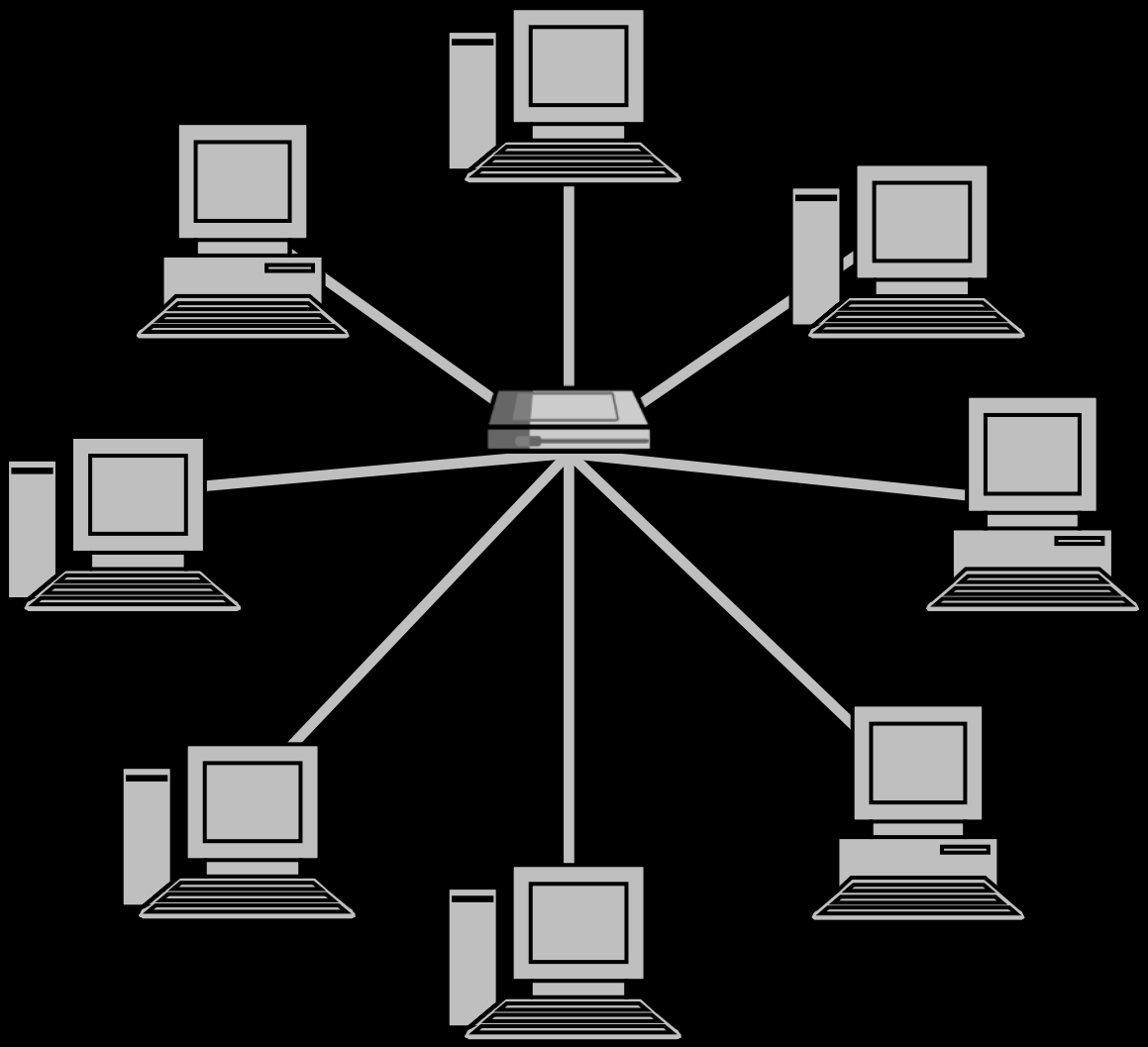
“Experience is a hard teacher because she gives the test first, the lesson afterwards.”

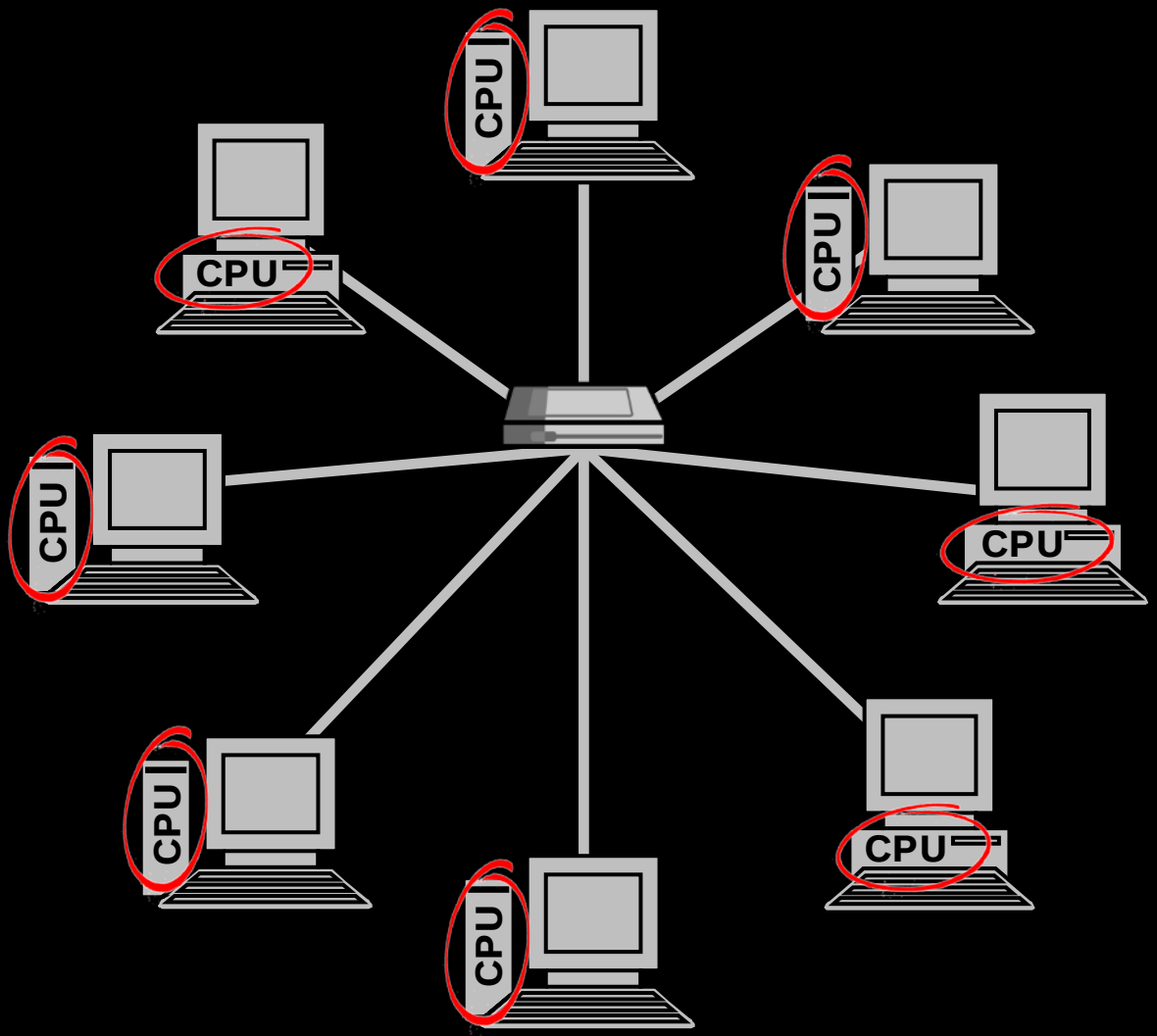
-- Vernon Sanders Law

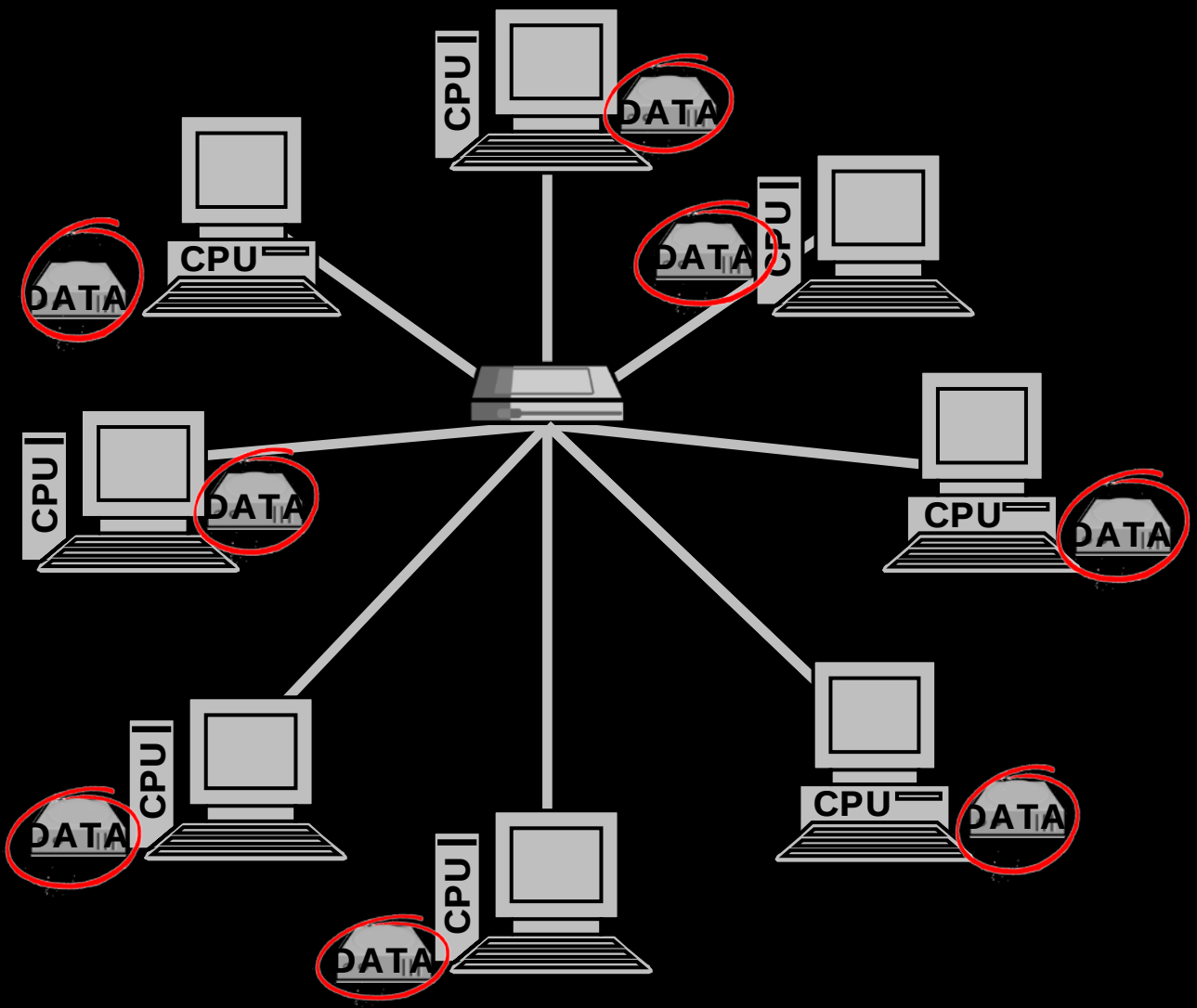
Lesson one

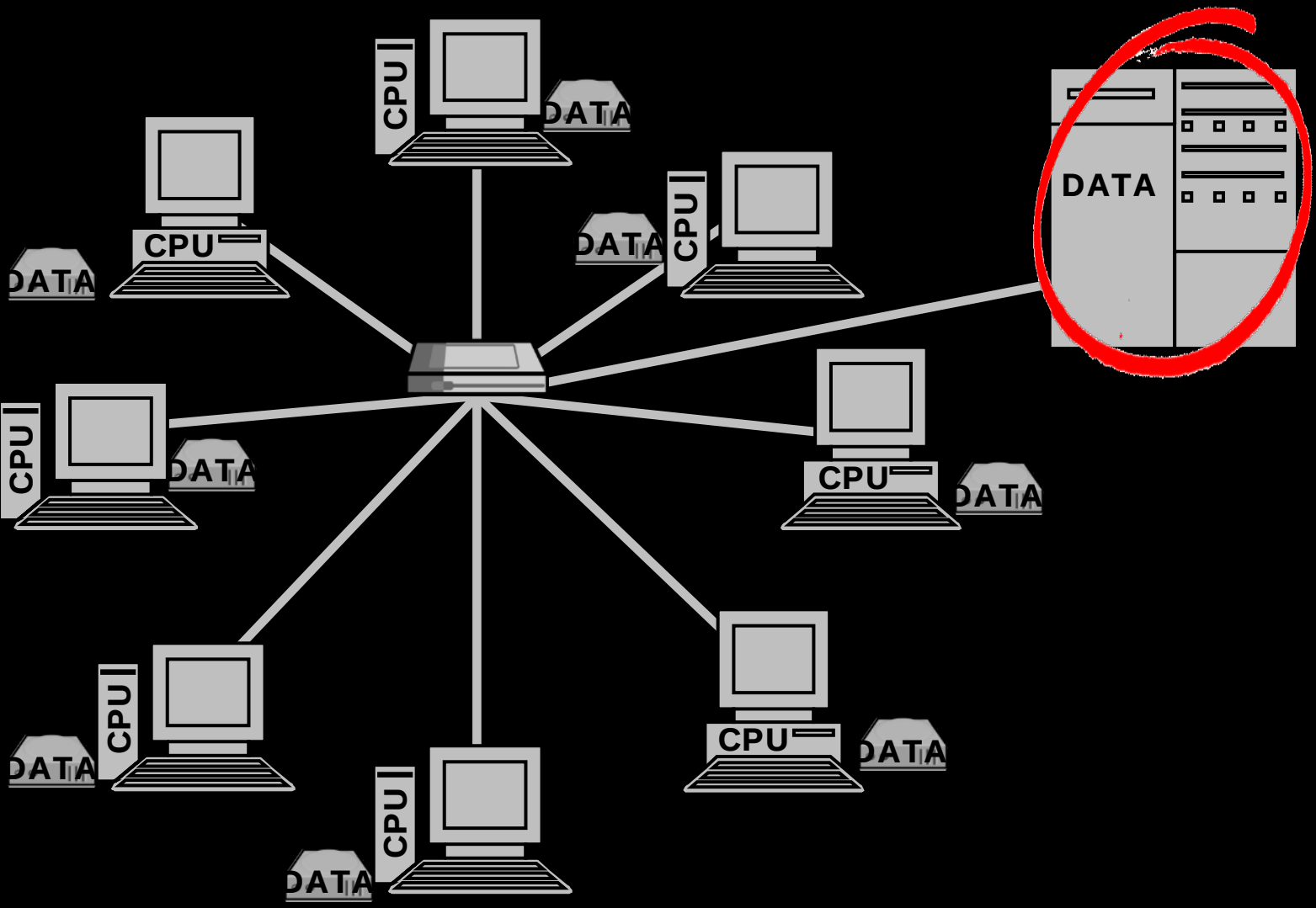
How to process a lot of data?

