



Netherlands Forensic Institute
Ministry of Security and Justice

Measuring and mitigating errors in a `Digital Forensics as a Service` environment

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



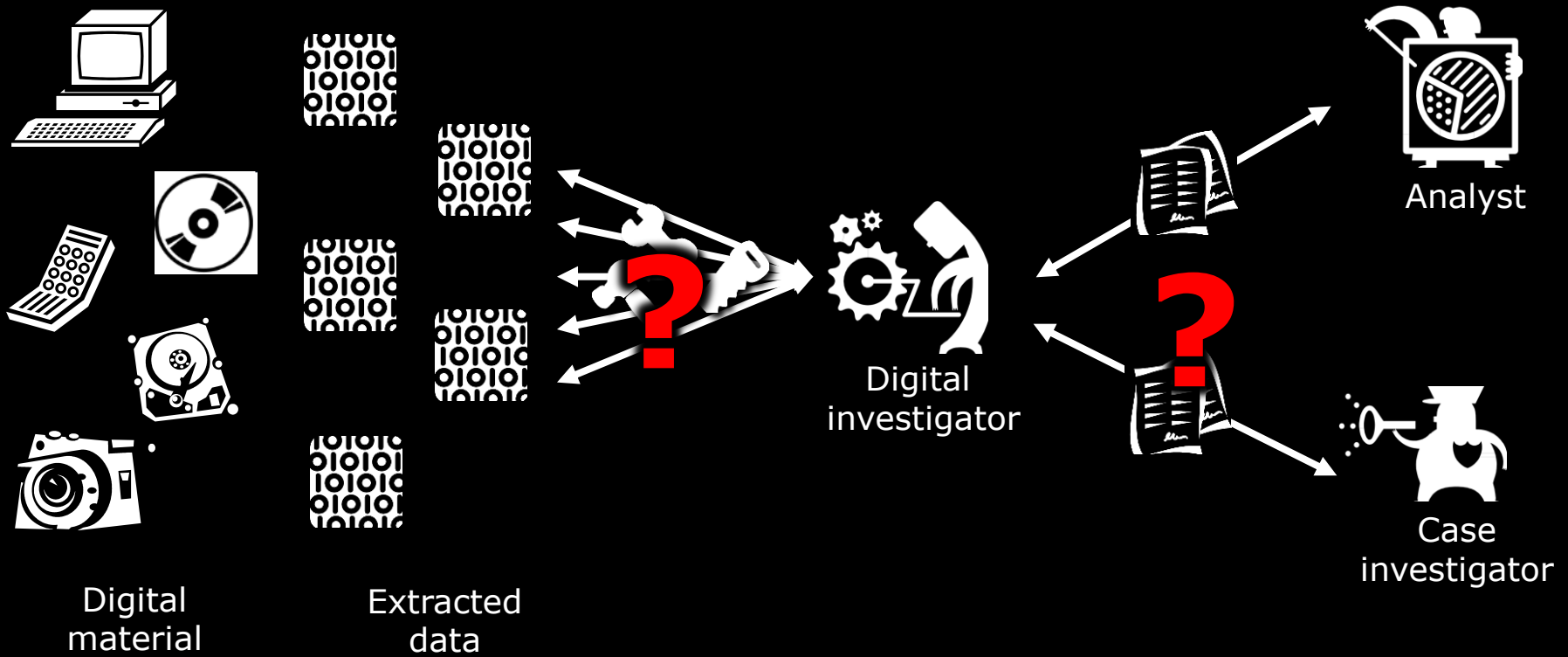
Netherlands Forensic Institute
Ministry of Security and Justice

