



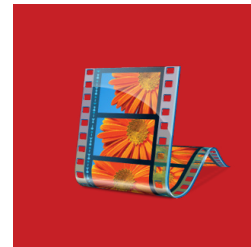
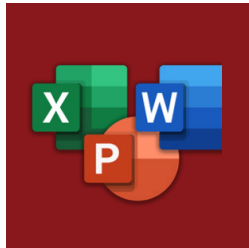
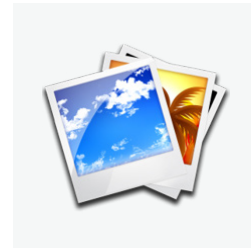
INSURANCE

FRAUD ON
CLAIM
DOCUMENTS



BANKING

KNOW
YOUR
CUSTOMER



OTHER

EXPENSE
FRAUD



Evidence-based validation of digital documents

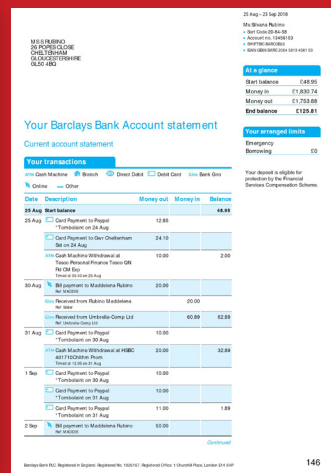
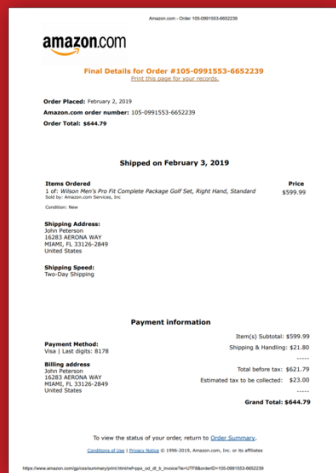
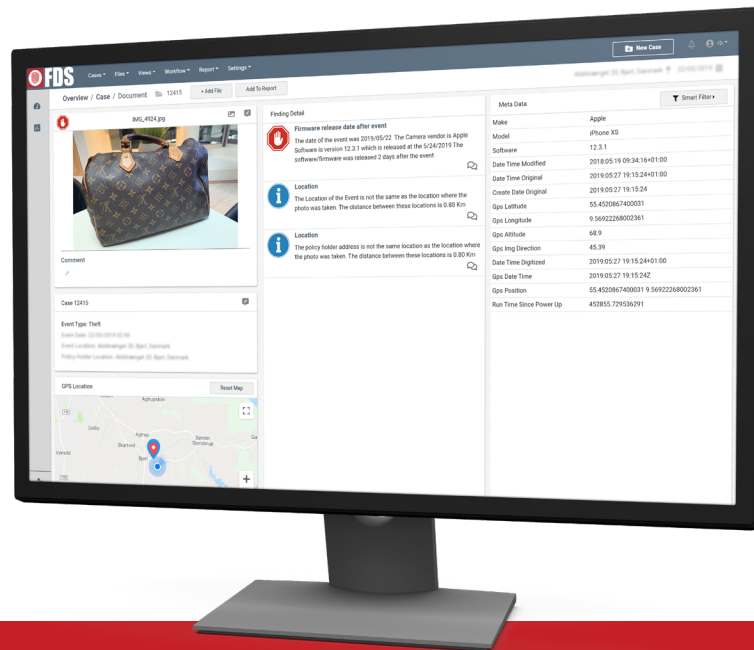
DETECTsystem has developed the Fraud Detect System (FDS), an advanced document validation platform for the purpose of disclosing false and fraudulent documentation



WHAT IS THE FDS PLATFORM?

FDS analyses a multitude of file types and utilizes over 100 detection methods to determine the validity of a document in seconds, such as claim forms, invoices, receipts, and identity documents.

Every branch and industry that are depending the authenticity of documents will experience benefits by using FDS on questionable documentation.



FILETYPES



Images: 1-2 seconds



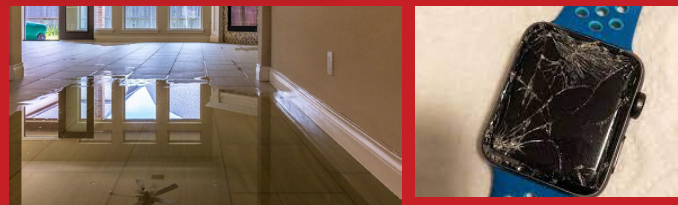
PDF Documents: 3-10 seconds



Office Documents: 3-8 seconds



Video and Recordings
FDS analyzes a range of video formats



Are any of these documents fraudulent?

