

Triage for Windows Systems with Autopsy

Luca Tännler, Mathias Vetsch
26th October 2016

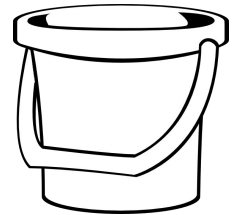
The Triage process



Known Good

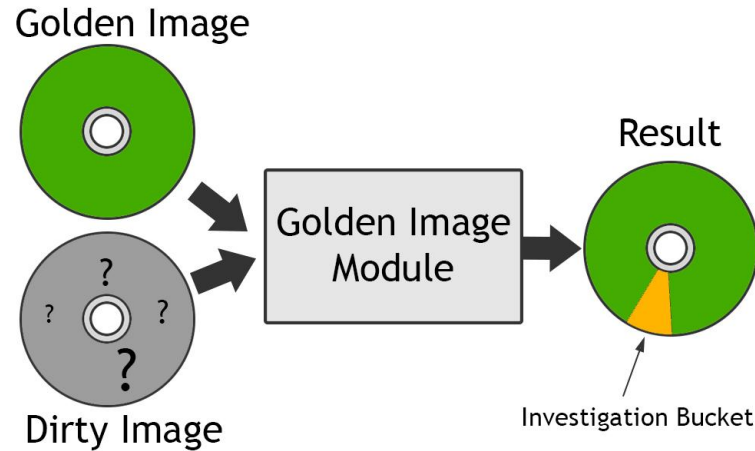


Known Bad



**Investigation
Bucket**

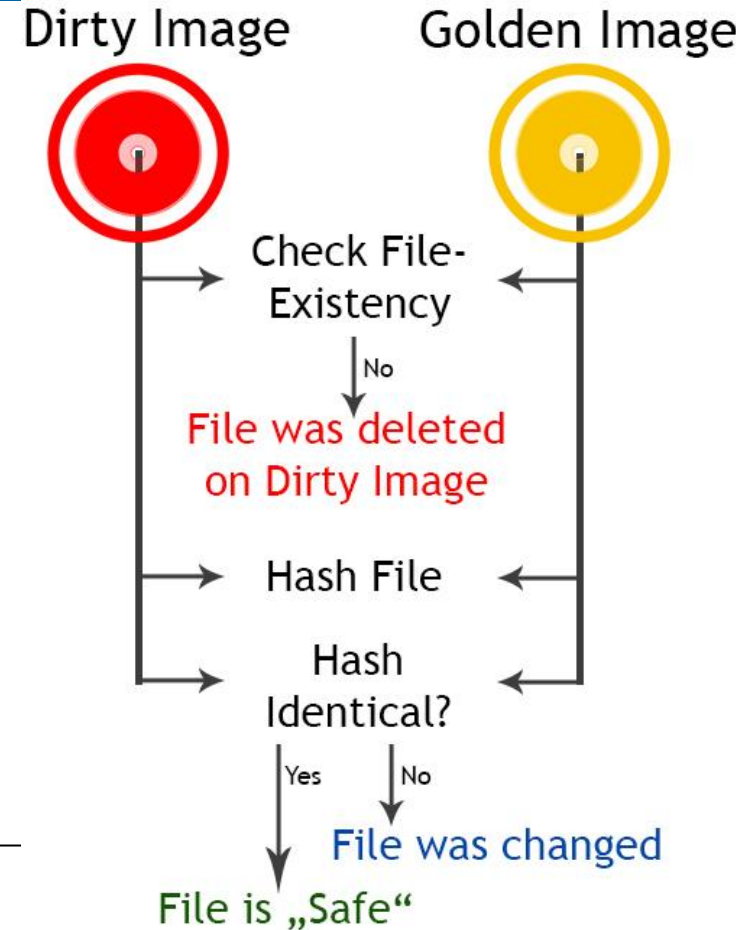
Golden Image Module



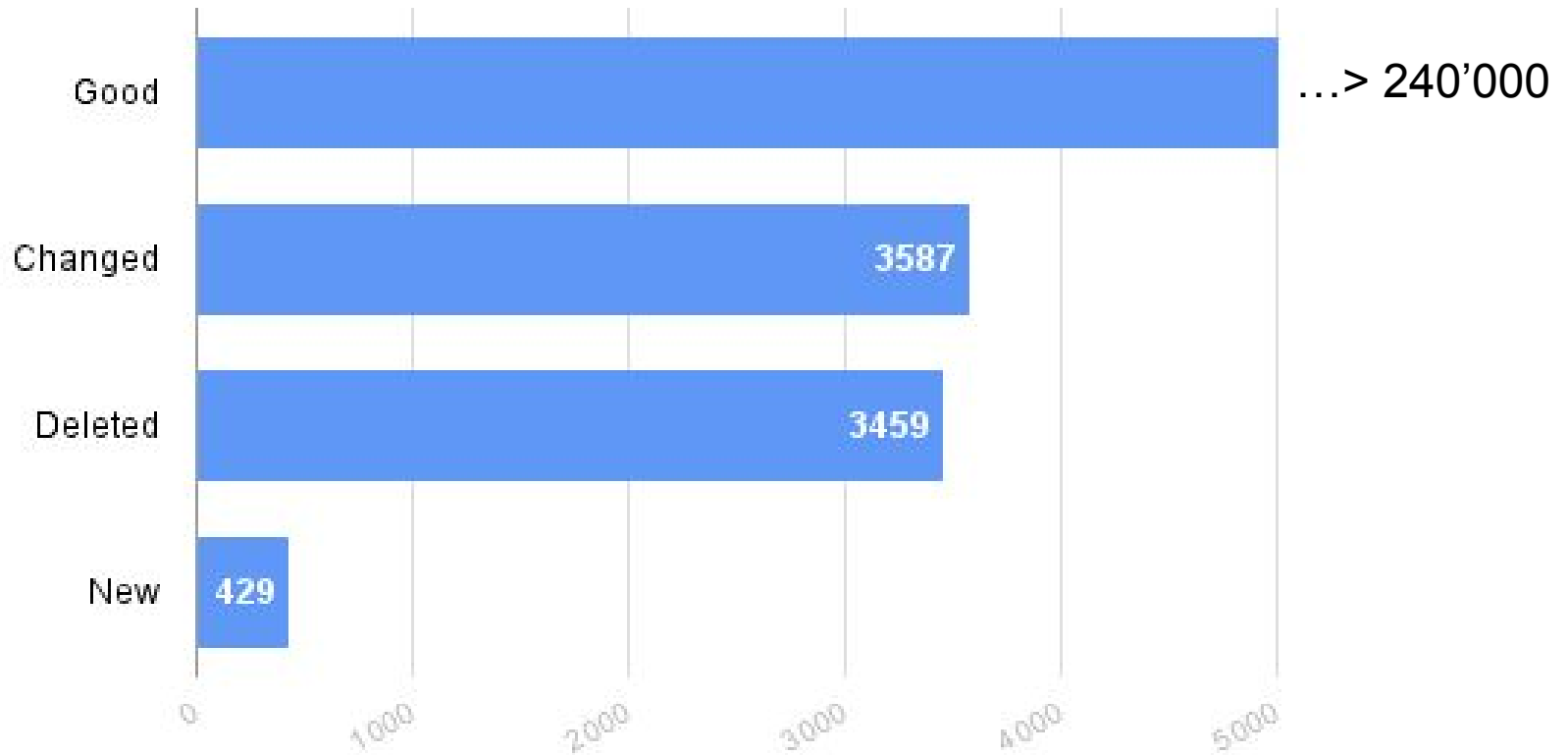
- **Suspicion a Windows computer was compromised**
- **What happened / changed?**
- **Huge set of data to be analyzed**

- **What is a “Golden Image”?**
 - f.Ex. Default Windows installation image
 - Often used in companies
- **What is a “Dirty Image”?**
 - Image based on the “Golden Image”
 - Possibly compromised / infected
- **What does it?**
 - Compare two images
 - “Dirty Image” vs. “Golden Image”
- **What is it good for?**
 - Reduce the set of data for further analysis

- **Iterate through “Golden Image”**
 - Check if file exists on “Dirty Image”
 - Hash Files
 - Compare Files
- **Tag Files**
 - “Safe”
 - Deleted
 - Changed