Be transparent

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

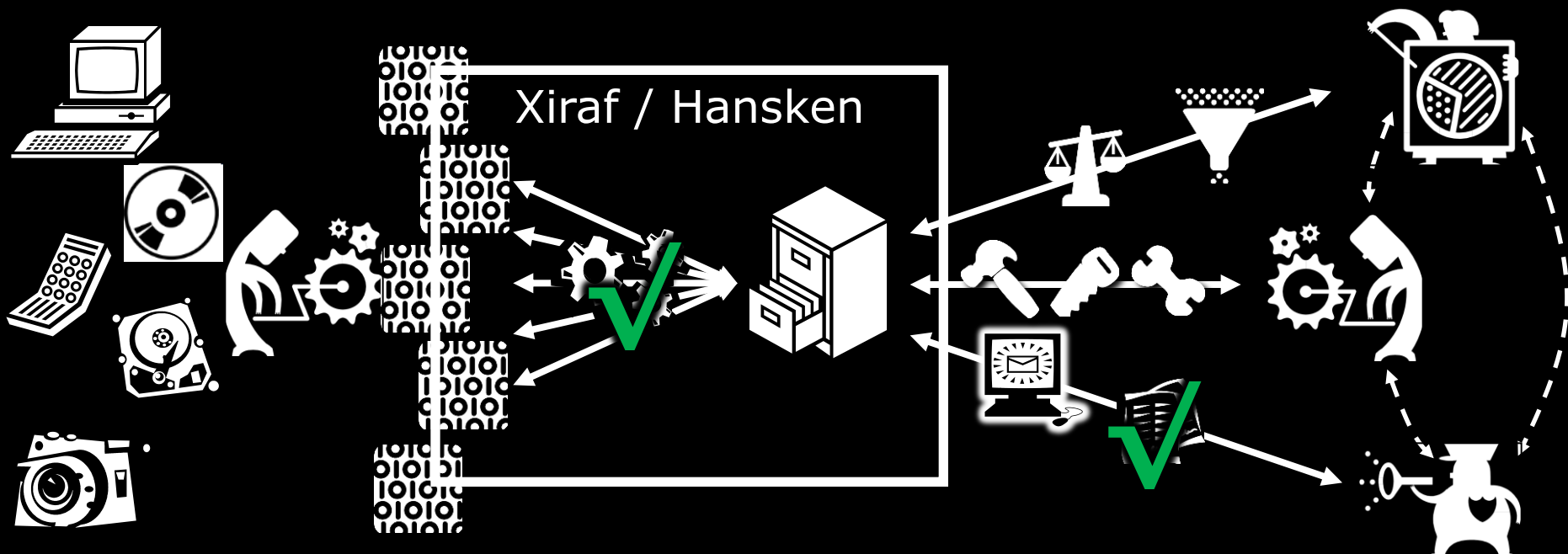


Traditional Digital Forensic Investigation





"Digital Forensics as a service" (since 2010)



Acquisition

Extraction

Analysis



> 500 cases

> 1 petabyte data processed

> 2300 case investigators trained

all (regional) Dutch police forces

Dutch National High Tech Crime Unit

RST Former Dutch Antilles

Toronto Police



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.
© 2014 The Authors. Published by Elsevier Ltd on behalf of DFRWS. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/3.0/>).

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

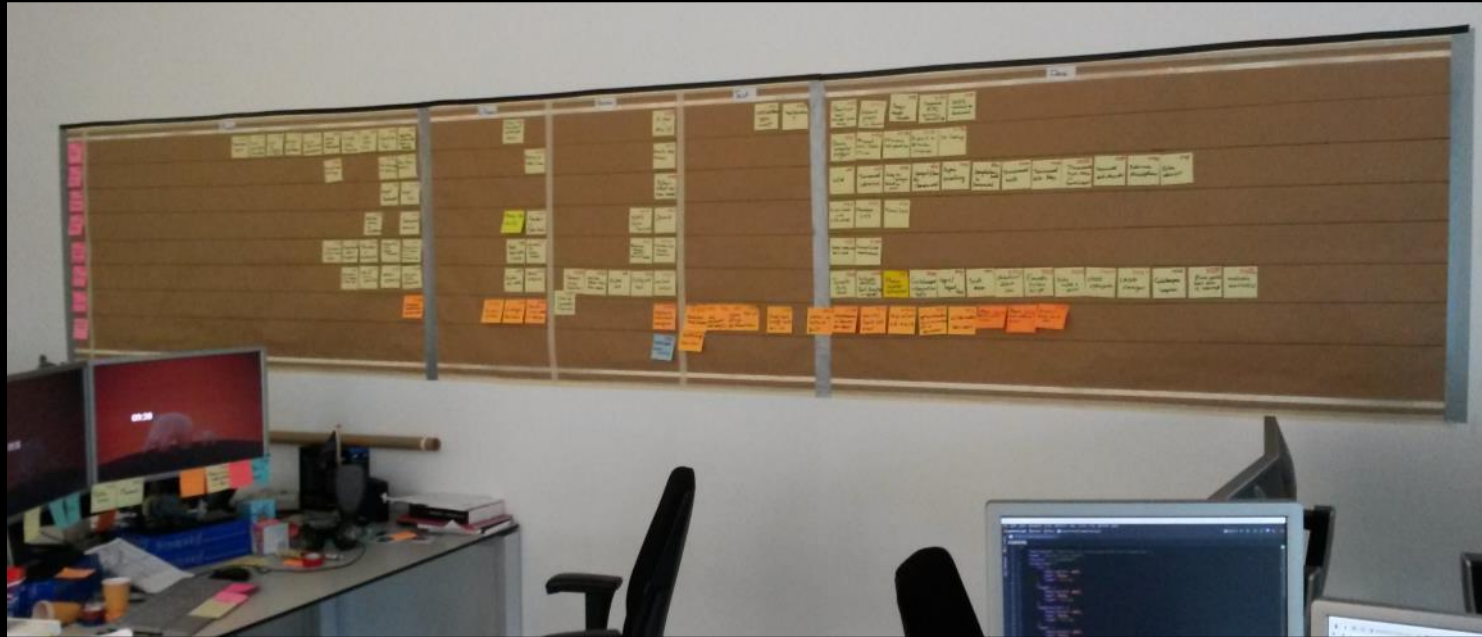
* Corresponding author.
E-mail addresses: ruud@holmes.nl (R.B. van Baar), harm@holmes.nl (H.M.A. van Beek), eijk@holmes.nl (E.J. van Eijk).
<http://dx.doi.org/10.1016/j.diin.2014.03.007>
1742-2876/© 2014 The Authors. Published by Elsevier Ltd on behalf of DFRWS. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/3.0/>).