THE NEEDLE IN THE HAYSTACK

Digital automation is an emerging core component for many organizations. Handling digital documents is becoming a vital part of the everyday business. Falsified and/or fraudulent documentation should be revealed in an efficient and reliable manner.



- ✓ FDS includes customizable workflows. The fully configurable data-driven detection model supports automation, as well as integration to current anti-fraud initiatives.
- ✓ A trained analyst can within 15-60 minutes analyse and verify a document. FDS provides you with tools to handle, conclude and report on any suspicious document in less than a minute.

DETECTION METHODS

The FDS Detection Engine utilizes +100 detection and cross-examination methods to determine the validity of submitted documents, and it delivers a reliable answer in seconds.



Intelligent Date Cross-check

Review all dates and timings encapsulated in the metadata and verify per taken-expectations via firmware, GPS dates, ICC-header, runtime since power-up, and additional parameters.



Advanced Location Detections

GPS location, satellite communication, and GPS within different range settings is verified according to the event location or the individual's home address.



Software and Editing Programs

FDS detect if documents have been edited in any software- or editing programs and can highlight new annotations, fonts, and modifications. FDS also alerts if the thumbnail is different from the submitted image.



PDF History and Deep Inspection

FDS analyzes revision changes done to a PDF Document, its source code, and it takes all layers apart to detect any manipulation or added layers. Additional features includes pixel-by-pixel and side-by-side comparisons.



Device and Firmware Release

FDS has a database currently consisting of +65,000 firmware and device release dates, to verify if a device or firmware was released prior to the create date of a submitted document.



Error Level Analysis (ELA)

FDS features an advanced Error Level Analysis that adds an extra layer of detection, highlighting where modifications have been done to an image, even if it has been flattened.

KEY FEATURES

The data-driven Detection Engine includes a full-featured rule and detection designer, report designer, and knowledge management (Q/A) designer utilized for risk assessments and analysis. Intelligent assignment and workflow ensure efficient processes and finally, KPI web dashboards are available in FDS and Excel.

UTILIZING FDS DATAPOINT

FDS ReFile helps insurers detect if a specific claim document has been used in previous claims, either internally or with other external insurers.

FDS FileStorm utilizes our database of millions of images to determine if a policy holder has downloaded documents from the internet, for use in an insurance claim. FDS FileStorm also covers documents that Google Image Search and TinEye don't have access to. With the patent-pending technology, FDS Cubes, photo analysis and comparison are revolutionized.

FDS Heritage alerts if a document has been generated online. Many suspicious websites provide services to create fake digital documentation such as invoices, receipts, and others.

EXAMPLES OF USE

The FDS platform is utilized by insurers, banks, accounting firms, lawyers and private organizations. Below is a brief excerpt of some area of use:

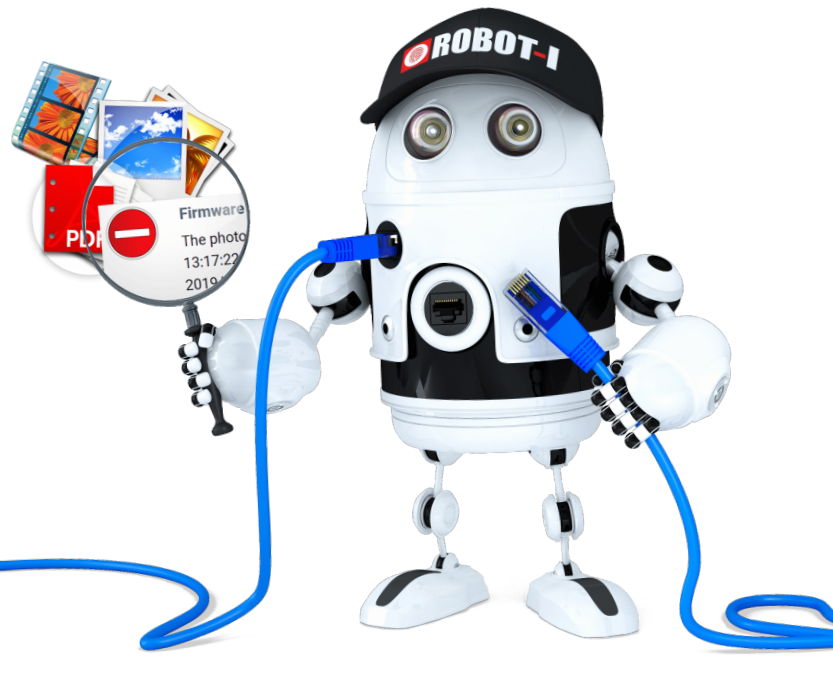
- ✔ A policy holder submits images of stolen items to an insurance claim. FDS reveals that photos are taken on a date after the alleged burglary and/or from a different location to the event location.
- ✔ A consumer who applies to open a bank account, obtain a credit card or loan must provide identity documentation. Basic computer skills make it possible to manipulate for instance proof-of-residence documentation such as utility bills, payslips or contract of employment. FDS can reveal such manipulation.
- ✔ An employee could make up private expenses such as travel expenses or additional office-supplies. Additional names such as family members could have been removed from travel documentation, and expense receipts could have been generated online.