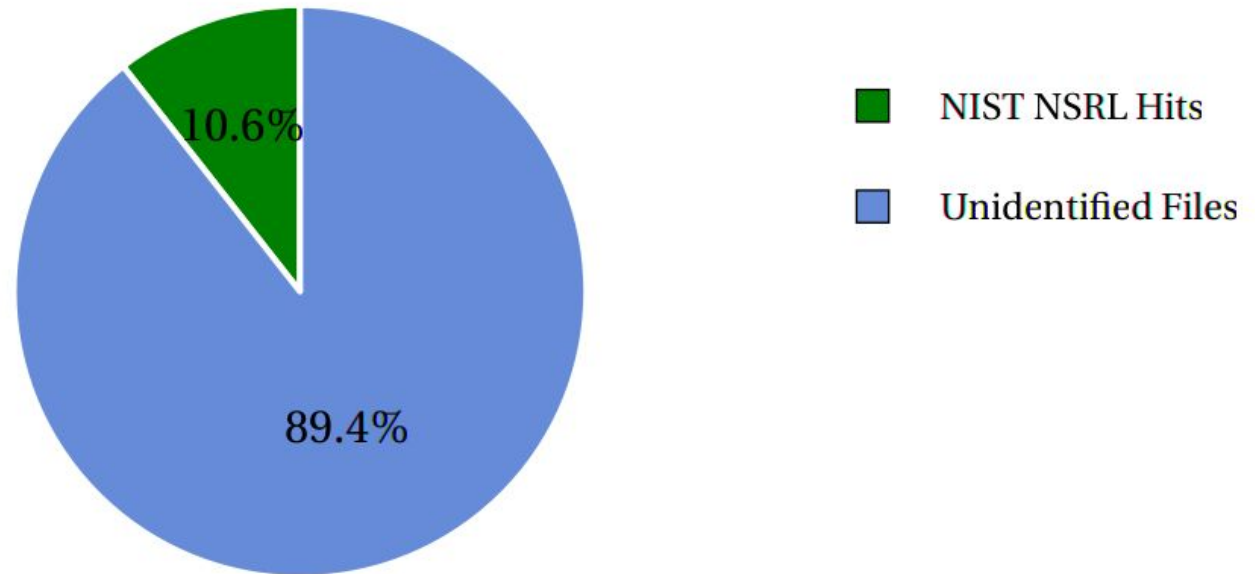
Benchmarking: Reboot



- **File Search / Comparison**
 - Independent from **filename** and **path**
 - Meta Data comparison

Eliminate Known Windows Files

■ NSRL HashSet



■ AuthentiCode

- Integrity
- Publisher Identification
- No Quality mark
- 2 different types



Embedded Signatures



— 00e6f1d5c22...b402505
— 15766f2be92...411ae7a
— c2d57383936...d14b523
— ee680b01dba...11cdfa5