> 1 per
> 2300
all
Dut

ned



Transparent software development (and deployment)





Hansken + Ganesha - Agile Board - Jira - Chromium

se.dev.holmes.nl/jira/secure/RapidBoard.jspx?rapidView=23&selectedIssue=HANSKEN-2269

Apps Confluence Jira Stash Bamboo

JIRA Dashboards ▾ Projects ▾ Issues ▾ Agile ▾ **Create** Search ? ⚙️ 👤

Hansken + Ganesha Backlog Active sprints Reports Board ▾

SPRINT: Sprint 28 ▾ QUICK FILTERS: Only My Issues Recently Updated

To Do	In Progress	Review	Test / Deploy	Done
▼ HANSKEN-2520 14 sub-tasks Test Sprint 28				
HANSKEN-2142 📌 The number of registryEntries between XIRAF and Hansken are	HANSKEN-2269 📌 Emails (eml and txt) are mime-typed as text/html or text/plain; and not		HANSKEN-1143 📌 hql-human: support single character wildcard ?	HANSKEN-2136 📌 All OLE2 are marked as type document which is undesirable
HANSKEN-2271 📌 GPS items from GPX file are not processed			HANSKEN-2181 📌 improve rpc error handling	HANSKEN-2263 📌 OLE2 ThumbnailArchives and MSG files are typed
HANSKEN-2346 📌 Carving of partial JPEG pictures				HANSKEN-2498 📌 No slack for \$BadClus
HANSKEN-2475 📌 For Demo2013 TomTom only one trace is created (type: image)				HANSKEN-2529 📌 Update export functionality in demo gui so you can select
HANSKEN-2505 📌 BadGuy: For CUTSCENES_STORY_1_BEGINNING.pvr.zip -				HANSKEN-2534 📌 Misc properties of the shortcut tool are upper case
HANSKEN-2523 📌 LocationTool				



Emails (eml and txt) are mime-typed as text/html or text/plain; and not processed correctly

[Edit](#) [Comment](#) [Assign](#) [More](#) [Ready for Review](#) [Export](#)

Details

Type:	Bug subtask	Status:	IN PROGRESS (View Workflow)
Priority:	Major	Resolution:	Unresolved
Affects Version/s:	None	Fix Version/s:	None
Component/s:	None		
Labels:	None		
Sprint:	Sprint 28		

People

Assignee: [Assign to me](#)

Reporter:

Votes: [Vote for this issue](#)

Watchers: [Start watching this issue](#)

Description

Also for mim

Example: Harm's Test Image

- x-mozilla-status-unread.eml
- x-mozilla-status-read.eml
- x-mozilla-status-read-and-marked.eml

Dates

Created: 10/Feb/15 3:59 PM

Updated: Now

Development

[Create branch](#)

Agile

Active Sprint: [Sprint 28 ends 02/Apr/15](#)

[View on Board](#)

Issue Links

- depends on [TRACES-343 Valid eml not recognized as email](#) [OPEN](#)
- mentioned in [Test Results Test image](#)
- [Test Status - Demo - sprint 27](#)
- [Top Test Issues](#)



Pull requests for repository hansken - Stash - Chromium

se.dev.holmes.nl/stash/projects/HANSKEN/repos/hansken/pull-requests

Apps Confluence Jira Stash Bamboo

Stash Projects Repositories Find a repository...

Pull requests

Open Merged Declined

ID	Title	Author	Reviewers	Source	Destination	Updated
#843	HANSKEN 831 support java 8			HANSKEN-831	master	6 days ago
#1001	HANSKEN 2398 entitytool			HANSKEN-2398	HANSKEN-2392	2 days ago
#1056	HANSKEN-2583 fully depend on tika-1.7, n...			HANSKEN-2583	master	2 days ago
#1055	HANSKEN-2575 clean up SmoothToolSink			HANSKEN-2575	master	2 days ago
#1053	HANSKEN-2580: Keystore service rest inter...			HANSKEN-2580	master	2 days ago
#1059	HANSKEN-2592 exclude \$Bad slack from d...			HANSKEN-2592	master	2 days ago
#1050	HANSKEN 2514 TextProcessorTool, TextTool			HANSKEN-2514	master	2 days ago
#1023	HANSKEN 2324 Add intrinsic properties to...			HANSKEN-2324	master	Yesterday
#1046	HANSKEN-2441: Enable image (un)linking i...			HANSKEN-2441	master	Yesterday
#1062	HANSKEN-2228 reenable jacoco support fo...			HANSKEN-2228-re...	master	Yesterday
#1065	HANSKEN-2411 Handle Login / HTTP errors			HANSKEN-2411	master	Yesterday
#1067	HANSKEN-1107: Remove logapi.logapi con...			HANSKEN-1107	master	Yesterday
#1015	[PREVIEW] HANSKEN-2428: Tracemodel r...			HANSKEN-2428	master	Yesterday
#1060	HANSKEN-2494: Update python-api to new			HANSKEN-2494	HANSKEN-2428	41 mins ago