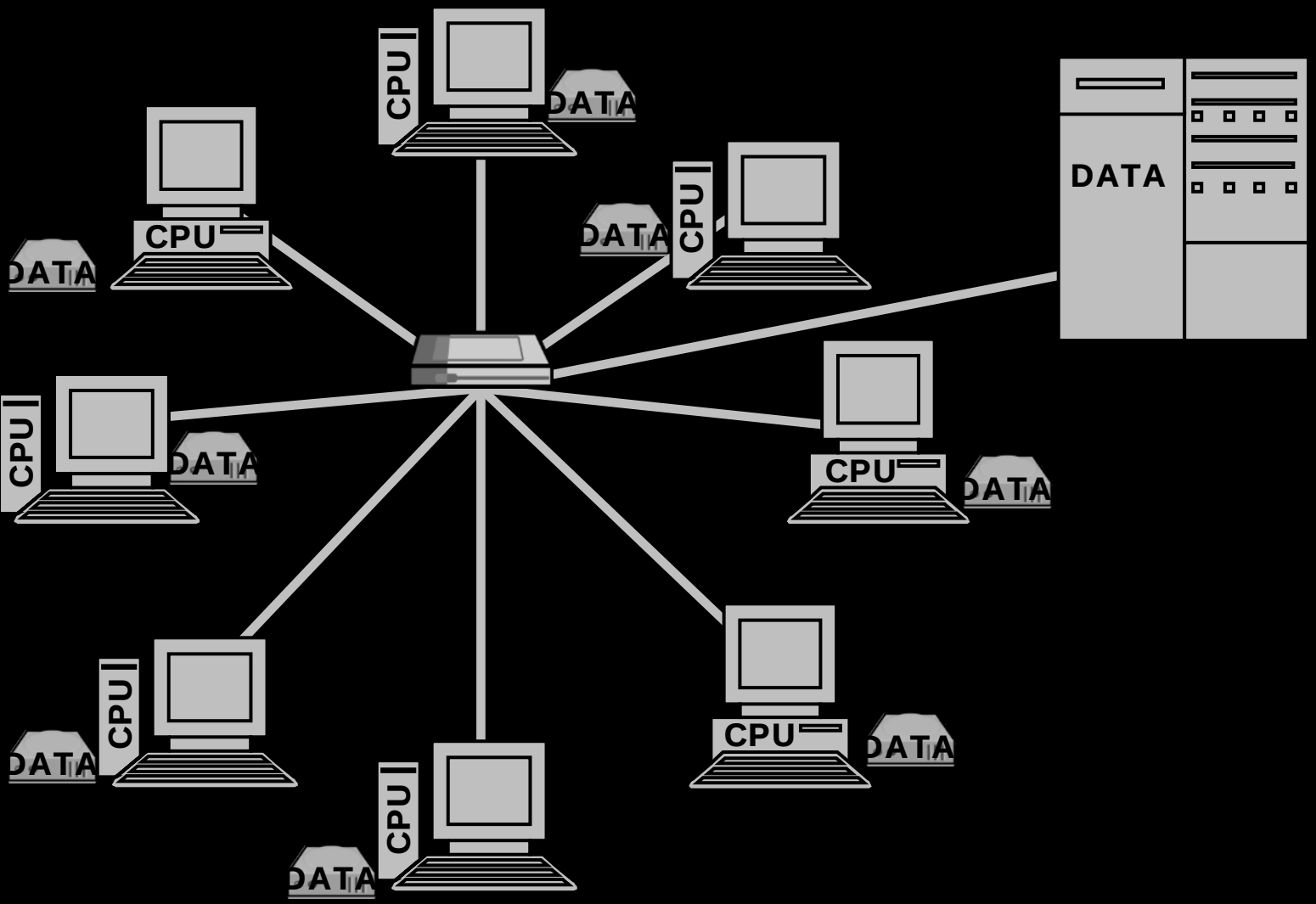
Bring computing power to the data

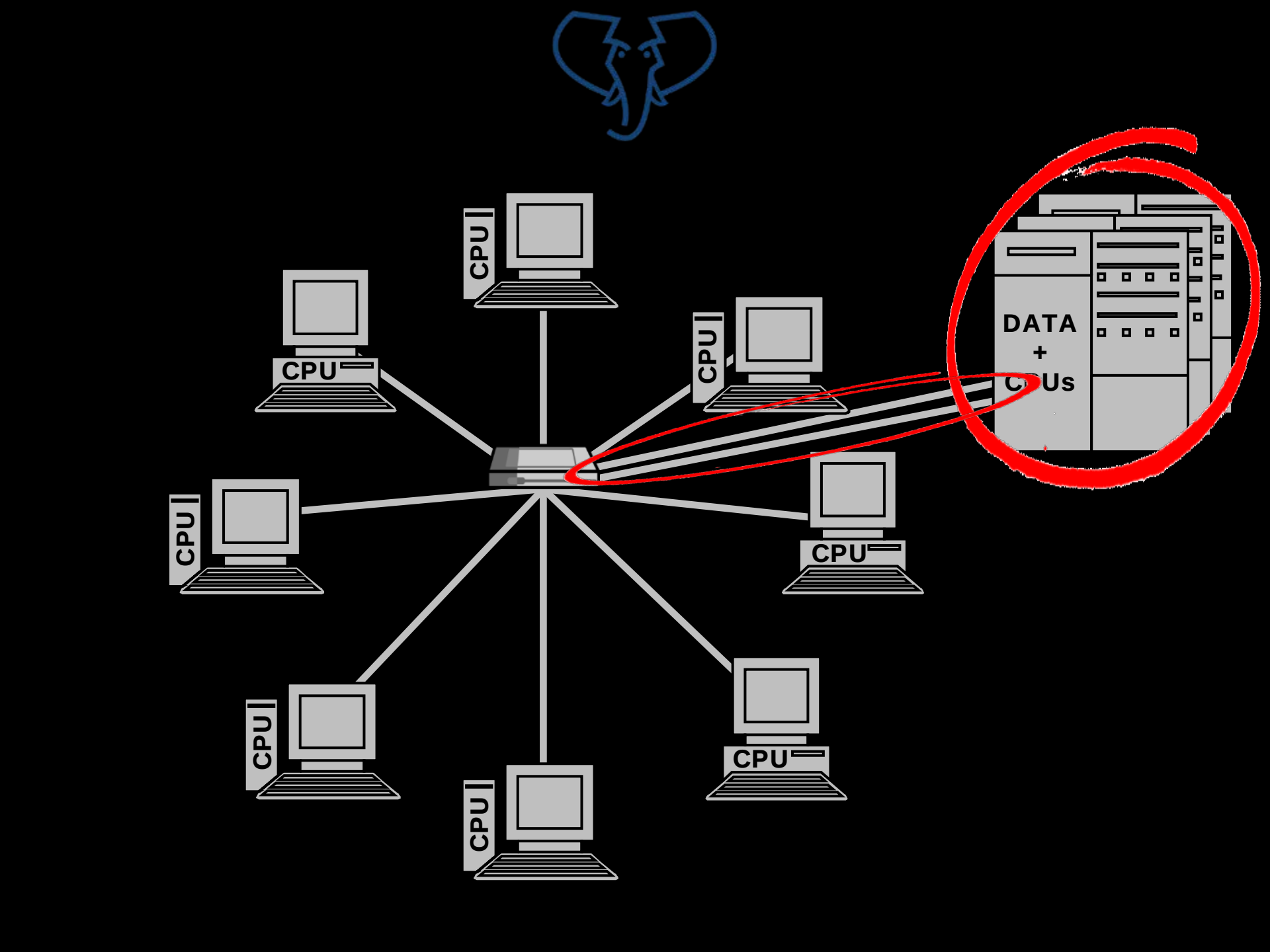


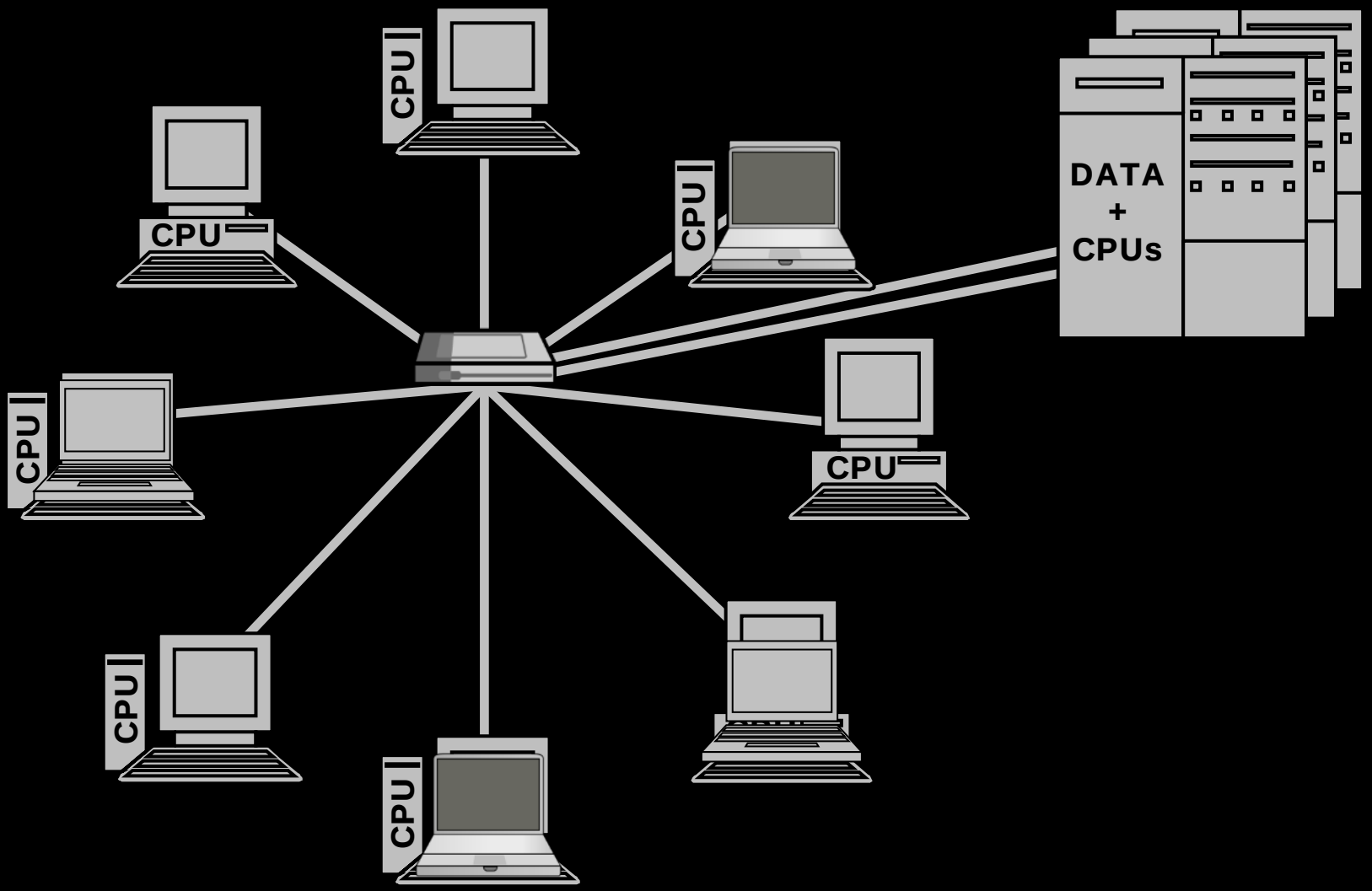

CPU
CPU
CPU
CPU
CPU
CPU
CPU
CPU

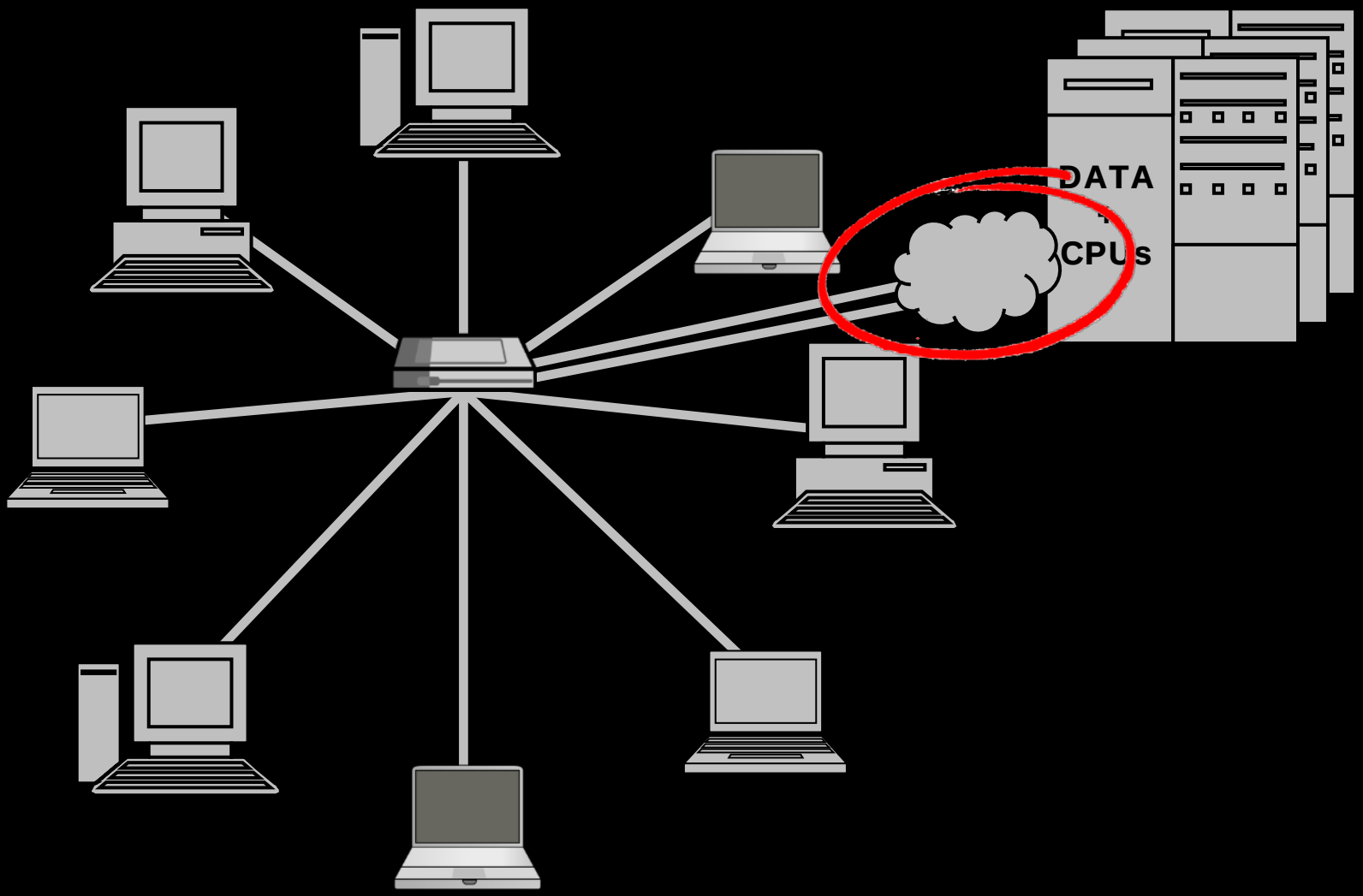

CPU
DATA
CPU
DATA
CPU
DATA
CPU
DATA
CPU
DATA
CPU
DATA
CPU
DATA
CPU
DATA

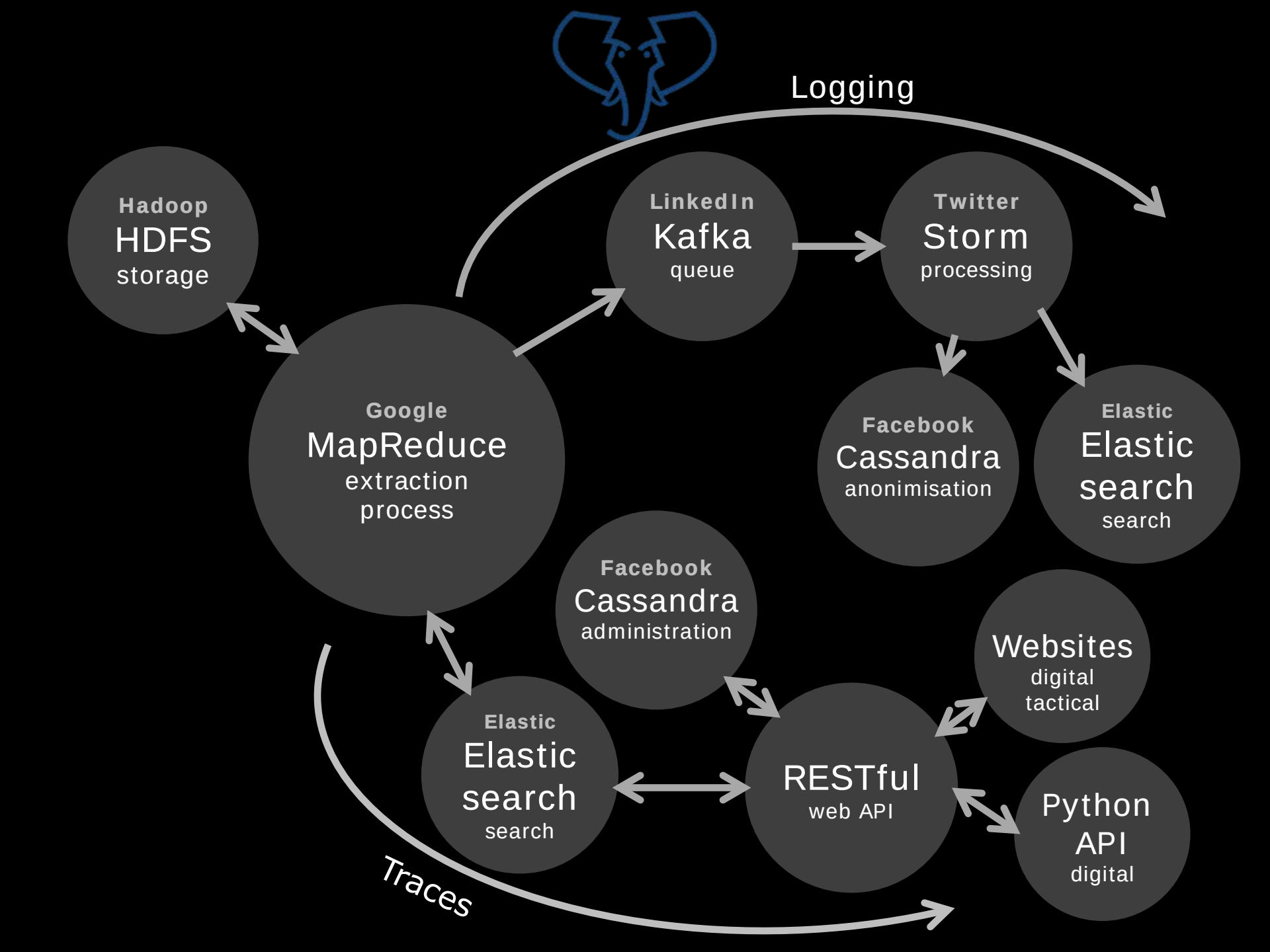

CPU
DATA
CPU
DATA
CPU
DATA
DATA
CPU
DATA
CPU
DATA
CPU
DATA
CPU
DATA
CPU
DATA


CPU
DATA
CPU
DATA
CPU
DATA
DATA
CPU
DATA
CPU
DATA
CPU
DATA
CPU
DATA
CPU
DATA


CPU
CPU
CPU
CPU
CPU
CPU
CPU
CPU
DATA
+
CPUs


CPU
CPU
CPU
CPU
CPU
CPU
CPU
CPU
DATA
+
CPUs


DATA
CPUs


Logging
Hadoop
HDFS
storage
LinkedIn
Kafka
queue
Twitter
Storm
processing
Google
MapReduce
extraction
process
Facebook
Cassandra
anonimisation
Elastic
Elastic
search
search
Facebook
Cassandra
administration
Websites
digital
tactical
Elastic
Elastic
search
search
RESTful
web API
Python
API
digital
Traces

ARTICLE IN PRESS
Digital Investigation xxx (2015) 1–19
Contents lists available at ScienceDirect
Digital Investigation
journal homepage: www.elsevier.com/locate/diin

Digital forensics as a service: Game on

H.M.A. van Beek*, E.J. van Eijk, R.B. van Baar, M. Ugen, J.N.C. Bodde, A.J. Siemelink
Netherlands Forensic Institute, Laan van Ypenburg 6, 2497 GB The Hague, The Netherlands

ARTICLE INFO
Article history:
Received 12 March 2015
Received in revised form 8 July 2015
Accepted 11 July 2015
Available online xxxx
Keywords:
Distributed systems
Digital forensics
Big data
XIRAF
Hansken

ABSTRACT
The big data era has a high impact on forensic data analysis. Work is done in speeding up the processing of large amounts of data and enriching this processing with new techniques. Doing forensics calls for specific design considerations, since the processed data is incredibly sensitive. In this paper we explore the impact of forensic drivers and major design principles like security, privacy and transparency on the design and implementation of a centralized digital forensics service.

Introduction

Many papers in the field of digital forensics start with the observation that the size of digital material increases, that the complexity and diversity of the digital evidence grows and that more advanced techniques are needed to be able to keep up with the evolving digital society.[1]

Since December 2010, the Netherlands Forensic Insitute has been using a service-based approach for processing and investigating high volumes of seized digital material: Digital Forensics as a Service (DFaaS) (van Baar et al., 2014). This service is called XIRAF (Bhoedjang et al., 2012).

Now, four years later, this approach has become a standard for hundreds of criminal cases and over a thousand investigators, both in The Netherlands and abroad. After having processed over a petabyte of data, we have experienced the impact of the XIRAF system and the paradigm shift it is causing (van Baar et al., 2014). XIRAF started in 2006 as a scientific research project aimed at identifying and developing techniques for automating (parts of) the data analysis process. XIRAF was never meant to be an operational system for processing petabytes of data and providing access to over a thousand investigators. As a result, design decisions taken during the development of XIRAF leave room for improvement.

In the beginning of 2012, we started working on the successor of XIRAF, named Hansken. This work consisted of defining design principles, building a proof of concept (PoC) based on the new principles and ideas, making design decisions based on the principles and PoC and building a production version to replace XIRAF. This paper provides an overview of the major design decisions that form the foundation for the Hansken solution for providing digital forensics as a service.

A lot of challenges arise when building a system to provide insight in petabytes of different types of data. Especially when integrity and confidentiality of the data are crucial. While it is tempting to focus on developing new techniques and building bigger and faster systems, boundaries need to be established in which such a system can operate. Without these boundaries, major risks of data breaches and leaks of sensitive information exist.

* Corresponding author.
E-mail address: harm.van.beek@nfi.minvenj.nl (H.M.A. van Beek).
[1] http://apmdigest.com/gartner-top-10-strategic-technology-trends-for-2013-big-data-cloud-analytics-and-mobile, visited March 11, 2015.

http://dx.doi.org/10.1016/j.diin.2015.07.004
1742-2876/

Lesson two

How to provide this service?

Do what you are good at!

We're not all digital investigators

Team of specialists

forensic software developers

platform developers

front-end developers

python developer

system administrators

software architect

quality engineers

operators

operational support

project leader

forensic scientists

Tea

forensic soft
developer

platform d

front-end

python

system

eers

l support

eader

scien

Digital Investigation 11 (2014) S54–S62

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Digital Forensics as a Service: A game changer

R.B. van Baar*, H.M.A. van Beek, E.J. van Eijk

Netherlands Forensics Institute, Laan van Ypenburg 6, 2497 GB The Hague, The Netherlands

Keywords:
Digital forensics
DFaaS
Digital forensic process
Process model
Xiraf

ABSTRACT

How is it that digital investigators are always busy and still never have enough time to actually dig deep into digital evidence? In this paper we will explore the current implementation of the digital forensic process and analyze factors that impact the efficiency of this process. Next we explain how in the Netherlands a Digital Forensics as a Service implementation reduced case backlogs and freed up digital investigators to help detectives better understand the digital material.

Introduction

It is impossible to imagine life today without digital material. Who does not use a computer, smartphone, tablet or other digital device nowadays? As a result of the explosive growth in the number of devices and their use, the traces produced by the use of these devices have become more and more important in combating crime. This growth requires a new understanding of forensic data analysis: of the manner in which the data on these devices is processed and of the manner in which the traces collected by this processing is analyzed.

Since December 2010, in the Netherlands a new approach is used for processing and investigating the high volume of seized digital material, viz. Digital Forensics as a Service (DFaaS). Now, three years later, this approach has become a standard for hundreds of criminal cases and over a thousand detectives. This paper describes our approach and the impact on both the digital and tactical investigative process.

This paper starts with describing related work in the next section. In Section Traditional digital investigation process we describe the traditional digital investigation process, that we analyze in Section Analysis of the traditional process. The service model helps to solve a number of bottlenecks. The DFaaS model is described in Section Digital Forensics as a Service and analyzed in Section Analysis of the Digital Forensics as a Service Process. Despite the big changes this model causes, there is still room for improvement. In Section Experience and future work these improvements are discussed. Section Conclusions will complete this paper with final conclusions.

Related work

In this paper we apply a digital forensic process model to the previous and current digital forensic process in the Netherlands. In the related work we discuss process models, techniques that can help optimize the current process and expected developments that have an impact on the forensic process.

Process model

Even though the digital forensic process model is not standardized, consensus on the abstract level about the digital forensics process exists. The latest effort by Kohn et al. (2013) to propose a model contains an overview of the most significant models described over the years. On a high level, Kohn described six processes: *documentation, preparation, incident, incident response, digital forensic*

* Corresponding author.
E-mail addresses: ruud@holmes.nl (R.B. van Baar), ham@holmes.nl (H.M.A. van Beek), eijk@holmes.nl (E.J. van Eijk).

http://dx.doi.org/10.1016/j.diin.2014.03.007
1742-2876/

Lesson three

Can we trust the service?

Test, test... and test!

Current test set

> 7,700 unit tests

> 12,500 integration tests

if 1 test fails,
the code is not accepted
(by the development platform)

Lesson four

How to represent the results?