Detached Signatures

Embedded Signatures



File Ingest Module

1. Look for a signature in the PE Header
2. Verify the certificate
3. Check the integrity of the Binary

Detached Signatures

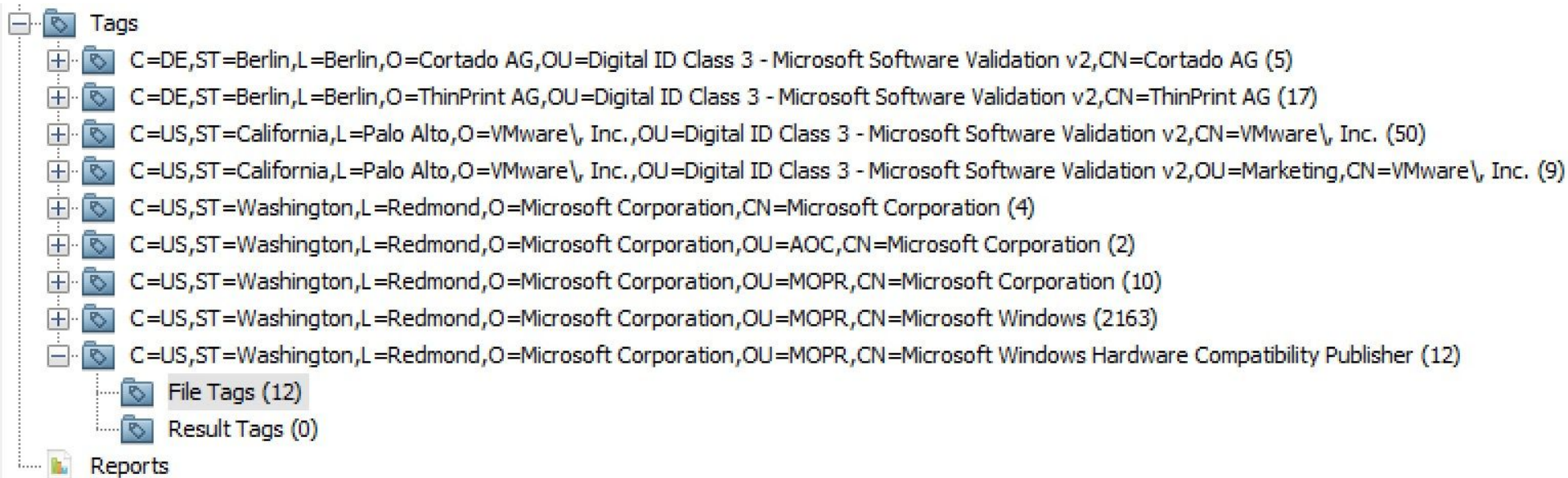


Data Source Ingest Module

1. Find all signed *.cat Files on a data source
2. Create a data structure with all signed hashes
3. Compute hashes of all files on the data source
4. Find the hashes in the data structure from step 2

Tag all matches with the publisher Name

■ The files are now grouped by Publisher





■ Certificate Metadata in a Content Viewer Module

Directory Listing

C=US,ST=Washington,L=Redmond,O=Microsoft Corporation,OU=MOPR,CN=Microsoft Windows Hardware Compatibility Publisher File Tags

TableThumbnail

File	File Path	Comment	Modified Time	Changed Time
 vmusbmouse.inf	/img_Win7Raw.dd/vol_vol3/Program Files/Common Files/VMware/Driv...	Signed by vmusbmouse.cat #14098	2014-03-22 02:06:52 MEZ	2014-11-26 23:18:55 MEZ
 vmmouse.inf	/img_Win7Raw.dd/vol_vol3/Program Files/Common Files/VMware/Driv...	Signed by vmmouse.cat #14094	2014-03-22 02:06:24 MEZ	2014-11-26 23:18:55 MEZ

<

HexStringsFile MetadataResultsIndexed TextMediaTagsAuthentiCode

The following AuthentiCode Information where found on the Image

Signature Found in:

vmusbmouse.inf

Signer

C=US,ST=Washington,L=Redmond,O=Microsoft Corporation,OU=MOPR,CN=Microsoft Windows Hardware Compatibility Publisher

Issuer

C=US,ST=Washington,L=Redmond,O=Microsoft Corporation,OU=Copyright (c) 2002 Microsoft Corp.,CN=Microsoft Windows Hardware Compatibility PCA

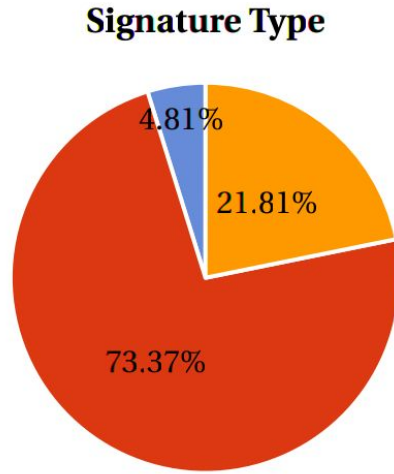
Valid From

Mon Dec 19 23:40:20 CET 2011

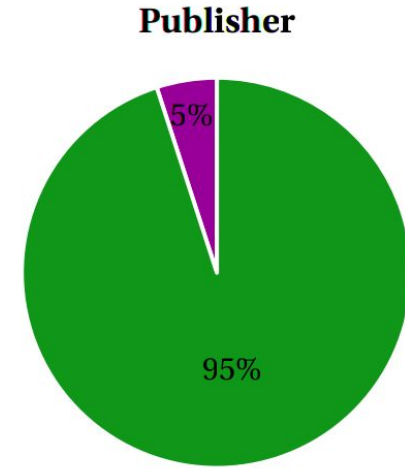
Valid Until

Tue Mar 19 23:40:20 CET 2013

■ Benchmarking



- Embedded Signatures
- Detached Signatures
- Files without Signature



- Microsoft
- 3rd Party (Drivers)