Pull Request #1059: HANSKEN-2592 exclude \$Bad slack from data - Stash - Chromium

se.dev.holmes.nl/stash/projects/HANSKEN/repos/hansken/pull-requests/1059/diff

Find text in diff and context lines

- projects/services/analysis-service/tools/snorkel/src
 - main/java/nl/minvenj/nfi/hansken/analysis/tool/snorkel
 - NodeWriter.java** (MODIFIED)
 - test
 - images
 - NTFS-20060227.E01.properties
 - java/nl/minvenj/nfi/hansken/analysis/tool/snorkel
 - FilesystemToolTest.java

```
320 320      final String slackname = SLACK_PREFIX + fileNode.getEntryIdentifier() + ":" +
321 -      slack.data(DATA_TYPE, descriptor(dataNode, slackname, NodeType.SLACK), slackSi
322 -      final long pos = getSlackImageOffset(trace, dataNode);
323 -      if (pos >= 0) {
324 -          slack.imageOffset(DATA_TYPE, pos);
321 +
322 +      // the special alternate data stream $BadClus:$Bad will not contain slack data
323 +      if (!$BadClus:$Bad".equals(trace.getName())) {
324 +
325 +      slack.data(DATA_TYPE, descriptor(dataNode, slackname, NodeType.SLACK), sla
326 +          final long pos = getSlackImageOffset(trace, dataNode);
327 +          if (pos >= 0) {
328 +              slack.imageOffset(DATA_TYPE, pos);
329 +          }
330 +      }
331
332
333      slack.type("unallocated");
```

Is there no better way to detect this; is the name of the trace *the* place to read this? I'd expect the `StreamNode` to know something about this.

Reply · Create task · Like · Yesterday

Did a quick check, unfortunately there isn't. `StreamNode` doesn't know nothin' .. It will be API digging and class casting which will defy the elegance of just filtering by name (and they will stay the same as it is a NTFS directory entry)

Reply · Delete · Create task · Like · Yesterday

yeah i know, it is done the same way as for non-slack \$BadClus:\$Bad, though once it is fixed in snorkel ([SNORKEL-1047](#)), then it can be removed here ([HANSKEN-2603](#))

Reply · Delete · Create task · Like · 19 mins ago (edited 2 mins ago)



Build projects / HANSKEN

Maven main build

Builds the core maven project

Navigation icons: back, refresh, stop, play, error, success, run, actions, share

- Plan summary
- Branches
- Recent failures
- History
- Tests
- Issues
- Deployments 2

Plan summary

Showing Last 7 days

Current activity

HANSKEN-CTP-2496 Manual build by [redacted] with revision HANSKEN-2151_revert

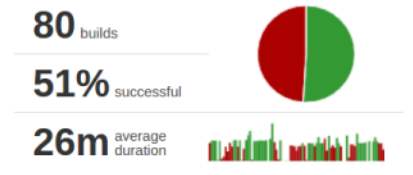
Waiting to be built...

Recent history

#2495	Changes by [redacted]	6 minutes ago	1 of 5539 failed	
#2494	Custom build by [redacted] with revision HANSKEN-2428	15 hours ago	13 of 6201 failed	CUSTOM REVISION
#2493	Custom build by [redacted] with revision HANSKEN-2428	16 hours ago	1 of 5923 failed	CUSTOM REVISION
#2492	Changes by N...	17 hours ago	6317 passed	
#2491	Changes by N...	18 hours ago	6317 passed	
#2490	Custom build by N... with revision HANSKEN-2387	18 hours ago	6317 passed	CUSTOM REVISION
#2489	Custom build by [redacted] with revision HANSKEN-2228-re-enable-jacoco-support-for	19 hours ago	Testless build	CUSTOM REVISION
#2488	Custom build by [redacted] with revision HANSKEN-2581	19 hours ago	6317 passed	CUSTOM REVISION
#2487	Custom build by [redacted] with revision HANSKEN-2581	19 hours ago	Testless build	CUSTOM REVISION
#2486	Custom build by [redacted] with revision HANSKEN-2324	20 hours ago	5698 passed	CUSTOM REVISION

Latest build Last successful build

Plan statistics



Branches

- HANSKEN-2494 #1
- HANSKEN-1107 #1
- HANSKEN-2411 #3
- HANSKEN-2585 #1
- HANSKEN-2596 #3
- HANSKEN-2581 #7
- HANSKEN-2228-re-enable-jacoco-support-for #1
- HANSKEN-2430 #2
- HANSKEN-2469 #2
- HANSKEN-2579 #4