Use a uniform data model

Type of trace

Select a value

Chat message
Compressed
Contact
Content
Cookie
Cookie archive
Deleted
Document
Email
Email archive
Email folder
Encrypted
Event
Event log
File
File archive
File system
Folder
GPS entry
Image

+ add filter

search

Netherlands Forensic Institute Em Phone (+31) (0)70 – 888 6 440 Version

Type of trace ▾ | Email ▾

Choose a property ▾ | − remove

Choose a property
Application
From
Has attachment
Headers
In reply to
Message ID
Read
References
Sent
Subject
To

with | without | filter

case sensitive | invert selection

starts with | contains word | exact | ends wit

+ add filter

search

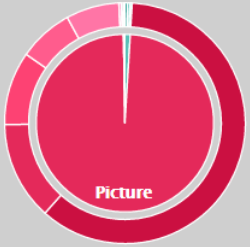
Lesson five

How to present the results?

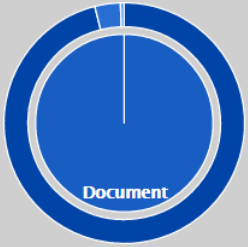
Listen to your colleagues

Dashboard

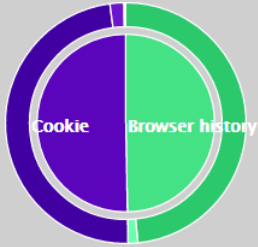
Media



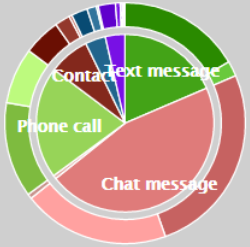
Documents



Web

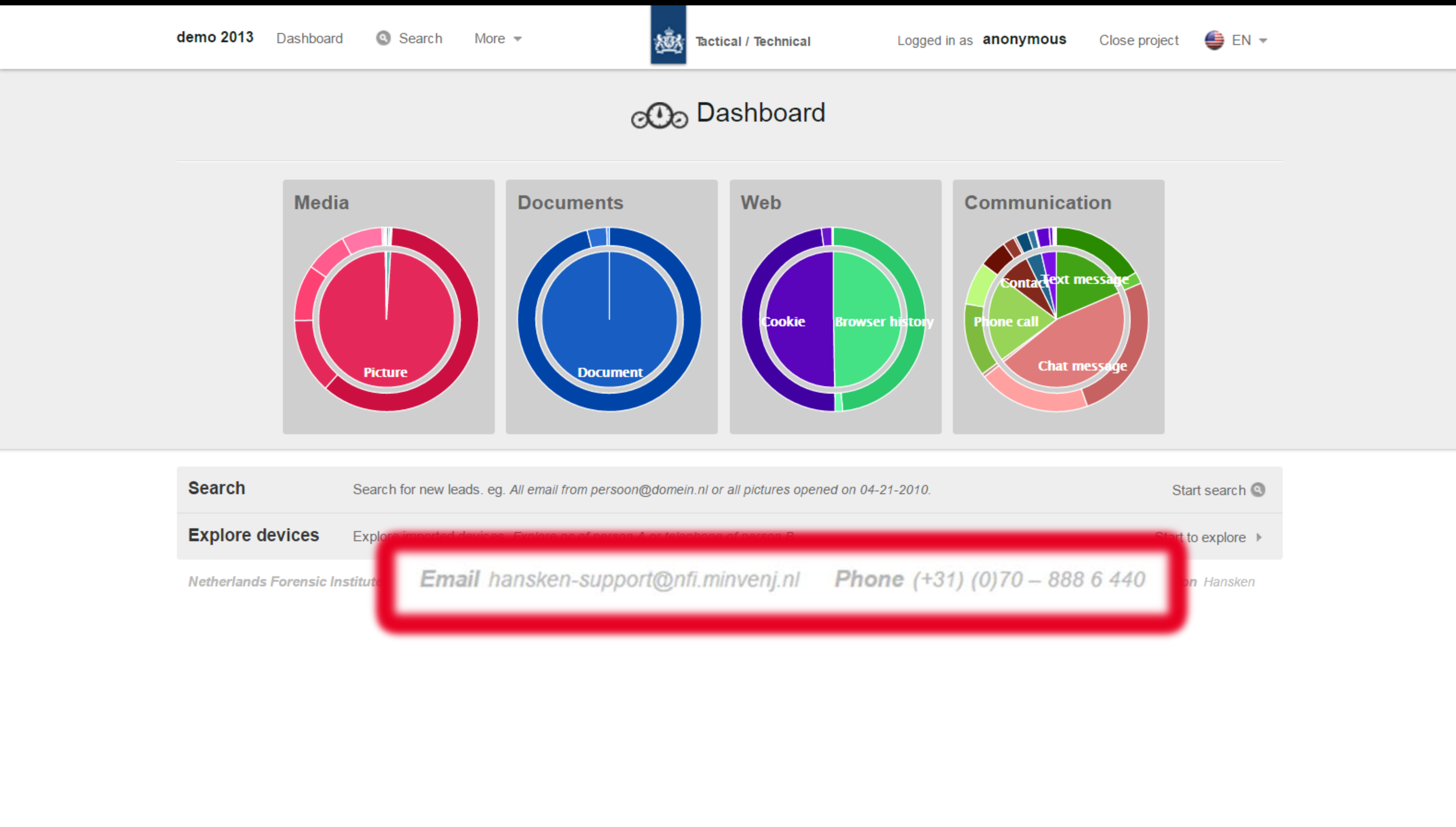


Communication



Search Search for new leads. eg. *All email from persoon@domein.nl or all pictures opened on 04-21-2010.* Start search

Explore devices Explore imported devices. *Explore pc of person A or telephone of person B.* Start to explore



demo 2013
Dashboard
Search
More
Tactical / Technical
Logged in as anonymous
Close project
EN
Dashboard
Media
Picture
Documents
Document
Web
Cookie
Browser history
Communication
Contact
Text message
Phone call
Chat message
Search
Search for new leads. eg. All email from persoon@domein.nl or all pictures opened on 04-21-2010.
Start search
Explore devices
Start to explore
Netherlands Forensic Institut
Email hansken-support@nfi.minvenj.nl
Phone (+31) (0)70 – 888 6 440
Hansken

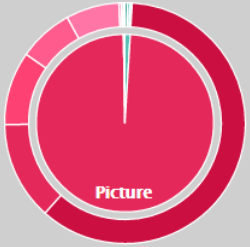
EN

EN

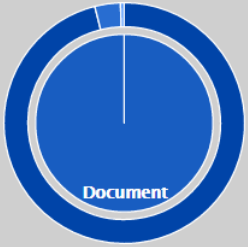
NL

Dashboard

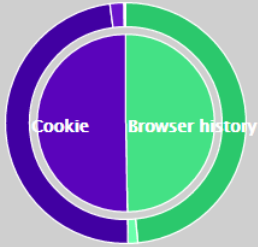
Media



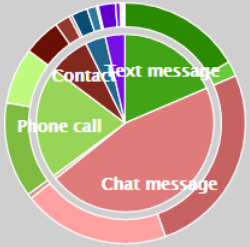
Documents



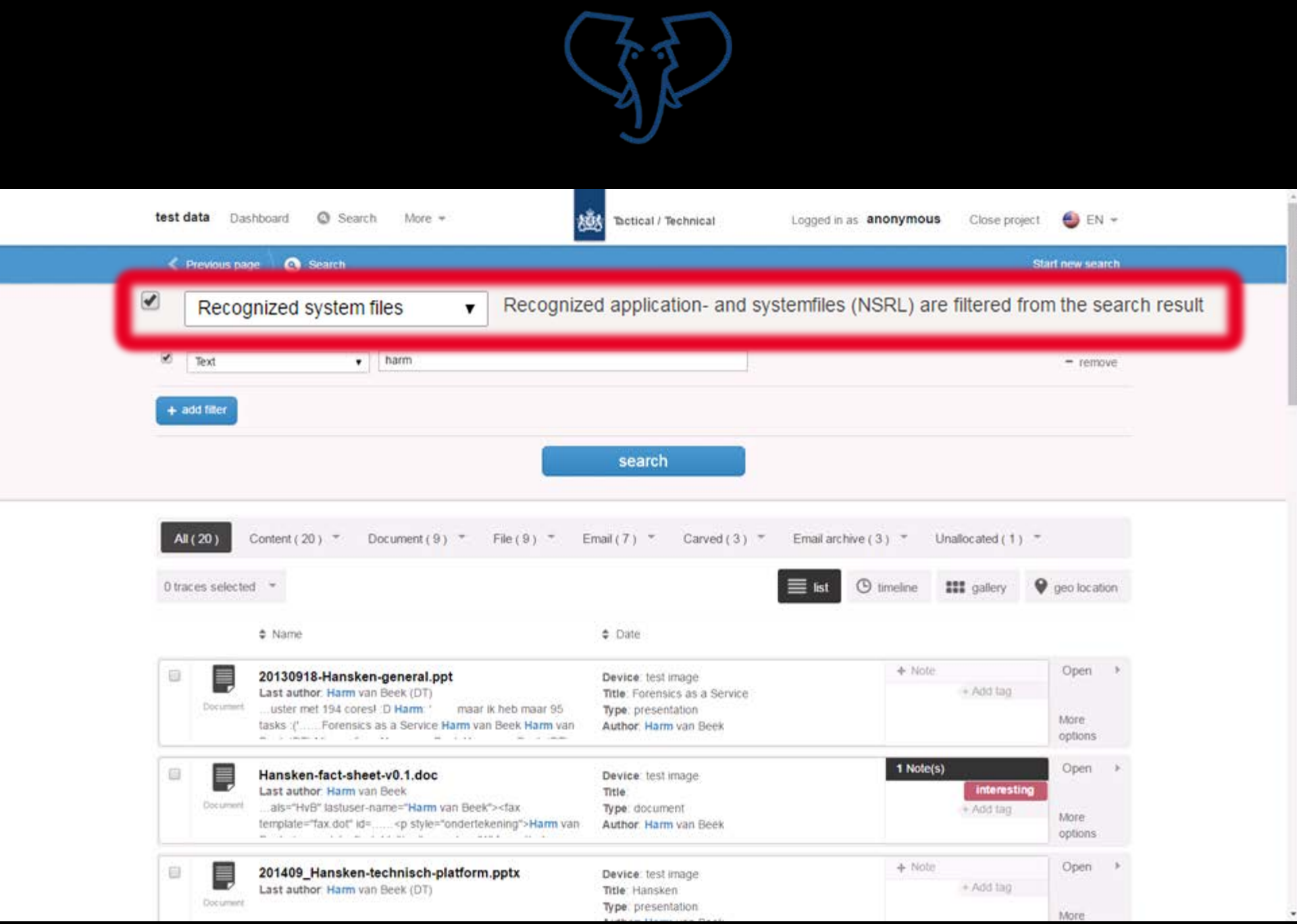
Web

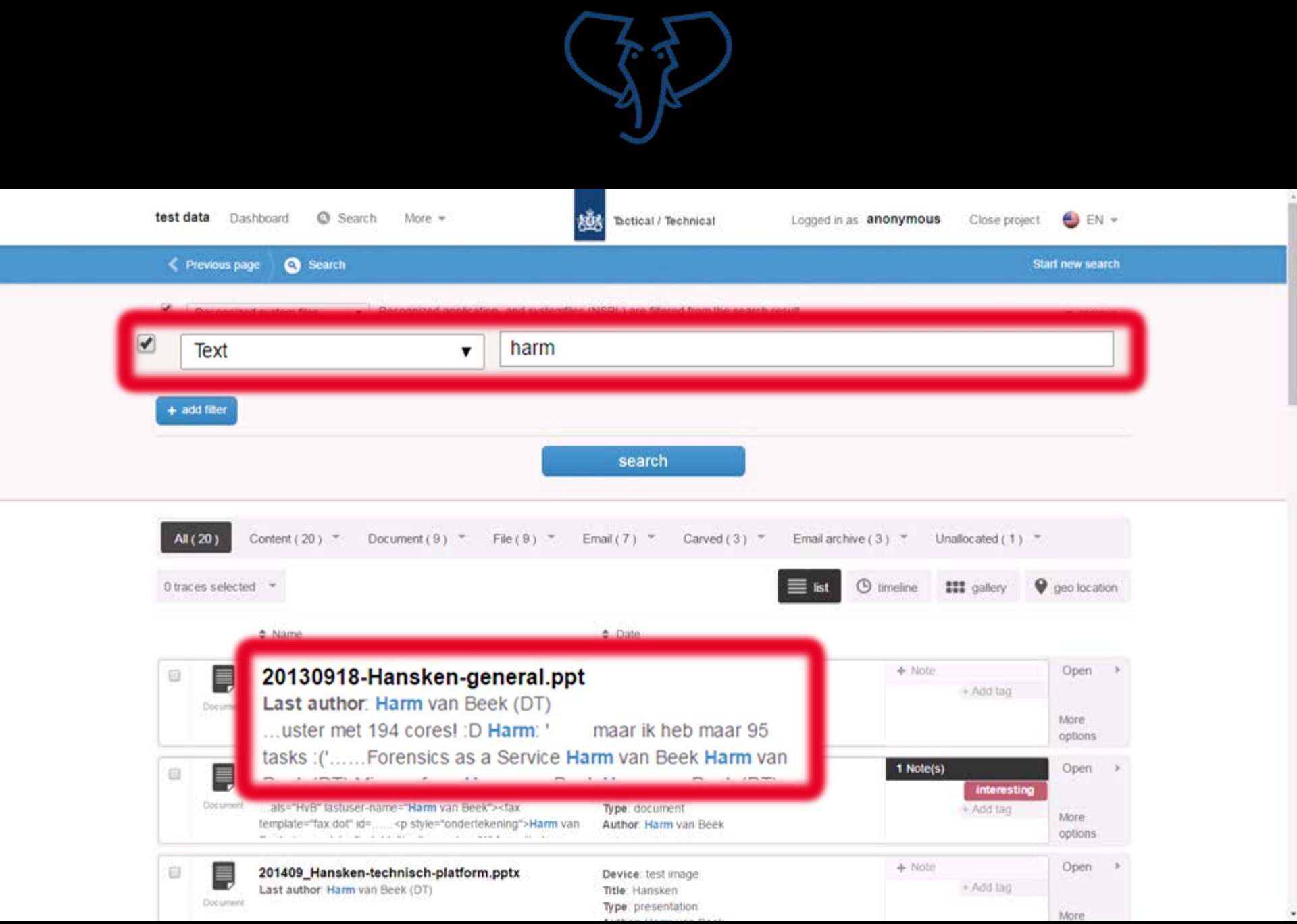


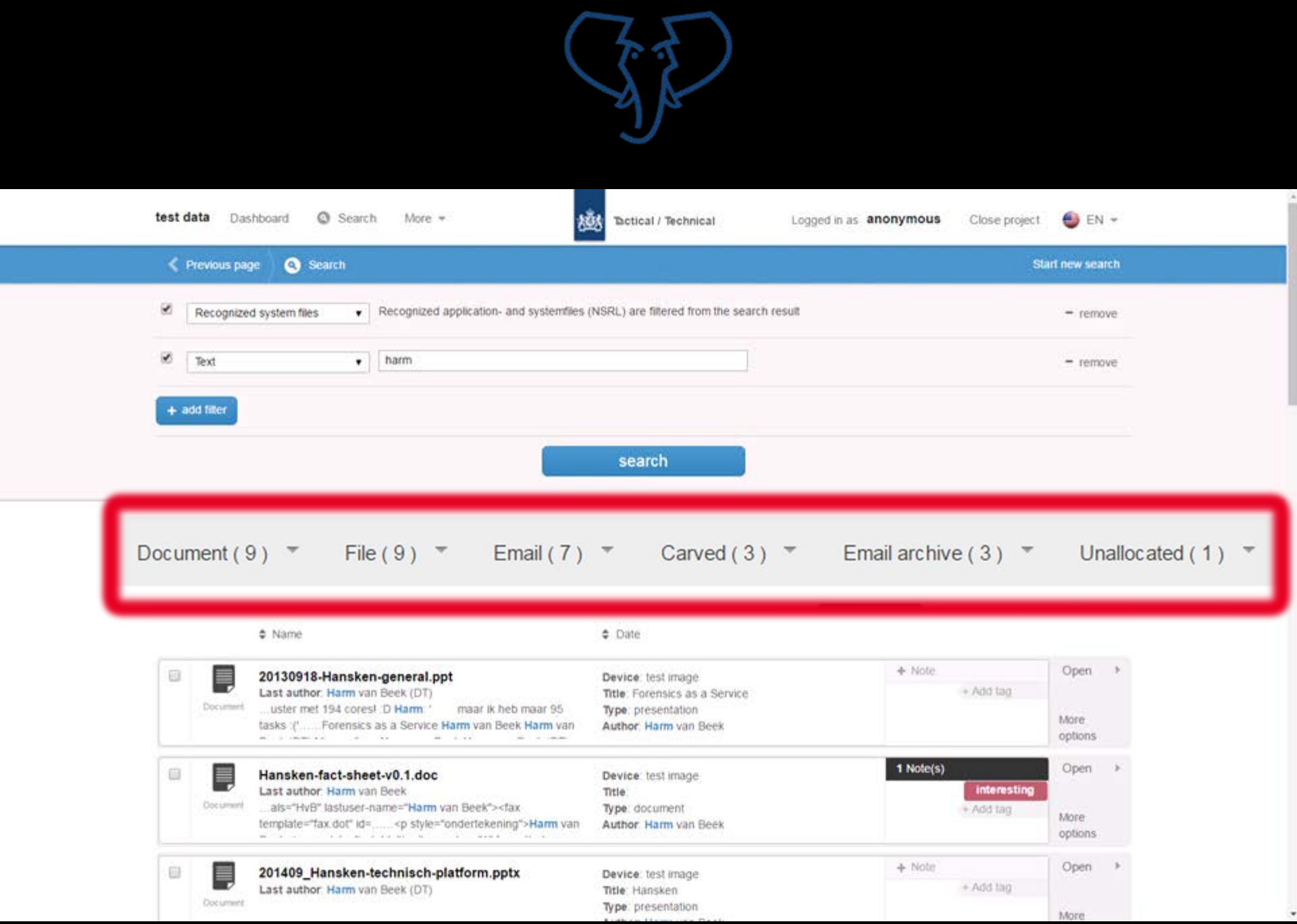
Communication

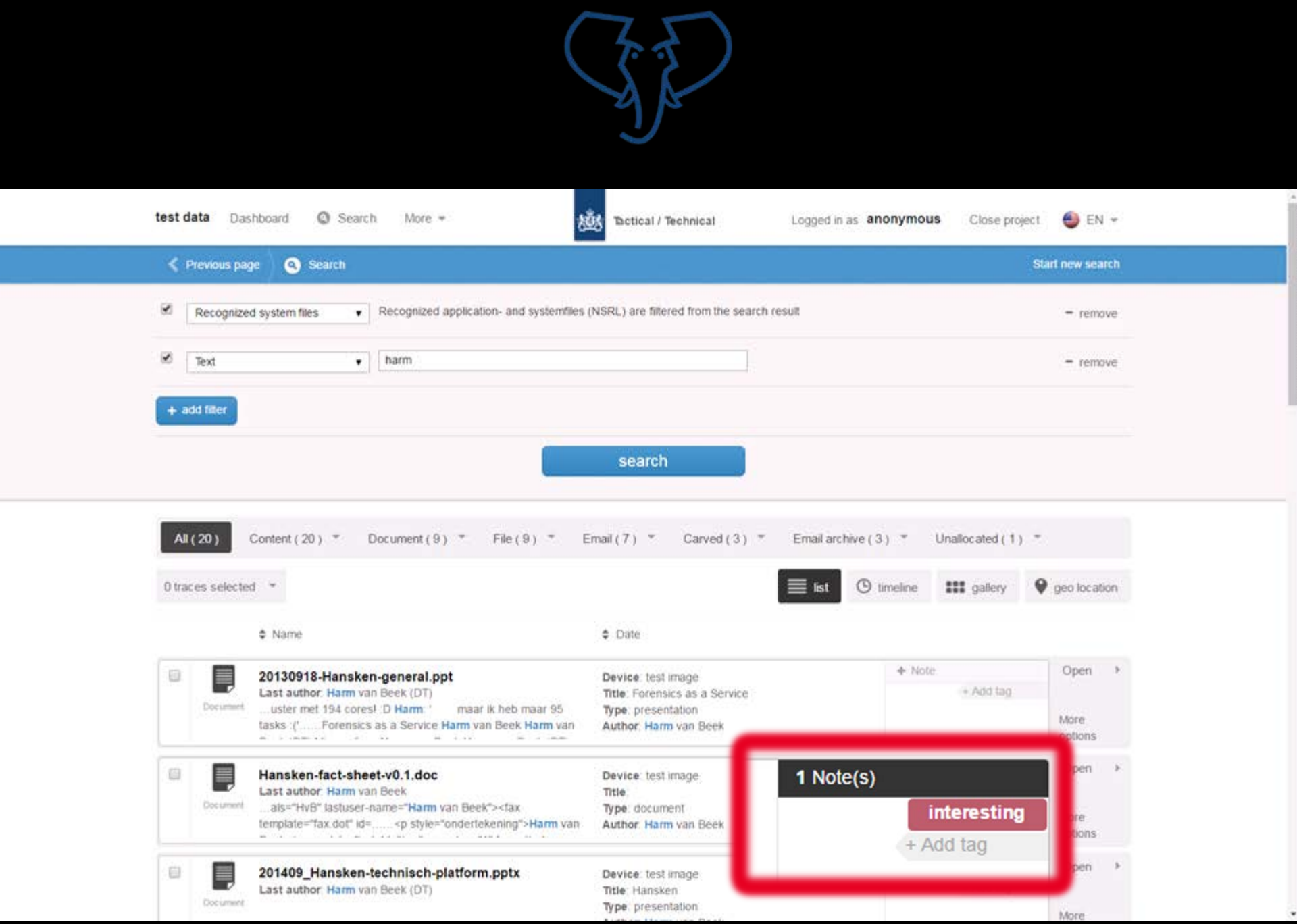


Search	Search for new leads. eg. *All email from persoon@domein.nl or all pictures opened on 04-21-2010.*	Start search
Explore devices	Explore imported devices. *Explore pc of person A or telephone of person B.*	Start to explore