AUTOLOAD ROBOT

With FDS AutoLoad Robot all documents submitted via web-frontend, TPA portals, or API can be automatically imported into FDS with results presented in seconds and referred to the correct department.

The FDS RESTful API is build to ensure that the Detection Engine enables a secure STP (straight-through-processing) environment with full integration abilities to other systems.



E-MAIL ROBOT

The E-mail Robot can be integrated into multiple shared mailboxes where it automatically extracts attached documents and any required information with upload for detection in FDS.

- ✔ It is easy to deploy and requires limited IT resources to implement.

FDS INTERACTIVE ROBOTICS

FDS Interactive Robotics can intelligently integrate into to a web frontend of any STP platform and interact live with employees, customers or policy holders. If uploaded documents are missing metadata or any discrepancies reside in the submitted documentation, the interactive robot will ask relevant questions or request further documentation.

- ✔ With the FDS platform, organizations can validate documents in real-time and swiftly resolve any found anomalies.



See the full video: detectsystem.com

To stay competitive, insurers need to transform parts of their operating models. As claims management accounts for approx. 28,5% of the operational cost, insurers need to build an operational power curve with disruptive technology.

Clear objectives with FDS



Improve fraud detection rate

Helping you improve screening processes to detect fraudulent claims and thereby reduce fraudulent payouts.



Improve operational cost

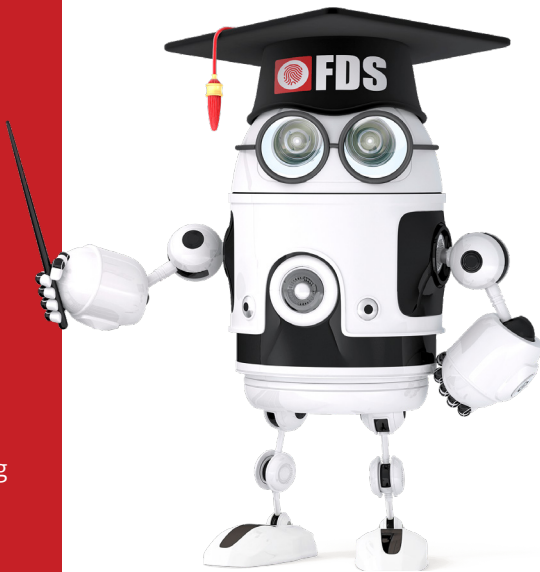
FDS automation improves claims handling and ensures that resources are only spent on evidence-based fraud and not wasted on legitimate claims.



Enhance customer value

Driving data innovation and facilitating a secure real-time STP strategy with fraud detection that meets customer expectations.

Free and remote training via our online e-learning platform included



To learn more about DETECTsystem's FDS platform and how to improve claims management in the insurance industry, please contact us for an online demo.

In regard to Data Protection regulations: The FDS platform is installed on-premise within your organization. Therefore, the DETECTsystem team does not have access to any of your data or your customer's data.

45-minute online demo (via Microsoft Teams)

The 45-minute demo includes industry insights and a live demo of the FDS platform, and we will introduce you to the Proof-of-Concept process.

Proof of Concept

In a PoC you decide which documents you would like us to screen through FDS and we will provide you with a PoC report on the findings, including the time spent.

CONTACT US

Address:

DETECTsystem A/S
Tirsbækvej 191
7120 Vejle Øst
Denmark

Contact info:

Email: info@detectsystem.com