View all branches



Status Summary Screen - Bamboo - Chromium			
✗ Maven main build HANSKEN 32 minutes ago Changes by [redacted]	✓ HANSKEN-1107 HANSKEN - Maven main build 16 hours ago First build for this plan	✓ HANSKEN-2228-re-... HANSKEN - Maven main build 20 hours ago First build for this plan	✗ HANSKEN-2411 HANSKEN - Maven main build 17 hours ago Changes by [redacted]
✗ HANSKEN-2430 HANSKEN - Maven main build 20 hours ago Changes by [redacted]	✗ HANSKEN-2469 HANSKEN - Maven main build 1 day ago Changes by [redacted]	✓ HANSKEN-2494 HANSKEN - Maven main build 16 minutes ago Changes by [redacted]	✓ HANSKEN-2575 HANSKEN - Maven main build 1 day ago First build for this plan
✓ HANSKEN-2579 HANSKEN - Maven main build 1 day ago Manual run by [redacted]	✓ HANSKEN-2580 HANSKEN - Maven main build 1 day ago Changes by [redacted]	✓ HANSKEN-2581 HANSKEN - Maven main build 19 hours ago Changes by [redacted]	✓ HANSKEN-2583 HANSKEN - Maven main build 1 day ago Code changes detected
✗ HANSKEN-2585 HANSKEN - Maven main build 17 hours ago First build for this plan	✗ HANSKEN-2588 HANSKEN - Maven main build 1 day ago Manual run by [redacted]	✓ HANSKEN-2592 HANSKEN - Maven main build 1 day ago First build for this plan	✗ HANSKEN-2596 HANSKEN - Maven main build 17 hours ago Manual run by [redacted]



Documentation - HANSKEN - Confluence - Chromium

se.dev.holmes.nl/confluence/display/HANSKEN/Documentation

Apps Confluence Jira Stash Bamboo

Confluence Spaces People Create

HANSKEN

Pages

SPACE SHORTCUTS

- Documentation
- Development Environment
- Parkeerplaats
- Graphviz Diagrams

CHILD PAGES

- HANSKEN Home
 - Documentation
 - Hansken Glossary
 - Platform Architecture Document...
 - Use Cases
- 6 more child pages
- Create child page

Space tools <<

Pages / HANSKEN Home

Documentation

Created by [redacted], last modified by [redacted] on Mar 04, 2015

Hansken Glossary

Platform Architecture Document (PAD)

- 0. Introduction to the Hansken Platform Document
 - 0.1 Objectives
 - 0.2 Document Scope
 - 0.3 Intended Audience
 - 0.4 References
 - 0.5 Document Overview
- 1. Hansken Introduction
 - 1.1 Drivers
 - 1.2 Objectives
 - 1.3 The 'Platform' concept
 - 1.4 Hansken Forensic Implementation
 - 1.5 Architecture and Design – Lines of Approach
 - 1.5.1 IAF's framework - models
- 2. Contextual View
 - 2.1 Platform Context
 - 2.2 Architectural Objectives
 - 2.3 Business Drivers
 - 2.4 Principles
 - 2.4.1 Security
 - 2.4.2 Privacy
 - 2.4.3 Transparency
 - 2.4.4 Reliability
 - 2.4.5 Multi Tenancy
 - 2.4.6 High Availability
 - 2.4.7 Future Proof



HANSKEN

Pages

SPACE SHORTCUTS

- Documentation
- Development Environment
- Parkeerplaats
- Graphviz Diagrams

CHILD PAGES

- Use Cases
 - Use Case: Query Trace Database
 - + Create child page

Space tools

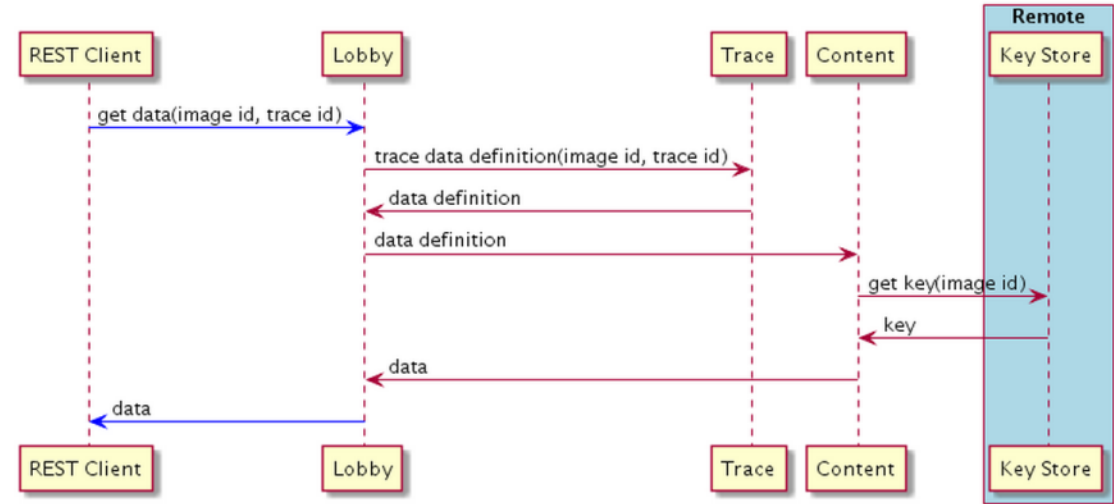
Pages / ... / Use Cases Edit Watch Share

Use Case: Query Trace Database

Created by [redacted], last modified on Sep 04, 2013

To query Hansken for getting data for one trace, the following steps are taken:

Query Trace database



Like Be the first to like this

No labels



Source of ganesha-login-xiraf... x +

se.dev.holmes.nl/stash/projects/HANSKEN/repos/full-integration-test/browse/fit-projects/fit-projects-ganesha/src/main/resources/stories/ganesha/login/ganesha-login-xiraf-prep.story

Find a repository...