test data
Dashboard
Search
More
Tactical / Technical
Logged in as anonymous
Close project
EN
Previous page
Search
Start new search
Recognized system files
Recognized application- and systemfiles (NSRL) are filtered from the search result
Text
harm
remove
+ add filter
search
All (20)
Content (20)
Document (9)
File (9)
Email (7)
Carved (3)
Email archive (3)
Unallocated (1)
0 traces selected
list
timeline
gallery
geo location
Name
Date
20130918-Hansken-general.ppt
Last author: Harm van Beek (DT)
...uster met 194 cores! :D Harm: ' maar ik heb maar 95 tasks :(' .....Forensics as a Service Harm van Beek Harm van
Device: test image
Title: Forensics as a Service
Type: presentation
Author: Harm van Beek
+ Note
+ Add tag
Open
More options
Hansken-fact-sheet-v0.1.doc
Last author: Harm van Beek
...als="HvB" lastuser-name="Harm van Beek"><fax template="fax.dot" id=.....<p style="ondertekening">Harm van
Device: test image
Title:
Type: document
Author: Harm van Beek
1 Note(s)
interesting
+ Add tag
Open
More options
201409_Hansken-technisch-platform.pptx
Last author: Harm van Beek (DT)
Device: test image
Title: Hansken
Type: presentation
+ Note
+ Add tag
Open
More


test data
Dashboard
Search
More
Tactical / Technical
Logged in as anonymous
Close project
EN
Previous page
Search
Start new search
Text
harm
+ add filter
search
All (20)
Content (20)
Document (9)
File (9)
Email (7)
Carved (3)
Email archive (3)
Unallocated (1)
0 traces selected
list
timeline
gallery
geo location
Name
Date
20130918-Hansken-general.ppt
Last author: Harm van Beek (DT)
...uster met 194 cores! :D Harm: ' maar ik heb maar 95 tasks :('.....Forensics as a Service Harm van Beek Harm van
+ Note
+ Add tag
Open
More options
1 Note(s)
interesting
Type: document
Author: Harm van Beek
201409_Hansken-technisch-platform.pptx
Last author: Harm van Beek (DT)
Device: test image
Title: Hansken
Type: presentation


test data
Dashboard
Search
More
Tactical / Technical
Logged in as anonymous
Close project
EN
Previous page
Search
Start new search
Recognized system files
Recognized application- and systemfiles (NSRL) are filtered from the search result
remove
Text
harm
remove
+ add filter
search
Document (9)
File (9)
Email (7)
Carved (3)
Email archive (3)
Unallocated (1)
Name
Date
20130918-Hansken-general.ppt
Last author: Harm van Beek (DT)
...uster met 194 cores! :D Harm: ' maar ik heb maar 95 tasks :(' .....Forensics as a Service Harm van Beek Harm van
Device: test image
Title: Forensics as a Service
Type: presentation
Author: Harm van Beek
+ Note
+ Add tag
Open
More options
Hansken-fact-sheet-v0.1.doc
Last author: Harm van Beek
...als="HvB" lastuser-name="Harm van Beek"><fax template="fax.dot" id=.....<p style="ondertekening">Harm van
Device: test image
Title:
Type: document
Author: Harm van Beek
1 Note(s)
interesting
+ Add tag
Open
More options
201409_Hansken-technisch-platform.pptx
Last author: Harm van Beek (DT)
Device: test image
Title: Hansken
Type: presentation
+ Note
+ Add tag
Open
More


test data
Dashboard
Search
More
Tactical / Technical
Logged in as anonymous
Close project
EN
Previous page
Search
Start new search
Recognized system files
Recognized application- and systemfiles (NSRL) are filtered from the search result
remove
Text
harm
remove
+ add filter
search
All (20)
Content (20)
Document (9)
File (9)
Email (7)
Carved (3)
Email archive (3)
Unallocated (1)
0 traces selected
list
timeline
gallery
geo location
Name
Date
20130918-Hansken-general.ppt
Last author: Harm van Beek (DT)
...uster met 194 cores! :D Harm: ' maar ik heb maar 95 tasks :(' .....Forensics as a Service Harm van Beek Harm van
Device: test image
Title: Forensics as a Service
Type: presentation
Author: Harm van Beek
+ Note
+ Add tag
Open
More options
Hansken-fact-sheet-v0.1.doc
Last author: Harm van Beek
...als="HvB" lastuser-name="Harm van Beek"><fax template="fax.dot" id=.....<p style="ondertekening">Harm van
Device: test image
Title:
Type: document
Author: Harm van Beek
1 Note(s)
interesting
+ Add tag
201409_Hansken-technisch-platform.pptx
Last author: Harm van Beek (DT)
Device: test image
Title: Hansken
Type: presentation
Document

Windows XP > NTFS; OS/2 IFS > / > Program Files > Bonjour > Bonjour.Resources > ru.lproj >

About Bonjour.rtf

Type: Document

Device: Windows XP
Title:
Type: document
Author: Anna

More ...

+ Note

+ Add tag

Download content of this trace

Generate report

Browse folder

Open in a new window

Start a new search

Name: About Bonjour.rtf

Created: 15-09-2011

Mark trace as potentially confidential

Confirm trace as confidential

Document Viewer Text

1 of 2

Search

О Bonjour

Пакет Bonjour для Windows предоставляет службы Bonjour для автоматического создания IP-сети без конфигурации или специальных серверов, используемые в ОС Windows такими приложениями как iTunes, Safari и Airport-Утилита.

Используя соответствующие промышленным стандартам IP-протоколы, Bonjour позволяет компьютерам, устройствам и службам автоматически обнаруживать друг друга без необходимости ввода IP-адресов или конфигурации серверов DNS. Технология Bonjour исключительно полезна при подключении таких устройств как базовая станция Airport, Apple TV и iPhone.

Требования к системе

Windows XP > NTFS; OS/2 IFS > / > Program Files > Bonjour > Bonjour.Resources > ru.lproj >

About Bonjour.rtf

Type: Document

Device: Windows XP
Title:
Type: document
Author: Anna

More ...

+ Note

+ Add tag

Download content of this trace

Generate report

Browse folder

Open in a new window

Start a new search

Name: About Bonjour.rtf

Created: 15-09-2011

О Bonjour

Пакет Bonjour для Windows предоставляет службы Bonjour для автоматического создания IP-сети без конфигурации или специальных серверов, используемые в ОС Windows такими приложениями как iTunes, Safari и Airport-Утилита.

Используя соответствующие промышленным стандартам IP-протоколы, Bonjour позволяет компьютерам, устройствам и службам автоматически обнаруживать друг друга без необходимости ввода IP-адресов или конфигурации серверов DNS. Технология Bonjour исключительно полезна при подключении таких устройств как базовая станция Airport, Apple TV и iPhone.

Требования к системе

Windows XP > NTFS; OS/2 IFS > / > Program Files > Bonjour > Bonjour.Resources > ru.lproj >

About Bonjour.rtf

Type: Document

Device: Windows XP
Title:
Type: document
Author: Anna

More ...

Download content of this trace
Generate report
Browse folder
Open in a new window

Start a new search
Name: About Bonjour.rtf
Created: 15-09-2011

Mark trace as potentially confidential
Confirm trace as confidential

Document Viewer | Text

1 of 2

Search

О Bonjour

Пакет Bonjour для Windows предоставляет службы Bonjour для автоматического создания IP-сети без конфигурации или специальных серверов, используемые в ОС Windows такими приложениями как iTunes, Safari и Airport-Утилита.

Используя соответствующие промышленным стандартам IP-протоколы, Bonjour позволяет компьютерам, устройствам и службам автоматически обнаруживать друг друга без необходимости ввода IP-адресов или конфигурации серверов DNS. Технология Bonjour исключительно полезна при подключении таких устройств как базовая станция Airport, Apple TV и iPhone.

Требования к системе

Windows XP > NTFS; OS/2 IFS > / > Program Files > Bonjour > Bonjour.Resources > ru.lproj >

About Bonjour.rtf

Type: Document

Device: Windows XP
Title:
Type: document
Author: Anna

More ...

+ Note

+ Add tag

Download content of this trace

Generate report

Browse folder

Open in a new window

Start a new search

Name: About Bonjour.rtf

Created: 15-09-2011

Mark trace as potentially confidential

Document Viewer Text

1 of 2

Search

О Bonjour

Пакет Bonjour для Windows предоставляет службы Bonjour для автоматического создания IP-сети без конфигурации или специальных серверов, используемые в ОС Windows такими приложениями как iTunes, Safari и Airport-Утилита.

Используя соответствующие промышленным стандартам IP-протоколы, Bonjour позволяет компьютерам, устройствам и службам автоматически обнаруживать друг друга без необходимости ввода IP-адресов или конфигурации серверов DNS. Технология Bonjour исключительно полезна при подключении таких устройств как базовая станция Airport, Apple TV и iPhone.

Требования к системе

demo 2013 Dashboard Search More Tactical / Technical Logged in as anonymous Close project EN

Previous page About Bonjour.rtf Start new search

Windows XP > NTFS; OS/2 IFS > / > Program Files > Bonjour > Bonjour.Resources > ru.lproj >

About Bonjour.rtf

Type: Document

Device: Windows XP
Title:
Type: document
Author: Anna

More ...

+ Note

+ Add tag

Generate report

Open in a new window

Start a new search

Name: About Bonjour.rtf

Created: 15-09-2011

Mark trace as potentially confidential

Confirm trace as confidential

Document Viewer Text

1 of 2

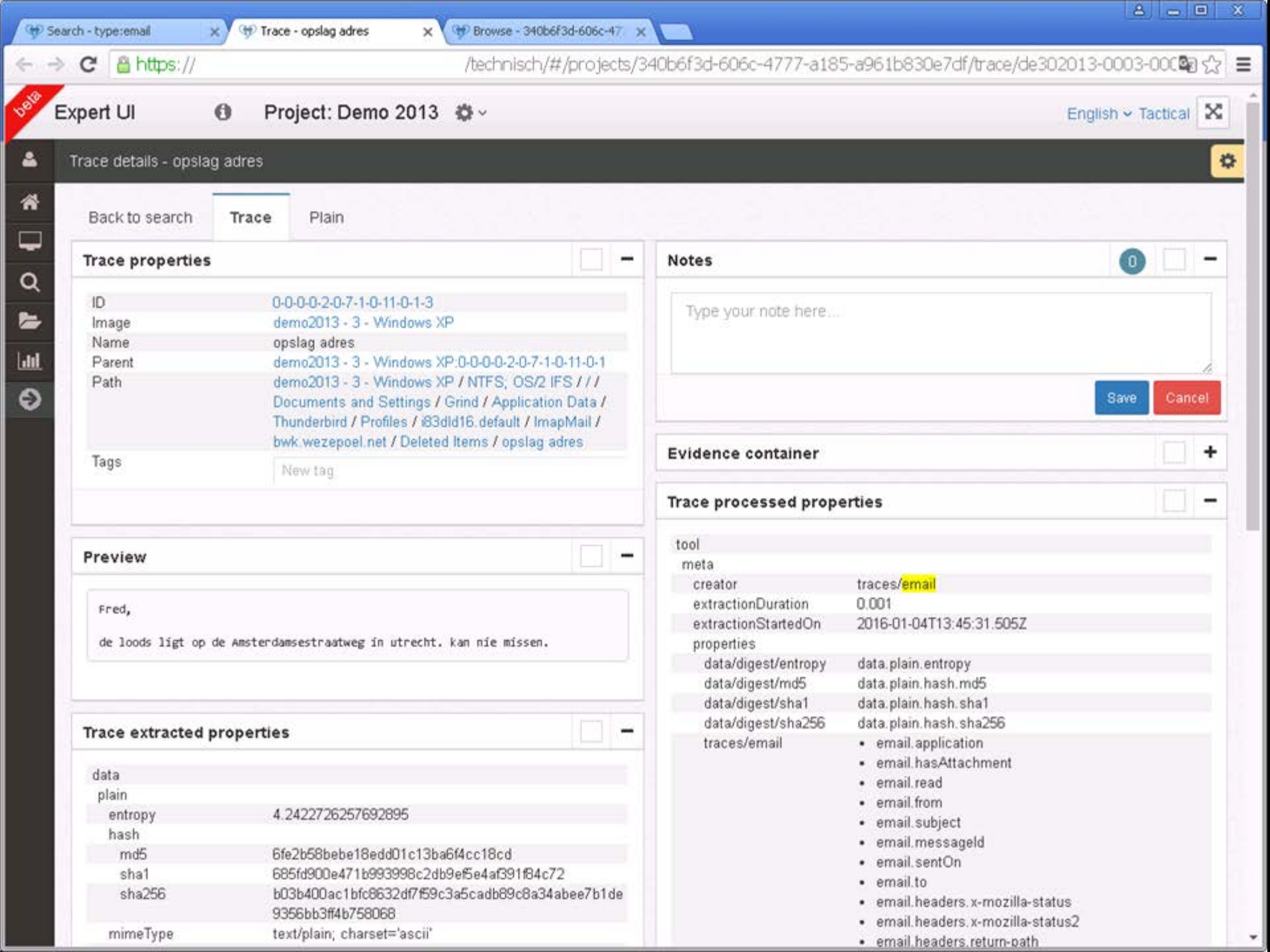
Search

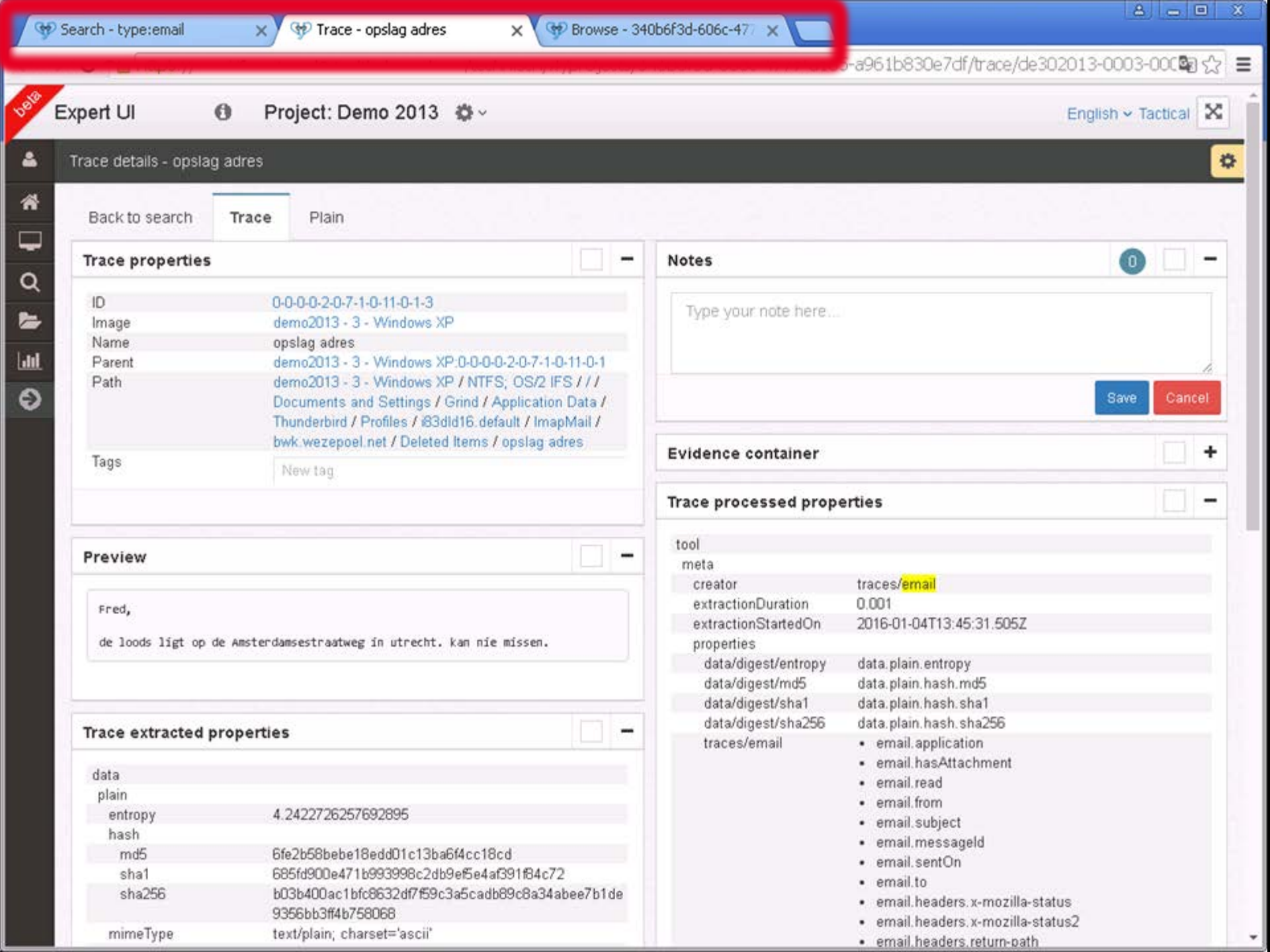
О Bonjour

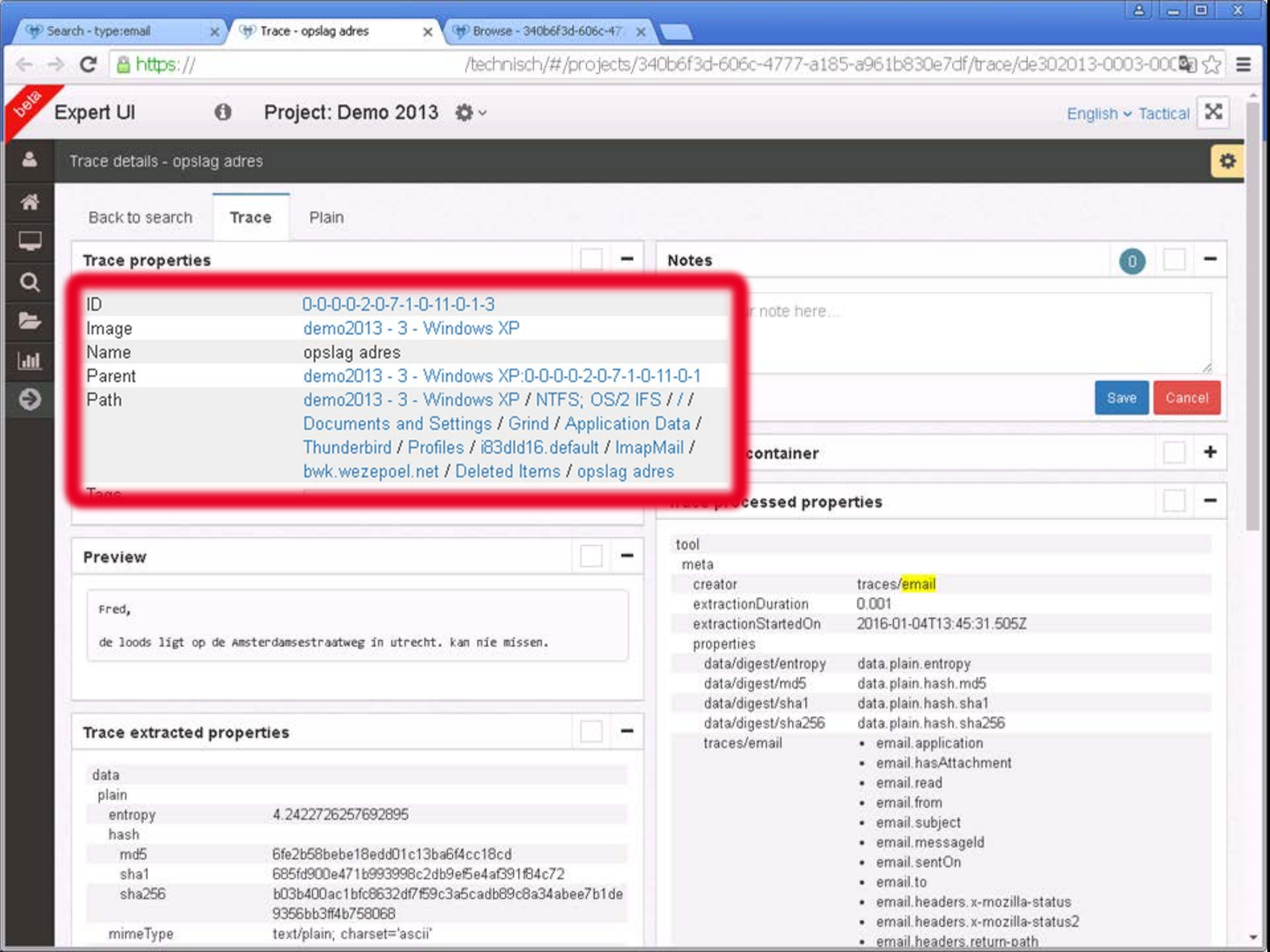
Пакет Bonjour для Windows предоставляет службы Bonjour для автоматического создания IP-сети без конфигурации или специальных серверов, используемые в ОС Windows такими приложениями как iTunes, Safari и Airport-Утилита.