Source

committed 6e8b2d0504a 09 Jun 2015

master

full-integration-test / fit-projects / fit-projects-ganesha /
src / main / resources / stories / ganesha / login /
ganesha-login-xiraf-prep.story

Source view | Diff to previous | History | Blame | Raw file

```
1 Feature: login to ganesha
2
3 Scenario: login to local ganesha instance on Hansken
4
5 Given I am on the page with URL /login.html
6 When I wait for the element with id username to be present
7 And I type the username with text user
8 And I type the password with text blabla
9 And I select Test (Hansken) of region select box
10 And I log in
11 Then I should be logged in as user
12 And I should be on page with URL /overview.html
13
14
```



Source of Hansken_Method_... x +

se.dev.holmes.nl/stash/projects/HANSKEN/repos/full-integration-test/browse/fit-projects/fit-projects-rest/src/main/resources/stories/authorization/Hansken_Method_Validation_403_readImage.story

Source view | Diff to previous | History ▾ | Blame | Raw file

```
2
3 Scenario: Before - User - no permissions
4 Given a request header Content-Type application/json
5 And request body {username:"test_readImage",password:"${testaccount.password}"}
6 When I do a POST request to /session/login
7
8 Scenario: Validation if an user is authorized on GET methods
9 When I do a GET request to <path>
10 Then I expect response code <status>
11 And I expect response body to contain <responseBody>
12
13 Examples:
14 |id      |path                                     |status |responseBody
15 |101     |/projects                               |403     |permission denied: missing permis
16 |102     |/projects/${ProjectUUID2}              |403     |permission denied: missing permis
17 |102a    |/projects/${ProjectUUIDX}              |403     |permission denied: missing permis
18 |103     |/projects/${ProjectUUID2}/images       |403     |permission denied: missing permis
19 |103a    |/projects/${ProjectUUIDX}/images       |403     |permission denied: missing permis
20 |104     |/images                                 |200     | |
21 |105     |/images/${ImageUUID2}                  |200     | |
22 |107     |/projects/${ProjectUUID2}/tracemodel   |403     |permission denied: missing permis
23 |107a    |/projects/${ProjectUUIDX}/tracemodel   |403     |permission denied: missing permis
24 |110     |/projects/${ProjectUUID2}/traces/roots |403     |permission denied: missing permis
25 |110a    |/projects/${ProjectUUIDX}/traces/roots |403     |permission denied: missing permis
26 |113     |/version                                 |200     |
27
28 Scenario: BUG SCENARIO'S GET
```



Source of Hansken_014_Sear... x +

se.dev.holmes.nl/stash/projects/HANSKEN/repos/full-integration-test/browse/fit-projects/fit-projects-rest/src/main/resources/stories/search/Hansken_014_Search_Traces_01_Term (POST).story

Search

Source view Diff to previous History ▾ Blame Raw file

```
529 And I expect response header Content-Type to be equal to ${ContentType}
530 And I expect response body to contain "totalResults":${TotalResults}
531
532 Scenario: 146 - Valid - Fullmatch ignored with boolean
533 Given property field = email.hasAttachment
534 And property value = false
535 And property fullmatch = false
536 And property TotalResults = 5579
537 And request body {count:0, query: {term: { field:"${field}", value:"${value}", fullMatch:${fullmatch}}}}
538 When I do a POST request to /projects/${ProjectUUID2}/search
539 Then I expect response code 200
540 And I expect response header Content-Type to be equal to ${ContentType}
541 And I expect response body to contain "totalResults":${TotalResults}
542
543 Scenario: 147 - Valid - Fullmatch ignored with boolean
544 Given property field = email.hasAttachment
545 And property value = false
546 And property fullmatch = true
547 And property TotalResults = 5579
548 And request body {count:0,query: {term: { field:"${field}", value:"${value}", fullMatch:${fullmatch}}}}
549 When I do a POST request to /projects/${ProjectUUID2}/search
550 Then I expect response code 200
551 And I expect response header Content-Type to be equal to ${ContentType}
552 And I expect response body to contain "totalResults":${TotalResults}
553
554 Scenario: 148 - Valid - Fullmatch ignored with boolean
555 Given property field = email.hasAttachment
```



HANSKEN

Pages

SPACE SHORTCUTS

- Documentation
- Development Environment
- Parkeerplaats
- Graphviz Diagrams

CHILD PAGES

- Test Results Index/Analysis
 - Test Results Test image

+ Create child page

Test Results Test image

Created by [redacted], last modified on Mar 24, 2015

	Project	XIRAF	HANSKEN		HANSKEN	HANSKEN	HANSKEN	HANSKEN	HANSKEN	HANSKEN
	Version	1.6.6.9			0.28	0.20	0.20	0.19	0.19	0.19
	Build nr				2433,2460,2482	2343,2271	2257,2231,2218,2211,2180	2149	2144,2121,2117,2098	2073
	Configuration				All-in-one	All-in-one	All-in-one	All-in-one	All-in-one	All-in-
	Environment	PREP			Local	Local	Local	Local	Local	Local
	Date	BASELINE	BASELINE	DIFF	19-03-2015	11-3-2015	5-3-2015	23-2-2012	23-2-2015	16-2-
	All	21007	25408	TO DO	25408	25408	25415	25415	17396	1739
3	addressBook	5	9		9	9	9	9	9	9
4	attachment	335	335		335	335	334	334	334	334
8	browserHistory	287	287		287	287	287	287	287	287
9	browserHistoryLog	9	8		8	8	8	8	8	8
12	carved	150	157		157	157	157	157	157	157
13	chatEvent	3	3		3	3	3	3	3	3
14	chatLog	57	14		14	14	14	14	14	14
15	chatMessage	339	4156		4156	4156	4156	4156	4156	4156
16	compressed	0	260		260	260	260	260	260	259
18	contact	19	25		25	25	25	25	25	25
19	cookie	301	301		301	301	301	301	301	301

HANSKEN-2346 - Carving of partial JPEG pictures OPEN



HANSKEN

Pages

SPACE SHORTCUTS

- Documentation
- Development Environment
- Parkeerplaats
- Graphviz Diagrams

CHILD PAGES

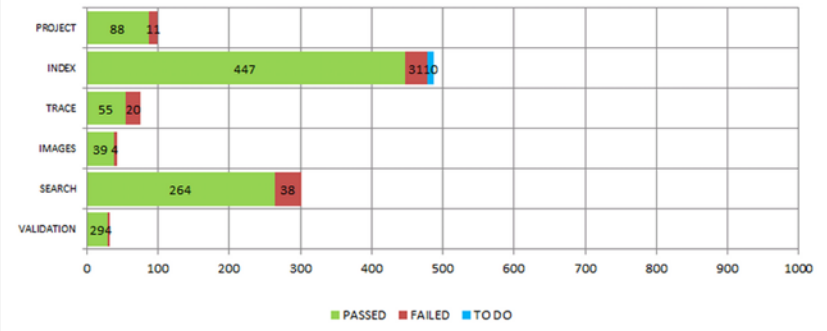
- Test Status - Demo
 - Test Status - Demo - sprint 27
 - AND/OR explained
 - BadGuy diff XIRAF and Hansken
 - Groupdoc Explained
 - Index pie-charts SP 27

Test Status - Demo - sprint 27

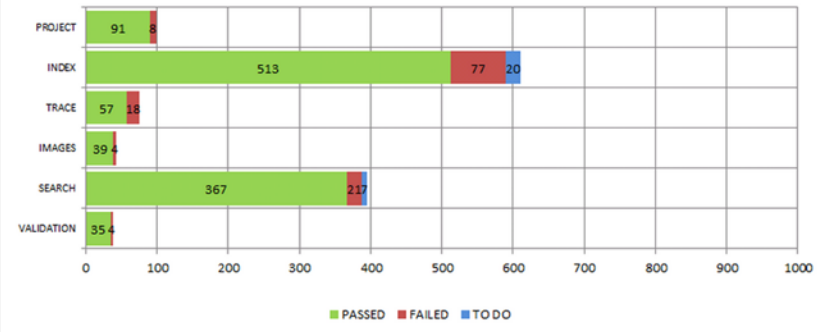
Created by [user], last modified on Mar 11, 2015

Status Hansken

- Status:**
- Date: 2015-02-18
 - Run: Release 0.19 - Bamboo build nr 2098 – issue 2335
 - Environment: OpenStack All-in-one
 - Main updates:
 - (Re-)validation of indexing Demo2013 (incl. XBOX), BadGuy and TestImage
 - Search Range Query
 - Validation Rest Call: Accept Headers, Method and MediaType



- Status:**
- Date: 2015-03-11
 - Run: Release 0.20- Bamboo build nr 2343
 - Environment: OpenStack All-in-one
 - Main updates:
 - ImageTool
 - Index/Analysis with NFI-format incl. encryption
 - Regression run with Firefly and Streams
 - Search AND, Or, Timeline Query
 - Many issues are resolved!