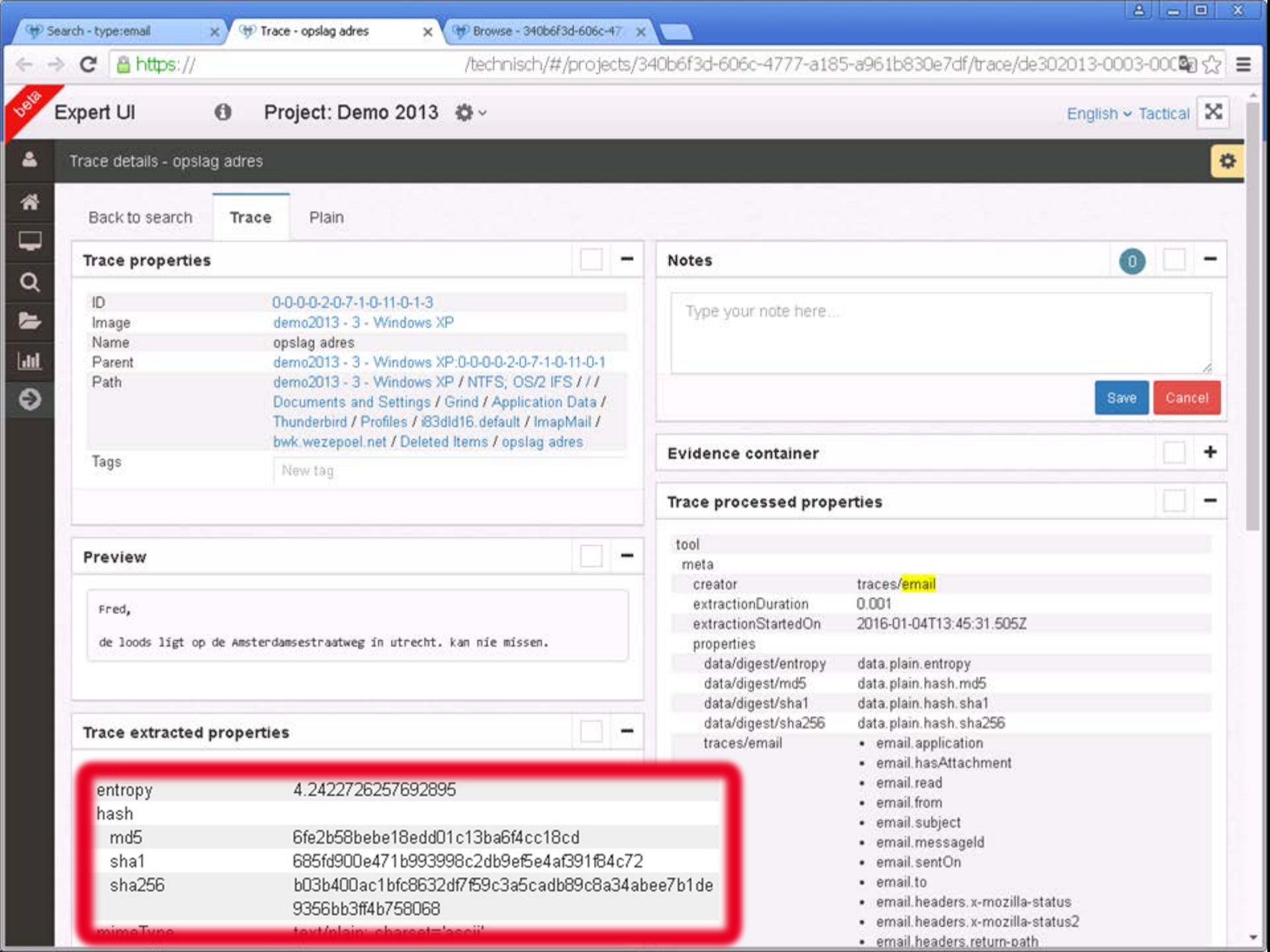
Используя соответствующие промышленным стандартам IP-протоколы, Bonjour позволяет компьютерам, устройствам и службам автоматически обнаруживать друг друга без необходимости ввода IP-адресов или конфигурации серверов DNS. Технология Bonjour исключительно полезна при подключении таких устройств как базовая станция Airport, Apple TV и iPhone.

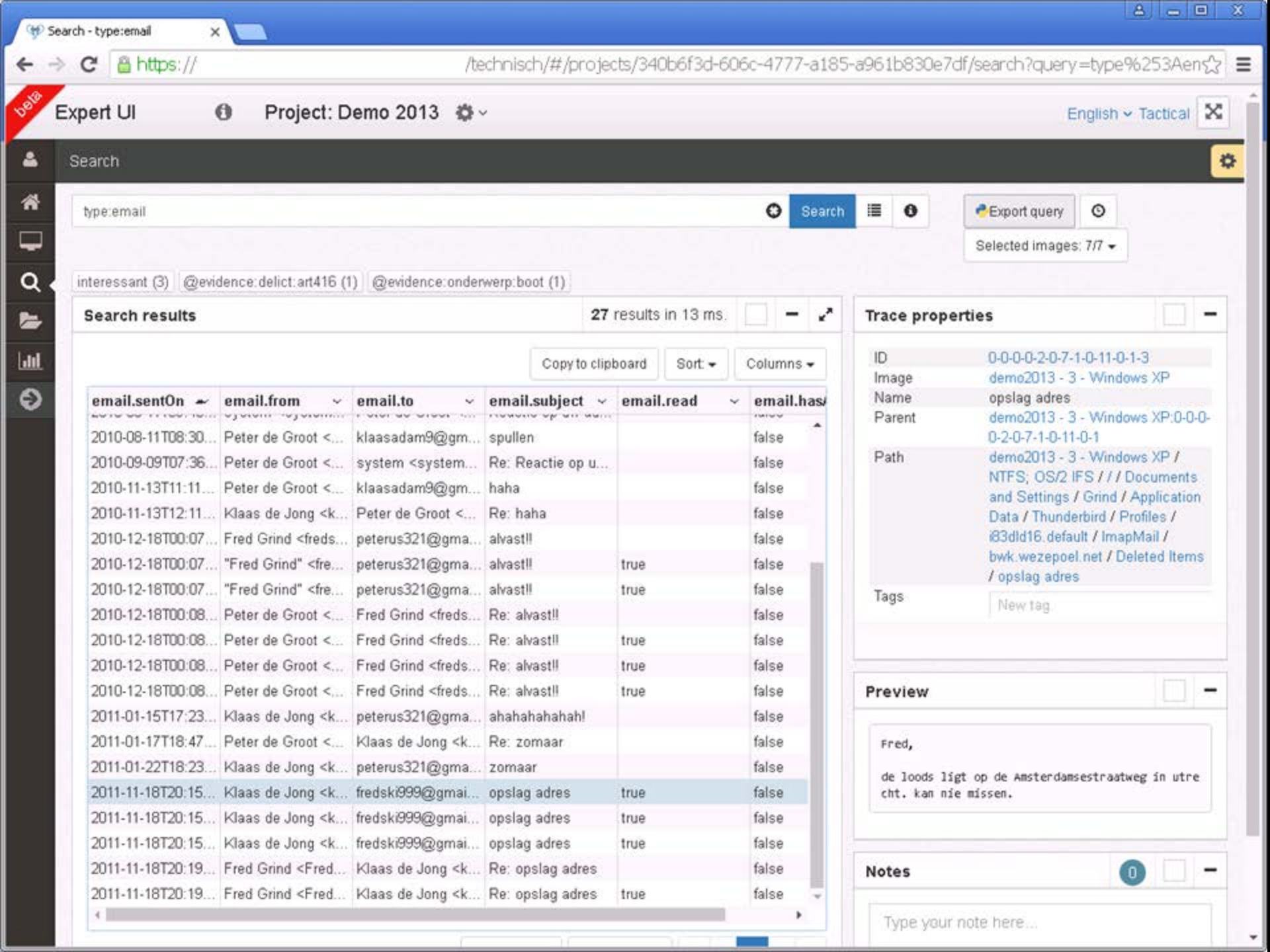
Требования к системе

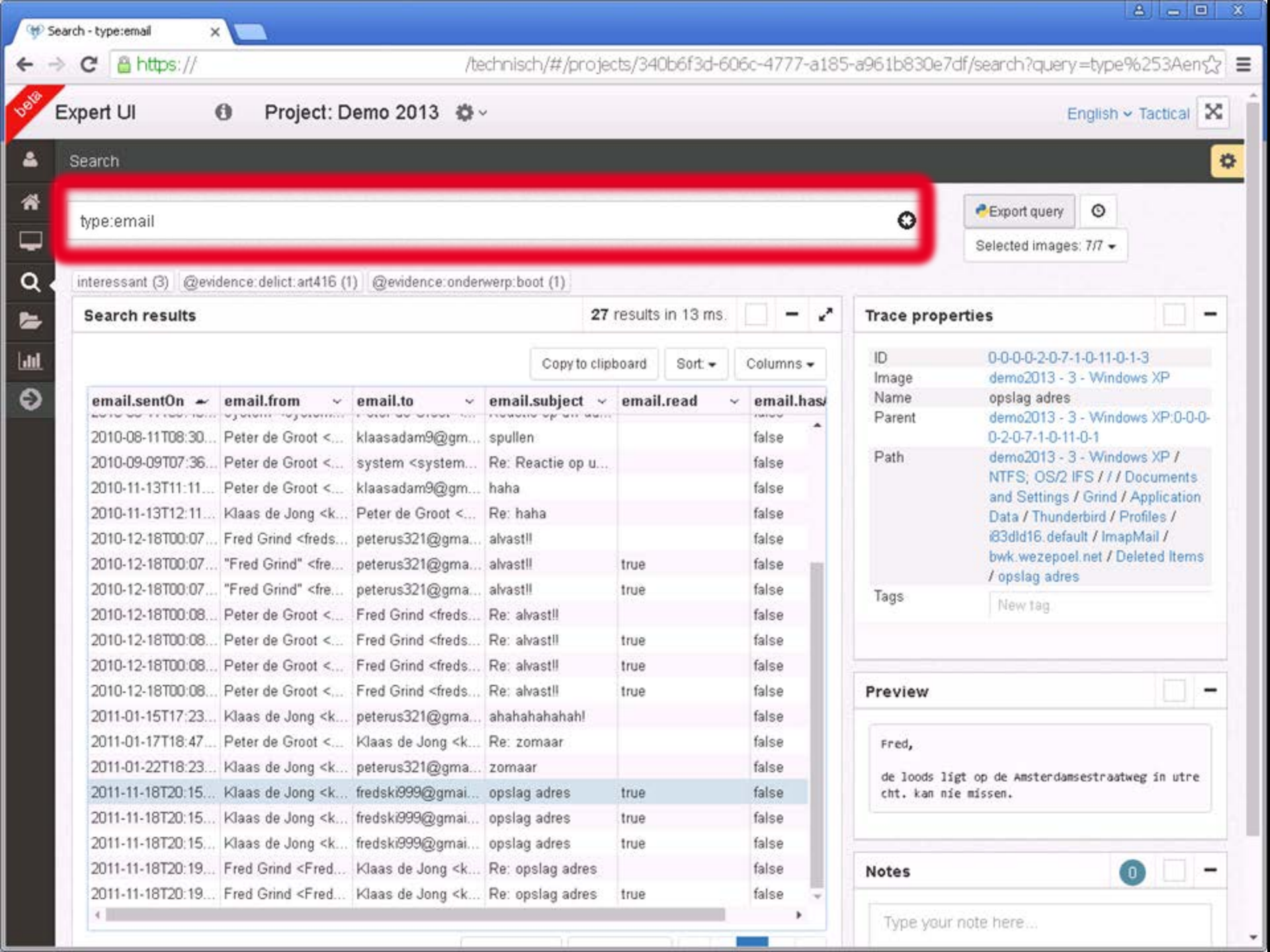

Search - type:email
Trace - opslag adres
Browse - 340b6f3d-606c-47
https://
/technisch/#/projects/340b6f3d-606c-4777-a185-a961b830e7df/trace/de302013-0003-000
beta
Expert UI
Project: Demo 2013
English
Tactical
Trace details - opslag adres
Back to search
Trace
Plain
Trace properties
ID 0-0-0-0-2-0-7-1-0-11-0-1-3
Image demo2013 - 3 - Windows XP
Name opslag adres
Parent demo2013 - 3 - Windows XP:0-0-0-0-2-0-7-1-0-11-0-1
Path demo2013 - 3 - Windows XP / NTFS; OS/2 IFS / / / Documents and Settings / Grind / Application Data / Thunderbird / Profiles / i83dld16.default / ImapMail / bwk.wezepoel.net / Deleted Items / opslag adres
Tags
New tag
Preview
Fred,
de loods ligt op de Amsterdamsestraatweg in utrecht. kan nie missen.
Trace extracted properties
data
plain
entropy 4.2422726257692895
hash
md5 6fe2b58bebe18edd01c13ba6f4cc18cd
sha1 685fd900e471b993998c2db9ef5e4af391f84c72
sha256 b03b400ac1bfc8632df7f59c3a5cadb89c8a34abee7b1de9356bb3ff4b758068
mimeType text/plain; charset='ascii'
Notes
0
Type your note here...
Save
Cancel
Evidence container
Trace processed properties
tool
meta
creator traces/email
extractionDuration 0.001
extractionStartedOn 2016-01-04T13:45:31.505Z
properties
data/digest/entropy data.plain.entropy
data/digest/md5 data.plain.hash.md5
data/digest/sha1 data.plain.hash.sha1
data/digest/sha256 data.plain.hash.sha256
traces/email
email.application
email.hasAttachment
email.read
email.from
email.subject
email.messageId
email.sentOn
email.to
email.headers.x-mozilla-status
email.headers.x-mozilla-status2
email.headers.return-path

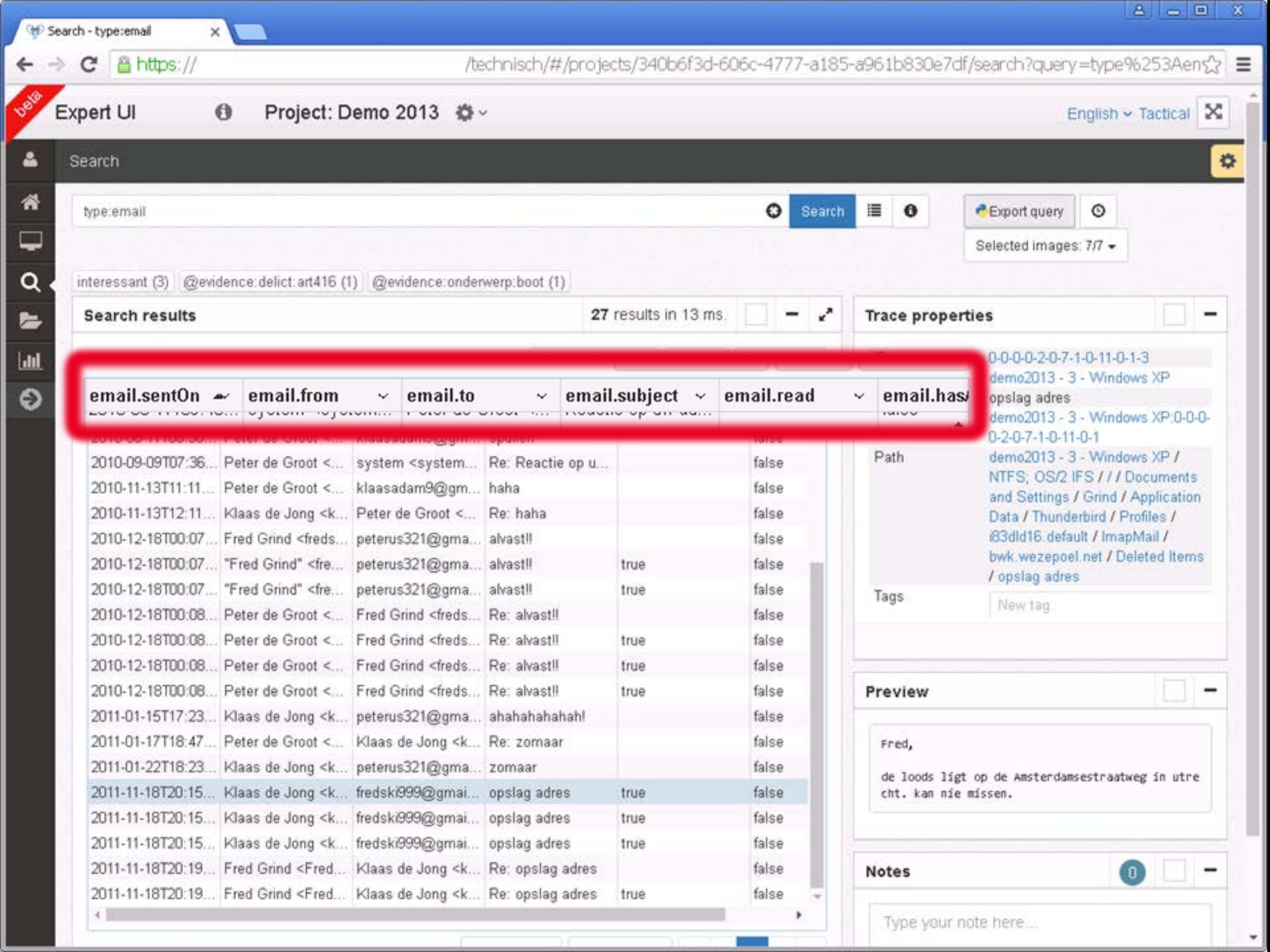

Search - type:email
Trace - opslag adres
Browse - 340b6f3d-606c-47
beta
Expert UI
Project: Demo 2013
English
Tactical
Trace details - opslag adres
Back to search
Trace
Plain
Trace properties
ID 0-0-0-0-2-0-7-1-0-11-0-1-3
Image demo2013 - 3 - Windows XP
Name opslag adres
Parent demo2013 - 3 - Windows XP:0-0-0-0-2-0-7-1-0-11-0-1
Path demo2013 - 3 - Windows XP / NTFS; OS/2 IFS / / / Documents and Settings / Grind / Application Data / Thunderbird / Profiles / i83dld16.default / ImapMail / bwk.wezepoel.net / Deleted Items / opslag adres
Tags
New tag
Preview
Fred,
de loods ligt op de Amsterdamsestraatweg in utrecht. kan nie missen.
Trace extracted properties
data
plain
entropy 4.2422726257692895
hash
md5 6fe2b58bebe18edd01c13ba6f4cc18cd
sha1 685fd900e471b993998c2db9ef5e4af391f84c72
sha256 b03b400ac1bfc8632df7f59c3a5cadb89c8a34abee7b1de9356bb3ff4b758068
mimeType text/plain; charset='ascii'
Notes
0
Type your note here...
Save
Cancel
Evidence container
Trace processed properties
tool
meta
creator traces/email
extractionDuration 0.001
extractionStartedOn 2016-01-04T13:45:31.505Z
properties
data/digest/entropy data.plain.entropy
data/digest/md5 data.plain.hash.md5
data/digest/sha1 data.plain.hash.sha1
data/digest/sha256 data.plain.hash.sha256
traces/email
email.application
email.hasAttachment
email.read
email.from
email.subject
email.messageId
email.sentOn
email.to
email.headers.x-mozilla-status
email.headers.x-mozilla-status2
email.headers.return-path