Current test set

> 7,500 unit tests

> 12,500 integration tests

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



Transparent analysis

DEMO




Hansken x +

localhost:9090/gui/#searchpage/search/1ce3da41-8fa4-41eb-85ba-f03ffcafd2d4/type%3Apicture type%3Afile/score- Zoeken

type:picture type:file

as Timeline, from to score (desc) 10 results Page 3 of 46 hits, found in 0.076 seconds.

summaries grid columns

date	size	name	types	mime	md5	
2015-02-12	61,211	picture1_6Thumbnails.jpg	file, picture	image/jpeg	a3f7c089aa61ab62a4d7a9b38295686c	
2015-02-12	787,434	picture1_WithoutThumbnail.jpg	file, picture	image/jpeg	791978e391e51835979c4a0d853a7b64	
2015-02-12	78,767	picture2_2Thumbnails.jpg	file, picture	image/jpeg	d80b31c1b9989230ffe62a0765989da2	
2015-02-12	132,874	picture3.jpg	file, picture	image/jpeg	9715519b69560b7e4ccebafe6ddd6f60	
2015-02-12	61,264	picture4.jpg	file, picture	image/jpeg	ad5294a30c2601d0a7322d919754f840	
2015-02-12	24,945	twopictures.jpg	file, picture	image/jpeg	fca735c06c254eee4c5f00ec3c998431	
2015-02-12	110,389	aab9b9638be5686022bae2d819f593e70e611d92	deleted, file, gps, picture	image/jpeg	ebaee670ce9da74692dc03e38bfbab8f	
2015-02-12	314,955	legorobot.jpg	deleted, file, picture	image/jpeg	a25515b1476fa0f351569fb7dbc25412	
2015-02-12		legorobot.jpg				view
deleted, file, picture		20150212-0000-0000-0000-000000000000:0-0-29-1				download
307.6 KB		/20150212-0000-0000-0000-000000000000///deleted/legorobot.jpg				
						
		add note				
2004-11-24	1,441	tomcat.gif	compressed, file, picture	image/gif	afdfa4a71ddab8f83677eda21fa989d5	
2015-02-12	436,438	GPS_ArubaDog.jpg	file, gps, picture	image/jpeg	92cee0e4eeacd4545d135a7eb19489f8	


Previous 1 2 3 4 5 Next



Hansken x +

localhost:9090/gui/#searchpage/search/1ce3da41-8fa4-41eb-85ba-f03ffcafd2d4/type%3Apicture type%3Afile/score- Zoeken

2015-02-12
deleted, file, picture
307.6 KB



legorobot.jpg
20150212-0000-0000-0000-000000000000:0-0-29-1
/20150212-0000-0000-0000-000000000000///deleted/legorobot.jpg

[view](#)
[download](#)

add note

data

raw	
entropy	7.979161142702118
hash	
md5	a25515b1476fa0f351569fb7dbc25412
sha1	8dad2fda9c7a9a5ec1d481aa4122ef508a831e08
sha256	bb8ac4ad2598cfef50b3ba9dd5d36b0b3b97dcafc5cbe740ffe45c0e901c0080
hashMisses	nsrl, lkpdb_kp
mimeType	image/jpeg
size	314955

deleted

file

accessedOn	2015-02-12T10:47:03.213Z
changedOn	2015-02-12T10:47:03.239Z
createdOn	2015-02-12T10:47:03.213Z
entryId	137
extension	jpg
modifiedOn	2015-02-12T10:47:03.239Z
name	legorobot.jpg
owner	S-1-5-32-544
path	/deleted/legorobot.jpg

picture

camera	W800i
digitizedOn	2006-10-30T12:39:59.000Z
exif	
colorSpace	sRGB



Hansken x +

localhost9090/gui/#searchpage/search/1ce3da41-8fa4-41eb-85ba-f03ffcafd2d4/type%3Apicture type%3Afile/score- Zoeken

tool	
meta	
analysisDuration	0
analysisStartedOn	2015-07-20T14:38:14.480Z
creator	snorkel/filesystem
properties	
data/digest/entropy	data.raw.entropy
data/digest/md5	data.raw.hash.md5
data/digest/sha1	data.raw.hash.sha1
data/digest/sha256	data.raw.hash.sha256
metadata/hashmatch	data.raw.hashMisses, data.raw.hashMisses
snorkel/filesystem	file.name, file.path, file.entryId, file.owner, file.extension, file.createdOn, file.accessedOn, file.modif...
traces/exif	picture.camera, picture.originalTakenOn, picture.modifiedOn, picture.digitizedOn, picture.exif.flash,...
traces/mime	data.raw.mimeType
traces/picture	picture.width, picture.height, previewTypes, previewData.image/jpeg
publishedOn	2015-07-20T14:35:27.954Z
success	traces/mime, traces/picture, traces/exif, nevis/file, document/document, metadata/hashmatch
types	
data	snorkel/filesystem
deleted	snorkel/filesystem
file	snorkel/filesystem
picture	traces/picture
version	
data/digest/entropy	0.1
data/digest/md5	0.1
data/digest/sha1	0.1
data/digest/sha256	0.1
document/document	1.0
metadata/hashmatch	1.0
nevis/file	1.0
snorkel/filesystem	1.0
text-processor	1.0



Netherlands Forensic Institute
Ministry of Security and Justice

Questions?

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