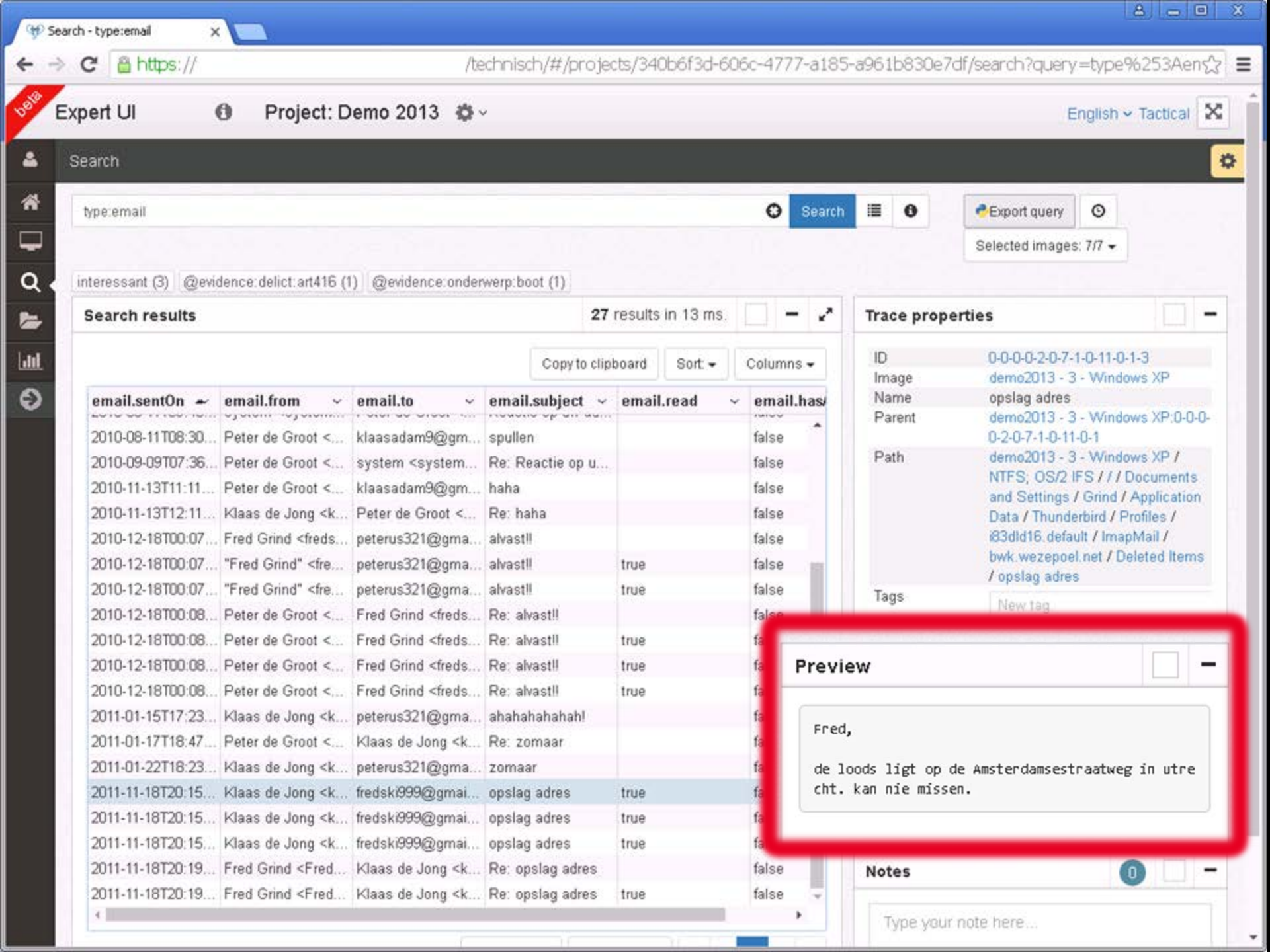

Search - type:email
Trace - opslag adres
Browse - 340b6f3d-606c-47
https://
/technisch/#/projects/340b6f3d-606c-4777-a185-a961b830e7df/trace/de302013-0003-000
beta
Expert UI
Project: Demo 2013
English
Tactical
Trace details - opslag adres
Back to search
Trace
Plain
Trace properties
ID 0-0-0-0-2-0-7-1-0-11-0-1-3
Image demo2013 - 3 - Windows XP
Name opslag adres
Parent demo2013 - 3 - Windows XP:0-0-0-0-2-0-7-1-0-11-0-1
Path demo2013 - 3 - Windows XP / NTFS; OS/2 IFS / / / Documents and Settings / Grind / Application Data / Thunderbird / Profiles / i83dld16.default / ImapMail / bwk.wezepoel.net / Deleted Items / opslag adres
Notes
0
r note here...
Save
Cancel
container
cessed properties
Preview
Fred,
de loods ligt op de Amsterdamsestraatweg in utrecht. kan nie missen.
Trace extracted properties
data
plain
entropy 4.2422726257692895
hash
md5 6fe2b58bebe18edd01c13ba6f4cc18cd
sha1 685fd900e471b993998c2db9ef5e4af391f84c72
sha256 b03b400ac1bfc8632df7f59c3a5cadb89c8a34abee7b1de9356bb3ff4b758068
mimeType text/plain; charset='ascii'
tool
meta
creator traces/email
extractionDuration 0.001
extractionStartedOn 2016-01-04T13:45:31.505Z
properties
data/digest/entropy data.plain.entropy
data/digest/md5 data.plain.hash.md5
data/digest/sha1 data.plain.hash.sha1
data/digest/sha256 data.plain.hash.sha256
traces/email
email.application
email.hasAttachment
email.read
email.from
email.subject
email.messageId
email.sentOn
email.to
email.headers.x-mozilla-status
email.headers.x-mozilla-status2
email.headers.return-path

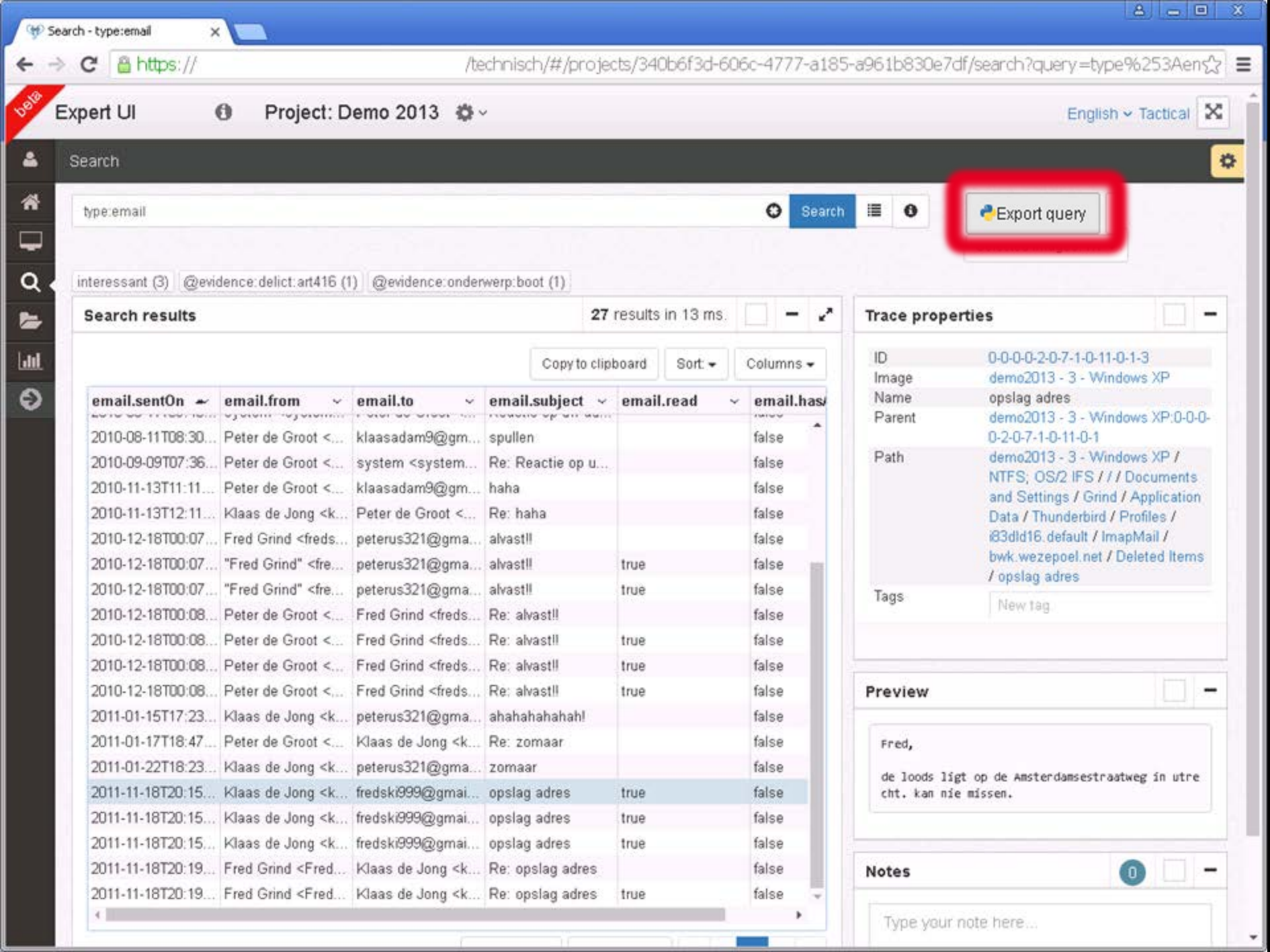

Search - type:email
Trace - opslag adres
Browse - 340b6f3d-606c-47
https://
/technisch/#/projects/340b6f3d-606c-4777-a185-a961b830e7df/trace/de302013-0003-000
beta
Expert UI
Project: Demo 2013
English
Tactical
Trace details - opslag adres
Back to search
Trace
Plain
Trace properties
ID 0-0-0-0-2-0-7-1-0-11-0-1-3
Image demo2013 - 3 - Windows XP
Name opslag adres
Parent demo2013 - 3 - Windows XP:0-0-0-0-2-0-7-1-0-11-0-1
Path demo2013 - 3 - Windows XP / NTFS; OS/2 IFS / / / Documents and Settings / Grind / Application Data / Thunderbird / Profiles / i83dld16.default / ImapMail / bwk.wezepoel.net / Deleted Items / opslag adres
Tags
New tag
Notes
0
Type your note here...
Save
Cancel
Evidence container
Trace processed properties
tool
meta
creator traces/email
extractionDuration 0.001
extractionStartedOn 2016-01-04T13:45:31.505Z
properties
data/digest/entropy data.plain.entropy
data/digest/md5 data.plain.hash.md5
data/digest/sha1 data.plain.hash.sha1
data/digest/sha256 data.plain.hash.sha256
traces/email
email.application
email.hasAttachment
email.read
email.from
email.subject
email.messageId
email.sentOn
email.to
email.headers.x-mozilla-status
email.headers.x-mozilla-status2
email.headers.return-path
Preview
Fred,
de loods ligt op de Amsterdamsestraatweg in utrecht. kan nie missen.
Trace extracted properties
entropy 4.2422726257692895
hash
md5 6fe2b58bebe18edd01c13ba6f4cc18cd
sha1 685fd900e471b993998c2db9ef5e4af391f84c72
sha256 b03b400ac1bfc8632df7f59c3a5cadb89c8a34abee7b1de9356bb3ff4b758068

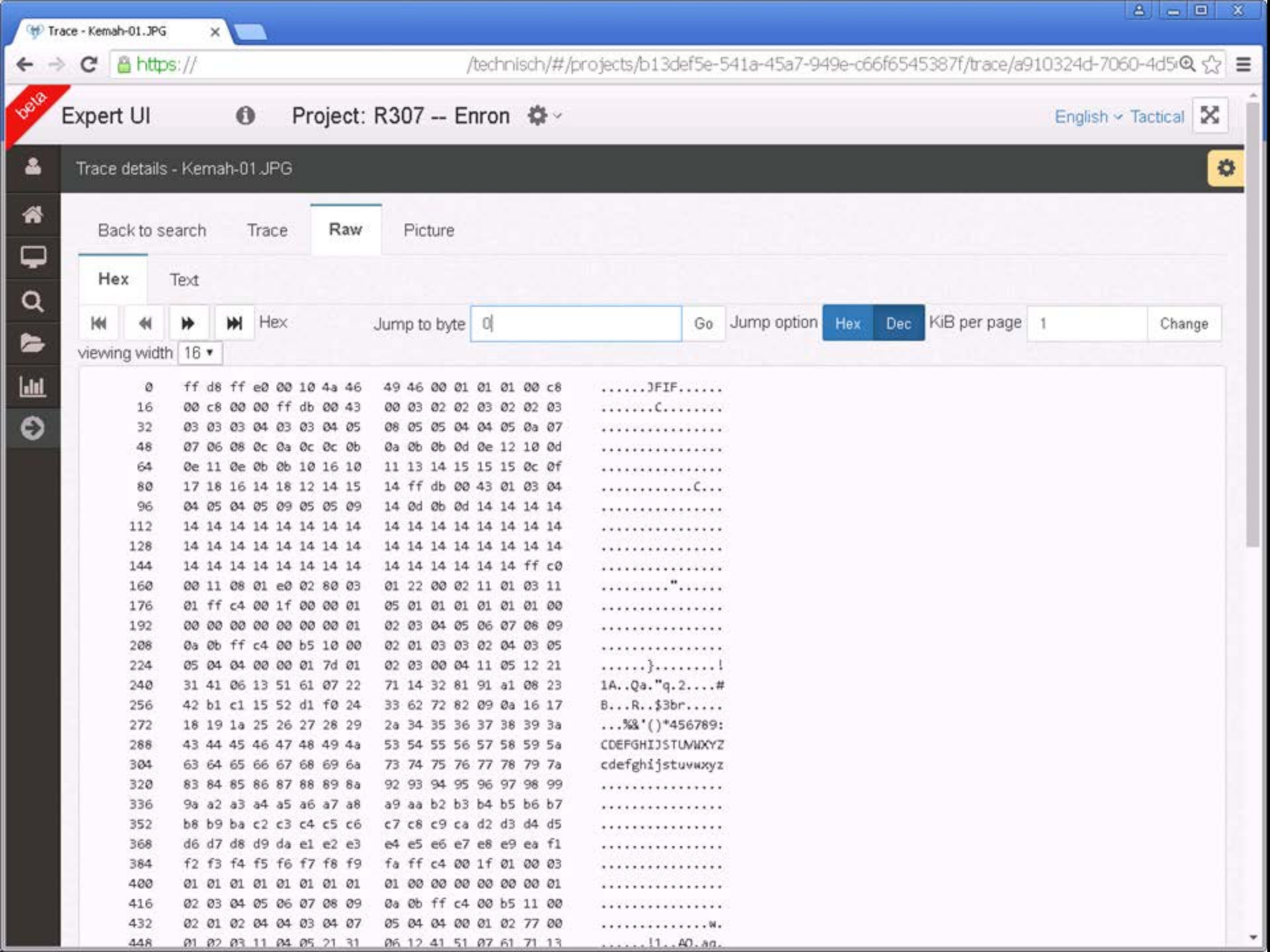

Search - type:email
https://
/technisch/#/projects/340b6f3d-606c-4777-a185-a961b830e7df/search?query=type%253Aem
beta
Expert UI
Project: Demo 2013
English
Tactical
Search
type:email
Search
Export query
Selected images: 7/7
interessant (3)
@evidence:delict:art416 (1)
@evidence:onderwerp:boot (1)
Search results
27 results in 13 ms.
Copy to clipboard
Sort:
Columns
email.sentOn
email.from
email.to
email.subject
email.read
email.has
2010-08-11T08:30... Peter de Groot <... klaasadam9@gm... spullen false
2010-09-09T07:36... Peter de Groot <... system <system... Re: Reactie op u... false
2010-11-13T11:11... Peter de Groot <... klaasadam9@gm... haha false
2010-11-13T12:11... Klaas de Jong <k... Peter de Groot <... Re: haha false
2010-12-18T00:07... Fred Grind <freds... peterus321@gma... alvast!! false
2010-12-18T00:07... "Fred Grind" <fre... peterus321@gma... alvast!! true false
2010-12-18T00:07... "Fred Grind" <fre... peterus321@gma... alvast!! true false
2010-12-18T00:08... Peter de Groot <... Fred Grind <freds... Re: alvast!! false
2010-12-18T00:08... Peter de Groot <... Fred Grind <freds... Re: alvast!! true false
2010-12-18T00:08... Peter de Groot <... Fred Grind <freds... Re: alvast!! true false
2010-12-18T00:08... Peter de Groot <... Fred Grind <freds... Re: alvast!! true false
2011-01-15T17:23... Klaas de Jong <k... peterus321@gma... ahahahahahah! false
2011-01-17T18:47... Peter de Groot <... Klaas de Jong <k... Re: zomaar false
2011-01-22T18:23... Klaas de Jong <k... peterus321@gma... zomaar false
2011-11-18T20:15... Klaas de Jong <k... fredski999@gmai... opslag adres true false
2011-11-18T20:15... Klaas de Jong <k... fredski999@gmai... opslag adres true false
2011-11-18T20:15... Klaas de Jong <k... fredski999@gmai... opslag adres true false
2011-11-18T20:19... Fred Grind <Fred... Klaas de Jong <k... Re: opslag adres false
2011-11-18T20:19... Fred Grind <Fred... Klaas de Jong <k... Re: opslag adres true false
Trace properties
ID 0-0-0-0-2-0-7-1-0-11-0-1-3
Image demo2013 - 3 - Windows XP
Name opslag adres
Parent demo2013 - 3 - Windows XP:0-0-0-0-2-0-7-1-0-11-0-1
Path demo2013 - 3 - Windows XP / NTFS; OS/2 IFS / / / Documents and Settings / Grind / Application Data / Thunderbird / Profiles / i83dld16.default / ImapMail / bwk.wezepoel.net / Deleted Items / opslag adres
Tags
New tag
Preview
Fred,
de loods ligt op de Amsterdamsestraatweg in utrecht. kan nie missen.
Notes
0
Type your note here...

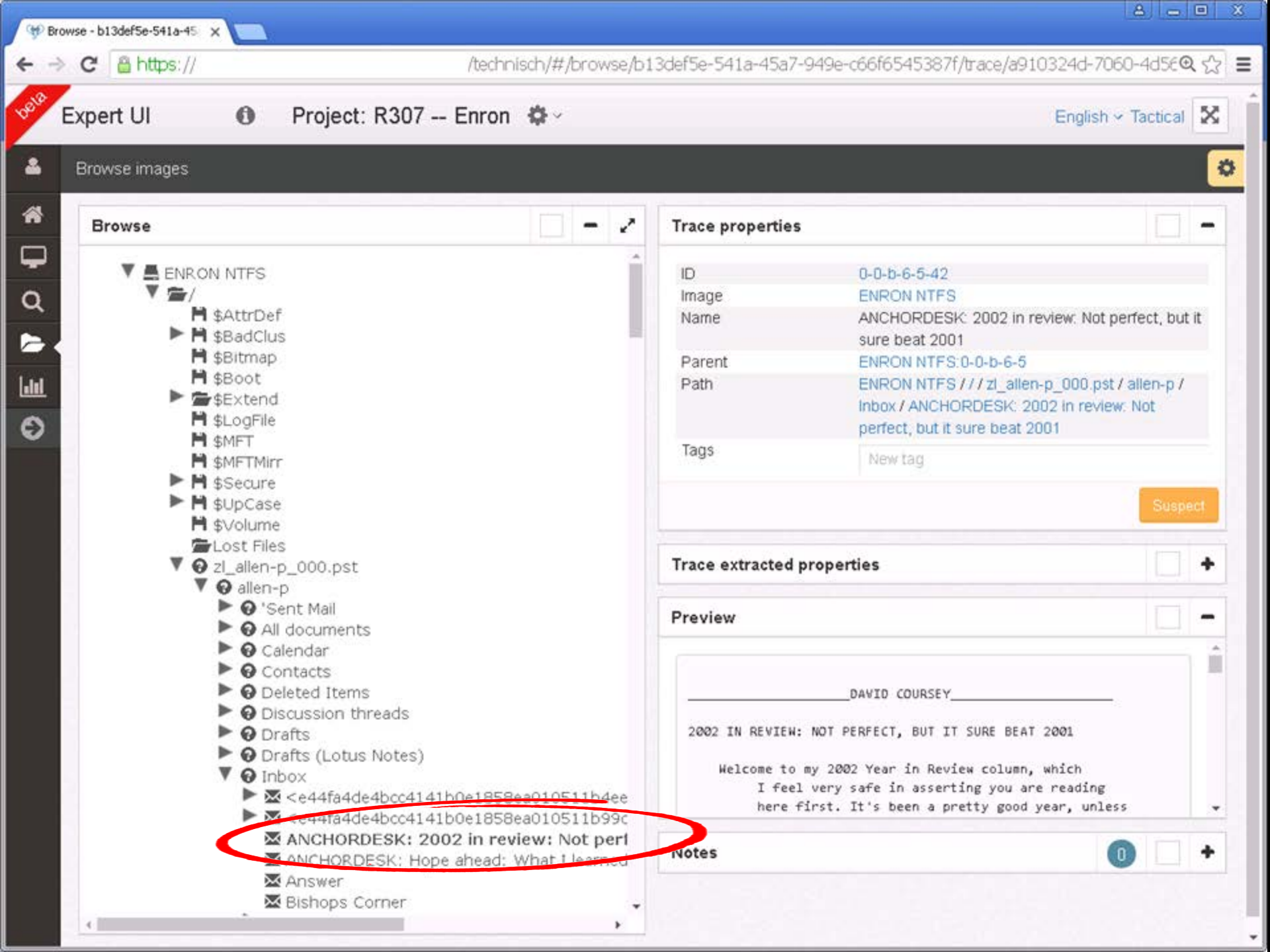

Search - type:email
https://
/technisch/#/projects/340b6f3d-606c-4777-a185-a961b830e7df/search?query=type%253Aem
beta
Expert UI
Project: Demo 2013
English
Tactical
Search
type:email
Export query
Selected images: 7/7
interessant (3)
@evidence:delict:art416 (1)
@evidence:onderwerp:boot (1)
Search results
27 results in 13 ms.
Copy to clipboard
Sort:
Columns
email.sentOn
email.from
email.to
email.subject
email.read
email.has
2010-08-11T08:30... Peter de Groot <... klaasadam9@gm... spullen false
2010-09-09T07:36... Peter de Groot <... system <system... Re: Reactie op u... false
2010-11-13T11:11... Peter de Groot <... klaasadam9@gm... haha false
2010-11-13T12:11... Klaas de Jong <k... Peter de Groot <... Re: haha false
2010-12-18T00:07... Fred Grind <freds... peterus321@gma... alvast!! false
2010-12-18T00:07... "Fred Grind" <fre... peterus321@gma... alvast!! true false
2010-12-18T00:07... "Fred Grind" <fre... peterus321@gma... alvast!! true false
2010-12-18T00:08... Peter de Groot <... Fred Grind <freds... Re: alvast!! false
2010-12-18T00:08... Peter de Groot <... Fred Grind <freds... Re: alvast!! true false
2010-12-18T00:08... Peter de Groot <... Fred Grind <freds... Re: alvast!! true false
2010-12-18T00:08... Peter de Groot <... Fred Grind <freds... Re: alvast!! true false
2011-01-15T17:23... Klaas de Jong <k... peterus321@gma... ahahahahahah! false
2011-01-17T18:47... Peter de Groot <... Klaas de Jong <k... Re: zomaar false
2011-01-22T18:23... Klaas de Jong <k... peterus321@gma... zomaar false
2011-11-18T20:15... Klaas de Jong <k... fredski999@gmai... opslag adres true false
2011-11-18T20:15... Klaas de Jong <k... fredski999@gmai... opslag adres true false
2011-11-18T20:15... Klaas de Jong <k... fredski999@gmai... opslag adres true false
2011-11-18T20:19... Fred Grind <Fred... Klaas de Jong <k... Re: opslag adres false
2011-11-18T20:19... Fred Grind <Fred... Klaas de Jong <k... Re: opslag adres true false
Trace properties
ID 0-0-0-0-2-0-7-1-0-11-0-1-3
Image demo2013 - 3 - Windows XP
Name opslag adres
Parent demo2013 - 3 - Windows XP:0-0-0-0-2-0-7-1-0-11-0-1
Path demo2013 - 3 - Windows XP / NTFS; OS/2 IFS / / / Documents and Settings / Grind / Application Data / Thunderbird / Profiles / i83dld16.default / ImapMail / bwk.wezepoel.net / Deleted Items / opslag adres
Tags
New tag
Preview
Fred,
de loods ligt op de Amsterdamsestraatweg in utrecht. kan nie missen.
Notes
0
Type your note here...


Search - type:email
https://
/technisch/#/projects/340b6f3d-606c-4777-a185-a961b830e7df/search?query=type%253Aem
beta
Expert UI
Project: Demo 2013
English
Tactical
Search
type:email
Search
Export query
Selected images: 7/7
interessant (3)
@evidence:delict:art416 (1)
@evidence:onderwerp:boot (1)
Search results
27 results in 13 ms.
email.sentOn
email.from
email.to
email.subject
email.read
email.has
2010-09-09T07:36... Peter de Groot <... system <system... Re: Reactie op u... false
2010-11-13T11:11... Peter de Groot <... klaasadam9@gm... haha false
2010-11-13T12:11... Klaas de Jong <k... Peter de Groot <... Re: haha false
2010-12-18T00:07... Fred Grind <freds... peterus321@gma... alvast!! false
2010-12-18T00:07... "Fred Grind" <fre... peterus321@gma... alvast!! true false
2010-12-18T00:07... "Fred Grind" <fre... peterus321@gma... alvast!! true false
2010-12-18T00:08... Peter de Groot <... Fred Grind <freds... Re: alvast!! false
2010-12-18T00:08... Peter de Groot <... Fred Grind <freds... Re: alvast!! true false
2010-12-18T00:08... Peter de Groot <... Fred Grind <freds... Re: alvast!! true false
2010-12-18T00:08... Peter de Groot <... Fred Grind <freds... Re: alvast!! true false
2011-01-15T17:23... Klaas de Jong <k... peterus321@gma... ahahahahahah! false
2011-01-17T18:47... Peter de Groot <... Klaas de Jong <k... Re: zomaar false
2011-01-22T18:23... Klaas de Jong <k... peterus321@gma... zomaar false
2011-11-18T20:15... Klaas de Jong <k... fredski999@gmai... opslag adres true false
2011-11-18T20:15... Klaas de Jong <k... fredski999@gmai... opslag adres true false
2011-11-18T20:15... Klaas de Jong <k... fredski999@gmai... opslag adres true false
2011-11-18T20:19... Fred Grind <Fred... Klaas de Jong <k... Re: opslag adres false
2011-11-18T20:19... Fred Grind <Fred... Klaas de Jong <k... Re: opslag adres true false
Trace properties
0-0-0-0-2-0-7-1-0-11-0-1-3
demo2013 - 3 - Windows XP
opslag adres
demo2013 - 3 - Windows XP:0-0-0-0-2-0-7-1-0-11-0-1
Path
demo2013 - 3 - Windows XP / NTFS; OS/2 IFS / / / Documents and Settings / Grind / Application Data / Thunderbird / Profiles / i83dld16.default / ImapMail / bwk.wezepoel.net / Deleted Items / opslag adres
Tags
New tag
Preview
Fred,
de loods ligt op de Amsterdamsestraatweg in utrecht. kan nie missen.
Notes
0
Type your note here...


Search - type:email
https://
/technisch/#/projects/340b6f3d-606c-4777-a185-a961b830e7df/search?query=type%253Aem
beta
Expert UI
Project: Demo 2013
English
Tactical
Search
type:email
Search
Export query
Selected images: 7/7
interessant (3)
@evidence:delict:art416 (1)
@evidence:onderwerp:boot (1)
Search results
27 results in 13 ms.
Copy to clipboard
Sort:
Columns
email.sentOn
email.from
email.to
email.subject
email.read
email.has
2010-08-11T08:30... Peter de Groot <... klaasadam9@gm... spullen false
2010-09-09T07:36... Peter de Groot <... system <system... Re: Reactie op u... false
2010-11-13T11:11... Peter de Groot <... klaasadam9@gm... haha false
2010-11-13T12:11... Klaas de Jong <k... Peter de Groot <... Re: haha false
2010-12-18T00:07... Fred Grind <freds... peterus321@gma... alvast!! false
2010-12-18T00:07... "Fred Grind" <fre... peterus321@gma... alvast!! true false
2010-12-18T00:07... "Fred Grind" <fre... peterus321@gma... alvast!! true false
2010-12-18T00:08... Peter de Groot <... Fred Grind <freds... Re: alvast!!
2010-12-18T00:08... Peter de Groot <... Fred Grind <freds... Re: alvast!! true
2010-12-18T00:08... Peter de Groot <... Fred Grind <freds... Re: alvast!! true
2010-12-18T00:08... Peter de Groot <... Fred Grind <freds... Re: alvast!! true
2011-01-15T17:23... Klaas de Jong <k... peterus321@gma... ahahahahahah!
2011-01-17T18:47... Peter de Groot <... Klaas de Jong <k... Re: zomaar
2011-01-22T18:23... Klaas de Jong <k... peterus321@gma... zomaar
2011-11-18T20:15... Klaas de Jong <k... fredski999@gmai... opslag adres true
2011-11-18T20:15... Klaas de Jong <k... fredski999@gmai... opslag adres true
2011-11-18T20:15... Klaas de Jong <k... fredski999@gmai... opslag adres true
2011-11-18T20:19... Fred Grind <Fred... Klaas de Jong <k... Re: opslag adres false
2011-11-18T20:19... Fred Grind <Fred... Klaas de Jong <k... Re: opslag adres true false
Trace properties
ID 0-0-0-0-2-0-7-1-0-11-0-1-3
Image demo2013 - 3 - Windows XP
Name opslag adres
Parent demo2013 - 3 - Windows XP:0-0-0-0-2-0-7-1-0-11-0-1
Path demo2013 - 3 - Windows XP / NTFS; OS/2 IFS / / / Documents and Settings / Grind / Application Data / Thunderbird / Profiles / i83dld16.default / ImapMail / bwk.wezepoel.net / Deleted Items / opslag adres
Tags
New tag
Preview
Fred,
de loods ligt op de Amsterdamsestraatweg in utrecht. kan nie missen.
Notes
0
Type your note here...


Search - type:email
https://
/technisch/#/projects/340b6f3d-606c-4777-a185-a961b830e7df/search?query=type%253Aem
beta
Expert UI
Project: Demo 2013
English
Tactical
Search
type:email
Search
Export query
interessant (3)
@evidence:delict:art416 (1)
@evidence:onderwerp:boot (1)
Search results
27 results in 13 ms.
Copy to clipboard
Sort:
Columns
email.sentOn
email.from
email.to
email.subject
email.read
email.has
2010-08-11T08:30...
Peter de Groot <...
klaasadam9@gm...
spullen
false
2010-09-09T07:36...
Peter de Groot <...
system <system...
Re: Reactie op u...
false
2010-11-13T11:11...
Peter de Groot <...
klaasadam9@gm...
haha
false
2010-11-13T12:11...
Klaas de Jong <k...
Peter de Groot <...
Re: haha
false
2010-12-18T00:07...
Fred Grind <freds...
peterus321@gma...
alvast!!
false
2010-12-18T00:07...
"Fred Grind" <fre...
peterus321@gma...
alvast!!
true
false
2010-12-18T00:07...
"Fred Grind" <fre...
peterus321@gma...
alvast!!
true
false
2010-12-18T00:08...
Peter de Groot <...
Fred Grind <freds...
Re: alvast!!
false
2010-12-18T00:08...
Peter de Groot <...
Fred Grind <freds...
Re: alvast!!
true
false
2010-12-18T00:08...
Peter de Groot <...
Fred Grind <freds...
Re: alvast!!
true
false
2010-12-18T00:08...
Peter de Groot <...
Fred Grind <freds...
Re: alvast!!
true
false
2011-01-15T17:23...
Klaas de Jong <k...
peterus321@gma...
ahahahahahah!
false
2011-01-17T18:47...
Peter de Groot <...
Klaas de Jong <k...
Re: zomaar
false
2011-01-22T18:23...
Klaas de Jong <k...
peterus321@gma...
zomaar
false
2011-11-18T20:15...
Klaas de Jong <k...
fredski999@gmai...
opslag adres
true
false
2011-11-18T20:15...
Klaas de Jong <k...
fredski999@gmai...
opslag adres
true
false
2011-11-18T20:15...
Klaas de Jong <k...
fredski999@gmai...
opslag adres
true
false
2011-11-18T20:19...
Fred Grind <Fred...
Klaas de Jong <k...
Re: opslag adres
false
2011-11-18T20:19...
Fred Grind <Fred...
Klaas de Jong <k...
Re: opslag adres
true
false
Trace properties
ID
0-0-0-0-2-0-7-1-0-11-0-1-3
Image
demo2013 - 3 - Windows XP
Name
opslag adres
Parent
demo2013 - 3 - Windows XP:0-0-0-0-2-0-7-1-0-11-0-1
Path
demo2013 - 3 - Windows XP / NTFS; OS/2 IFS / / / Documents and Settings / Grind / Application Data / Thunderbird / Profiles / i83dld16.default / ImapMail / bwk.wezepoel.net / Deleted Items / opslag adres
Tags
New tag
Preview
Fred,
de loods ligt op de Amsterdamsestraatweg in utrecht. kan nie missen.
Notes
0
Type your note here...


Trace - Kemah-01.JPG
https://
/technisch/#/projects/b13def5e-541a-45a7-949e-c66f6545387f/trace/a910324d-7060-4d5
beta
Expert UI
Project: R307 -- Enron
English
Tactical
Trace details - Kemah-01.JPG
Back to search
Trace
Raw
Picture
Hex
Text
Hex
Jump to byte
0
Go
Jump option
Hex
Dec
KiB per page
1
Change
viewing width
16
0 ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 c8 ......JFIF.....
16 00 c8 00 00 ff db 00 43 00 03 02 02 03 02 02 03 ....C........
32 03 03 03 04 03 03 04 05 08 05 05 04 04 05 0a 07 ....
48 07 06 08 0c 0a 0c 0c 0b 0a 0b 0b 0d 0e 12 10 0d ....
64 0e 11 0e 0b 0b 10 16 10 11 13 14 15 15 15 0c 0f ....
80 17 18 16 14 18 12 14 15 14 ff db 00 43 01 03 04 ....C...
96 04 05 04 05 09 05 05 09 14 0d 0b 0d 14 14 14 14 ....
112 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 ....
128 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 ....
144 14 14 14 14 14 14 14 14 14 14 14 14 14 14 ff c0 ....
160 00 11 08 01 e0 02 80 03 01 22 00 02 11 01 03 11 ....".......
176 01 ff c4 00 1f 00 00 01 05 01 01 01 01 01 01 00 ....
192 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 ....
208 0a 0b ff c4 00 b5 10 00 02 01 03 03 02 04 03 05 ....
224 05 04 04 00 00 01 7d 01 02 03 00 04 11 05 12 21 ......}........!
240 31 41 06 13 51 61 07 22 71 14 32 81 91 a1 08 23 1A..Qa."q.2....#
256 42 b1 c1 15 52 d1 f0 24 33 62 72 82 09 0a 16 17 B...R..$3br.....
272 18 19 1a 25 26 27 28 29 2a 34 35 36 37 38 39 3a ...%&'()*456789:
288 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a CDEFGHIJSTUVWXYZ
304 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a cdefghijstuvwxyz
320 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 ....
336 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 ....
352 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 ....
368 d6 d7 d8 d9 da e1 e2 e3 e4 e5 e6 e7 e8 e9 ea f1 ....
384 f2 f3 f4 f5 f6 f7 f8 f9 fa ff c4 00 1f 01 00 03 ....
400 01 01 01 01 01 01 01 01 01 00 00 00 00 00 00 01 ....
416 02 03 04 05 06 07 08 09 0a 0b ff c4 00 b5 11 00 ....
432 02 01 02 04 04 03 04 07 05 04 04 00 01 02 77 00 ....w.
448 01 02 03 11 04 05 21 31 06 12 41 51 07 61 71 13 ......!1..AQ.aq.


Browse - b13def5e-541a-45
https://
/technisch/#/browse/b13def5e-541a-45a7-949e-c66f6545387f/trace/a910324d-7060-4d5
beta
Expert UI
Project: R307 -- Enron
English
Tactical
Browse images
Browse
ENRON NTFS
/
$AttrDef
$BadClus
$Bitmap
$Boot
$Extend
$LogFile
$MFT
$MFTMirr
$Secure
$UpCase
$Volume
Lost Files
zl_allen-p_000.pst
allen-p
'Sent Mail
All documents
Calendar
Contacts
Deleted Items
Discussion threads
Drafts
Drafts (Lotus Notes)
Inbox
ANCHORDESK: 2002 in review: Not perf
Answer
Bishops Corner
Trace properties
ID
0-0-b-6-5-42
Image
ENRON NTFS
Name
ANCHORDESK: 2002 in review: Not perfect, but it sure beat 2001
Parent
ENRON NTFS:0-0-b-6-5
Path
ENRON NTFS / / / zl_allen-p_000.pst / allen-p / Inbox / ANCHORDESK: 2002 in review: Not perfect, but it sure beat 2001
Tags
New tag
Suspect
Trace extracted properties
Preview
_____DAVID COURSEY_____
2002 IN REVIEW: NOT PERFECT, BUT IT SURE BEAT 2001
Welcome to my 2002 Year in Review column, which
I feel very safe in asserting you are reading
here first. It's been a pretty good year, unless
Notes
0

Statistics

https://technisch/#/statistics/340b6f3d-606c-4777-a185-a961b830e7df

beta

Expert UI | Project: Demo 2013 | English | Tactical

Statistics

Image statistics

7 images

Filter: Enter text to search on every imag

show id | show details | show counters | show annotations | show labels

Description	State	# Traces	# Traces failed	# Framework failed	# Volumes	# File systems	# Files	# Carved
demo2013 - 1 - iPad	extracted	7,544	4 (0.05%)	-	-	-	-	-
demo2013 - 2 - Nokia Lumia	extracted	15	-	-	-	-	-	-
demo2013 - 3 - Windows XP	extracted	169,240	35 (0.02%)	-	3	1	28,504	2,572
demo2013 - 4 - iPhone	extracted	15,262	3 (0.02%)	-	-	-	-	-
demo2013 - 5 - Samsung	extracted	8,910	22 (0.25%)	-	-	-	-	-
demo2013 - 6 - TomTom	extracted	7,956	2 (0.03%)	-	13	3	1,817	2
demo2013 - 7 - Xbox	extracted	4,492	9 (0.20%)	-	1	-	-	3,047

Failed tools for all images

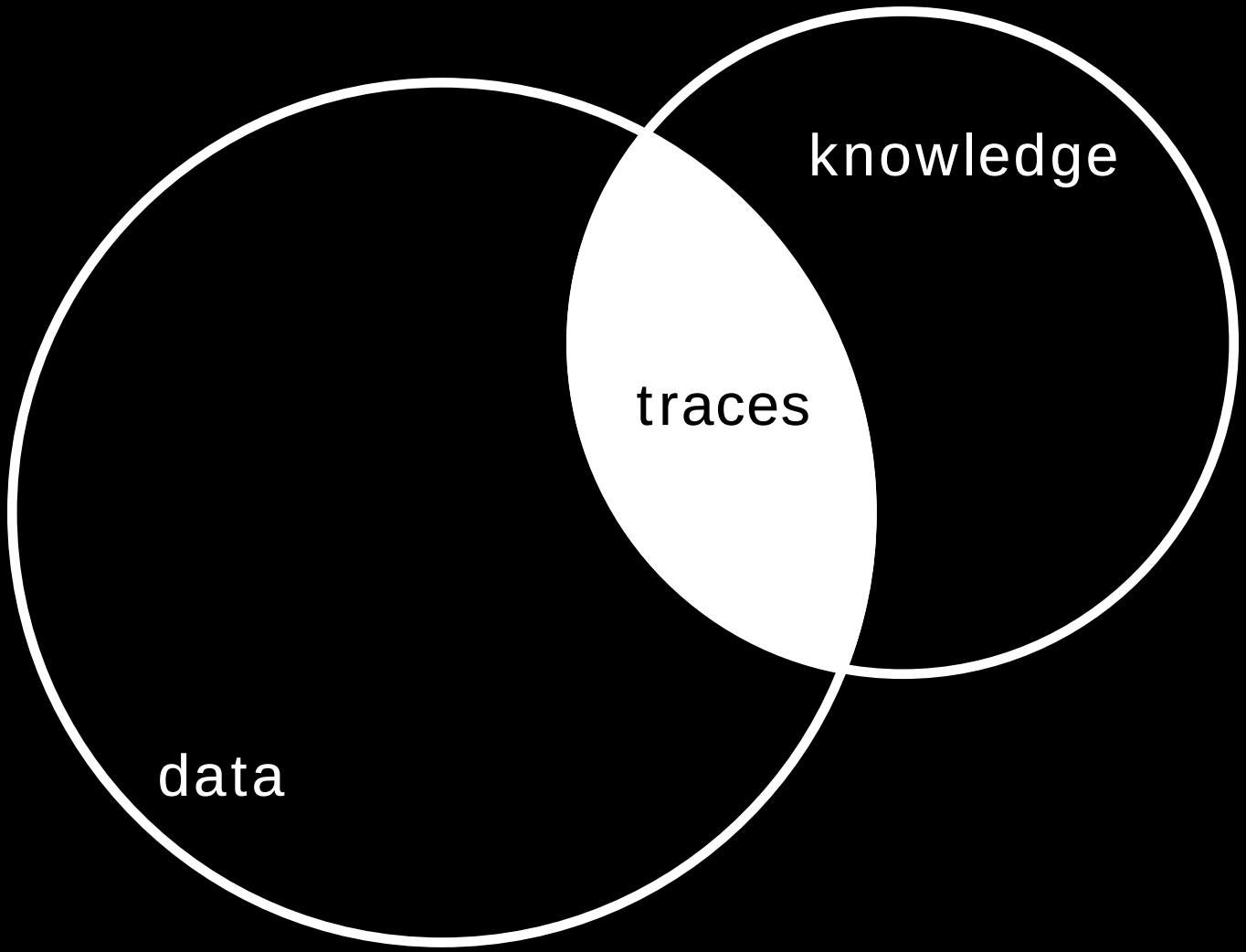
All images

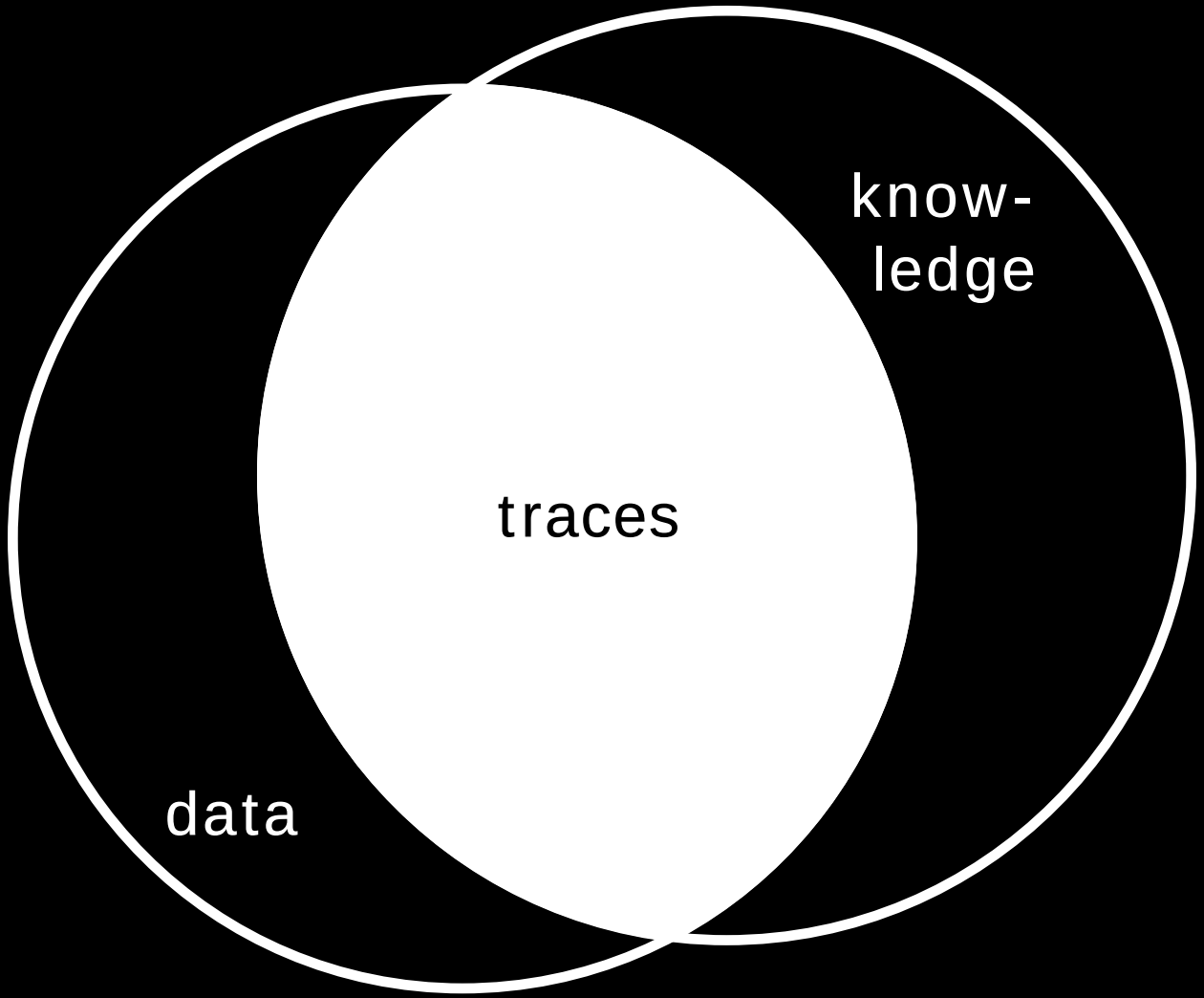
The tool failures are aggregated for all images.

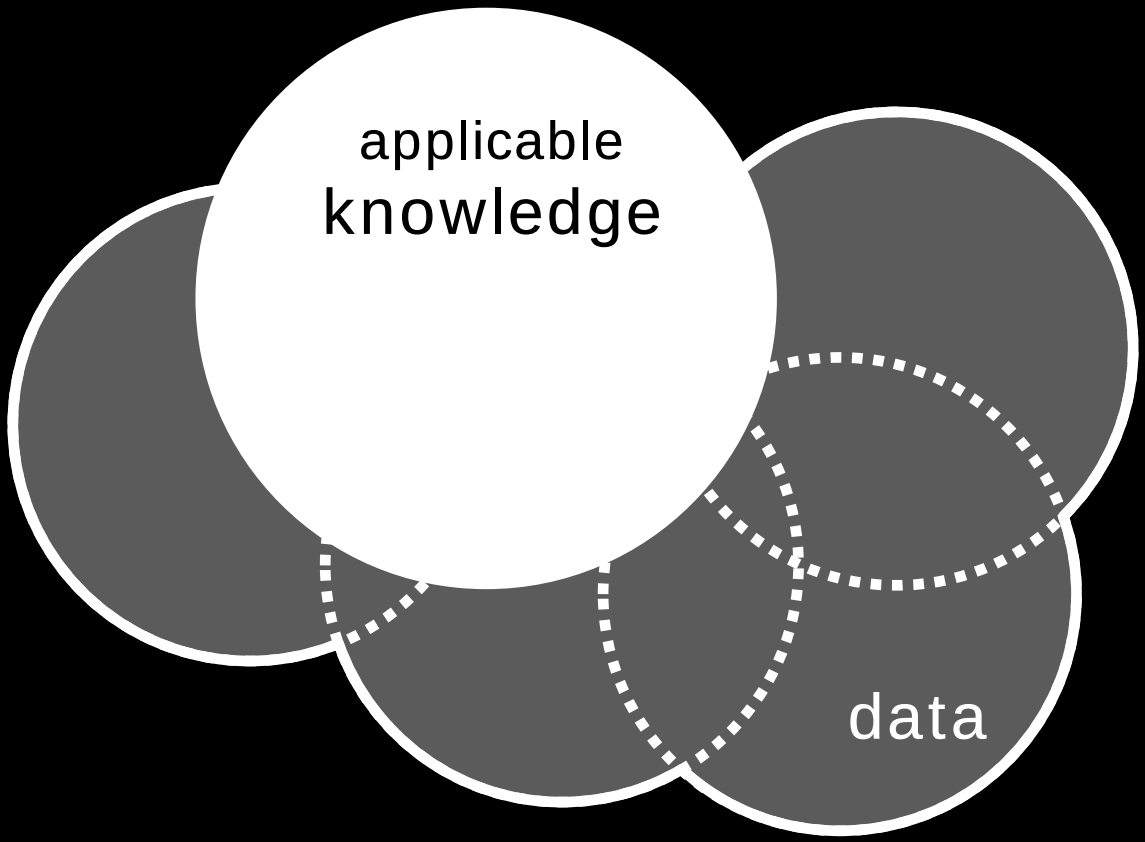
Lesson six

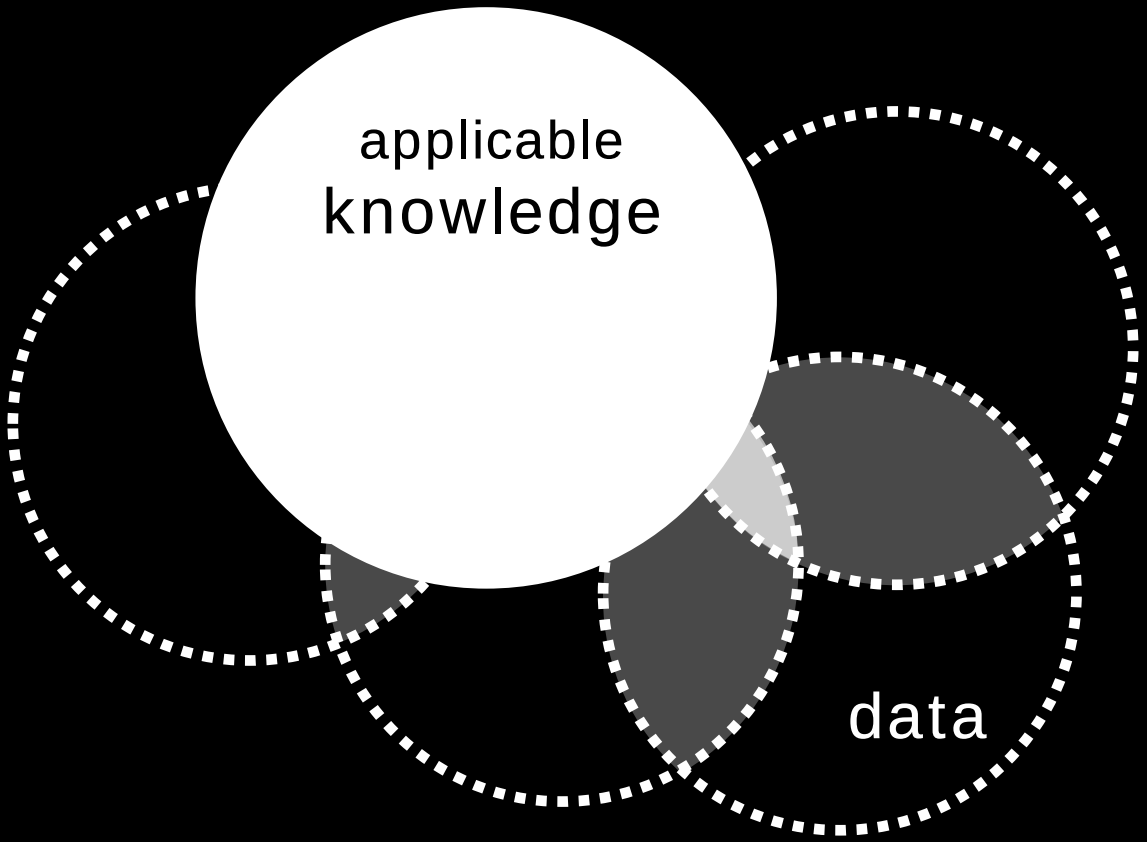
What to add next?

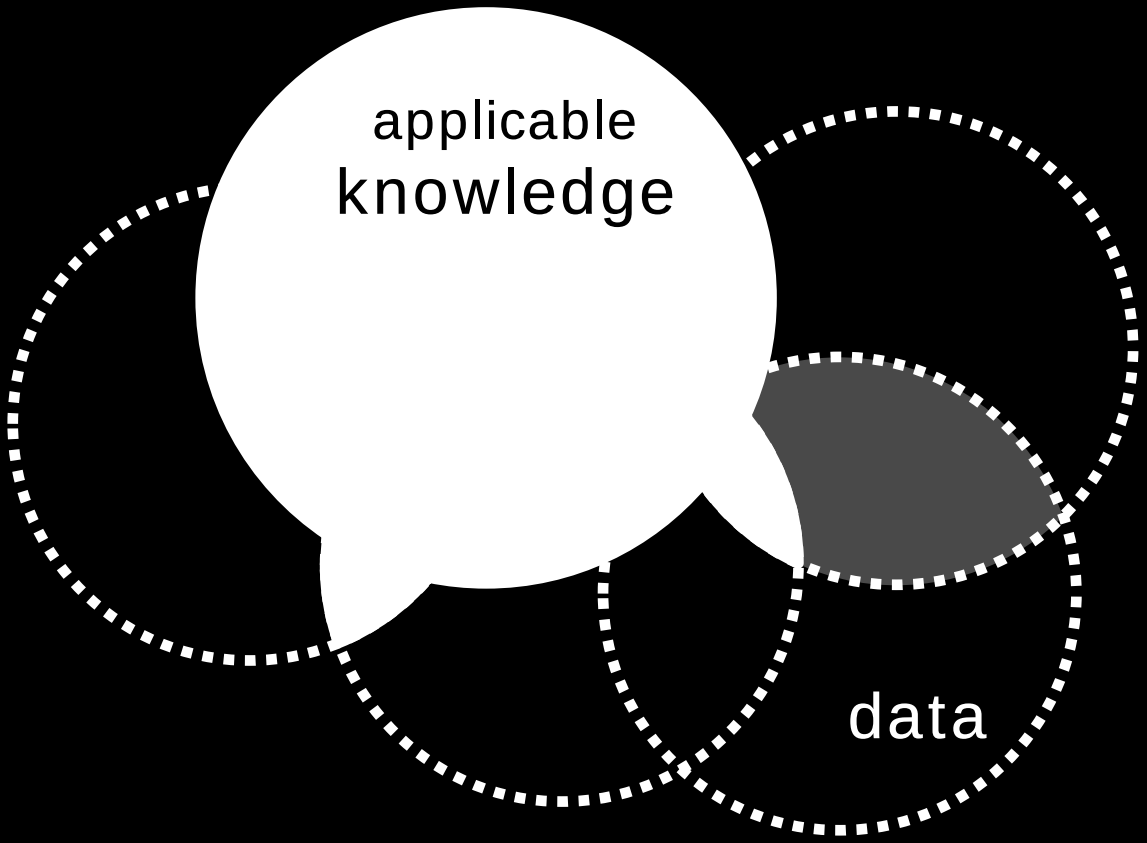
Follow the data


knowledge
traces
data

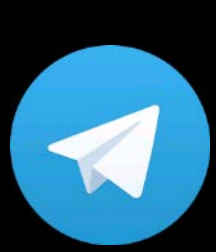

know-
ledge
traces
data


applicable
knowledge
data


applicable
knowledge
data


applicable
knowledge
data

Recently added



Lx01

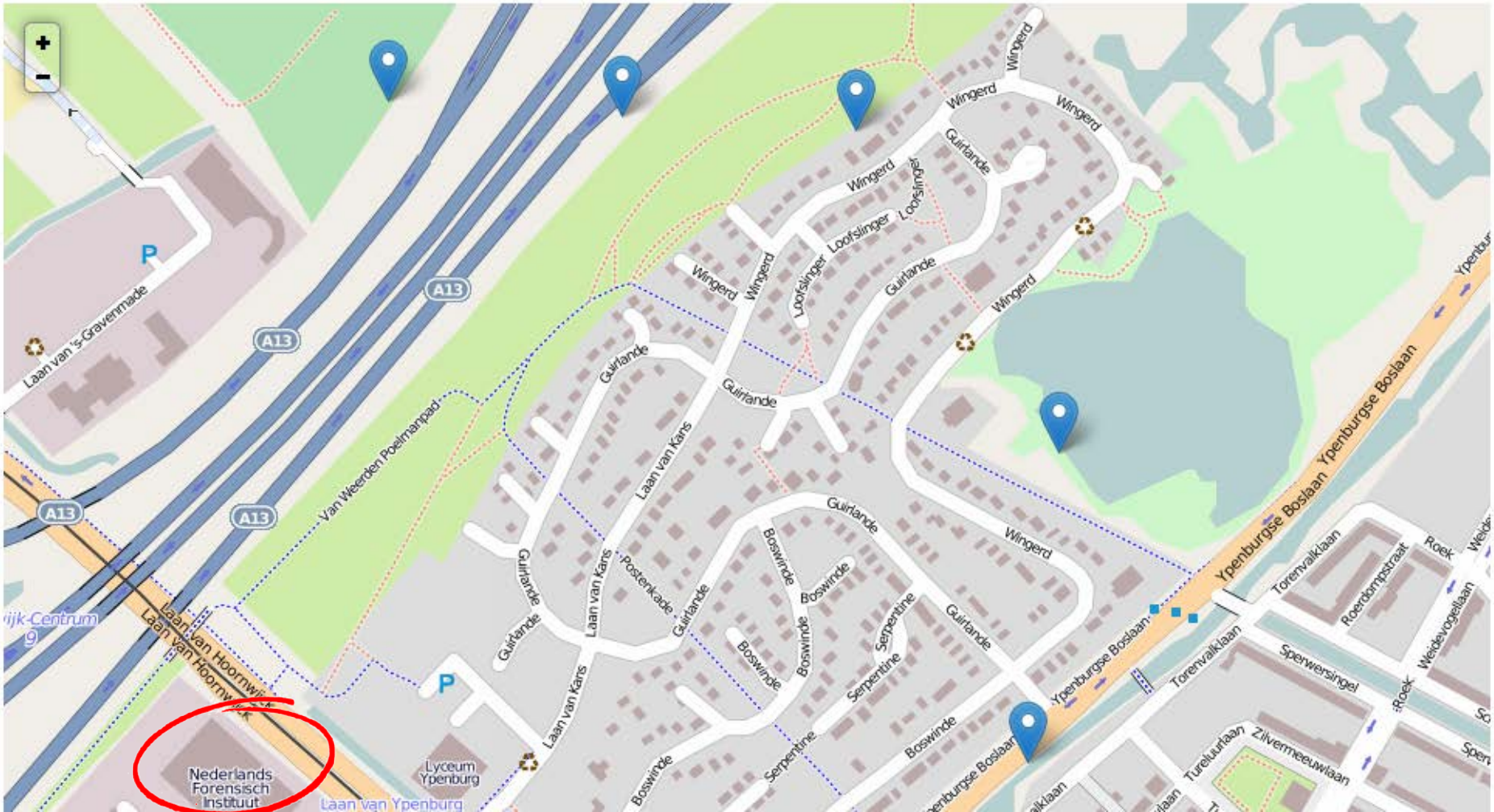
L01

AD1

All (5) Compressed (5) Content (5) File (5) GPS entry (5) [type.gpslog] (5)

5 of the in total 5 traces are located in this area.

list timeline gallery geo location



+ Note

OCR data >

SampleImage.bmp

Type: Picture

Device: OCR data
Camera:
Taken:
Size: 750 x 135

More ...

Download content of this trace

Generate report

Open in a new window

Start a new search

Name: SampleImage.bmp

Created:

Thum Preview OCR

Optical character recognition, usually abbreviated to OCR, is the mechanical or electronic translation of scanned images of handwritten, typewritten or printed text into machine-encoded text. It is widely used to convert books and documents into electronic files, to computerize a record-keeping system in an office, or to publish the text on a website. OCR makes it possible to edit the text, search for a word or phrase, store it more compactly, display or print a copy free of scanning artifacts, and apply techniques such as machine translation, text-to-speech and text mining to it. OCR is a field of research in pattern recognition, artificial intelligence and computer vision.

+ Note

OCR data >

SampleImage.bmp

Type: Picture

Device: OCR data
Camera:
Taken:
Size: 750 x 135

More ...

Download content of this trace

Generate report

Open in a new window

Start a new search

Name: SampleImage.bmp

Created:

Thumbnail Preview OCR

Optical character recognition, usually abbreviated to OCR, is the mechanical or electronic translation of
scanned images of handwritten, typewritten or printed text into machine-encoded text. It is widely used to convert
books and documents into electronic files, to computerize a record-keeping system in an office, or to publish the
text on a website. OCR makes it possible to edit the text, search for a word or phrase, store it more compactly,
display or print a copy free of scanning artifacts, and apply techniques such as machine translation, text-to-speech
and text mining to it. OCR is a field of research in pattern recognition, artificial intelligence and computer vision.

Work in progress

- Language detection
- Network tap data
- Entity extraction
- Call Detail Records
- Drone data
- Volume shadow copies

Hansken

Netherlands Forensic Institute

Digital Forensics as a Service

A game changer

dx.doi.org/10.1016/j.diin.2014.03.007

Game on

dx.doi.org/10.1016/j.diin.2015.07.004

Harm van Beek PhD

harm.van.beek@nfi.minvenj.nl