TagFilter Module

- **Several tags**
 - Some have same/similar meaning
 - f.Ex. “Known-Good/Bad” Tags
- **Currently in Autopsy: List per tag**
- **Limited Filters**
- **No listing of all “Known Good/Bad” files**

The Solution

Tag Filter Configuration


TAG Filter Configuration

 Add Filter  Add Filter Group

Datasource: All Datasources ▼

AND ▼	File	Doesn't Contain ▼	DI_Changed ▼	↓ ↑ ×
AND ▼	File	Doesn't Contain ▼	DI_Safe ▼	↓ ↑ ×

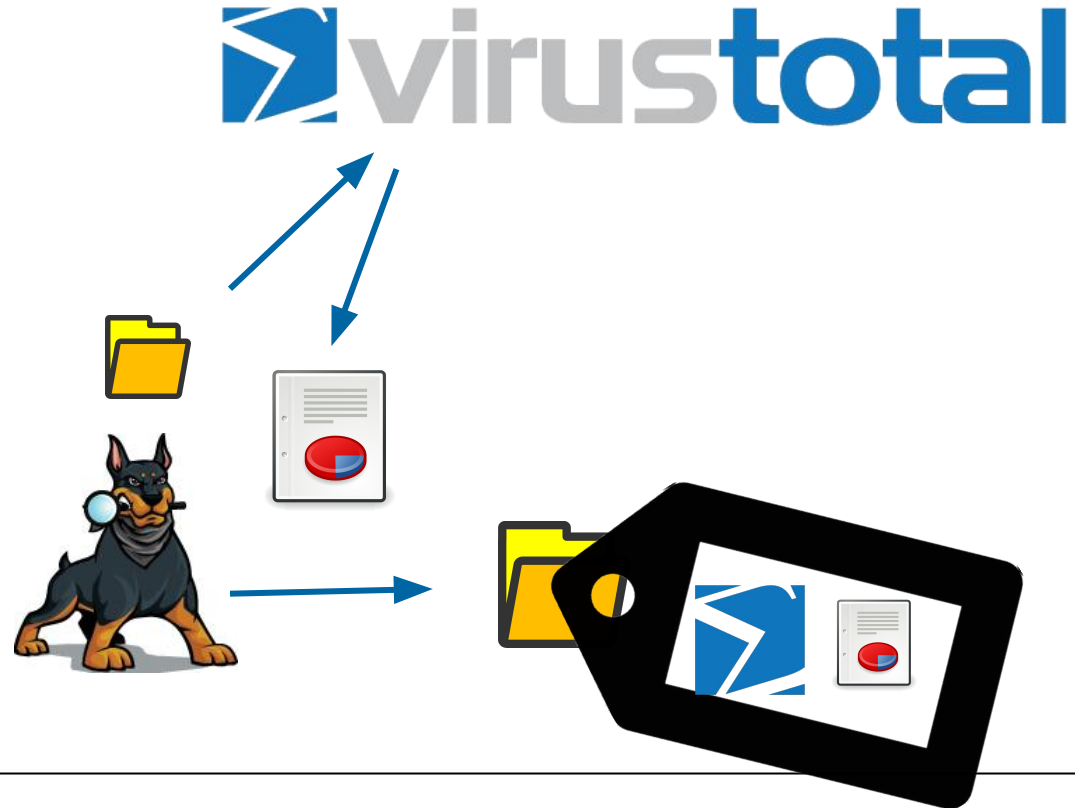
◀ ||| ▶

 Filter

- **Advanced filter options**
 - Change-/Create-date
 - Further Meta Data
- **Export of results**
- **Add Feature: Save Filter**
- **Run modules over filtered data**

VirusTotal Module

- Online Virus Database
- API key required
- Request are limited



There are more possibilities

- **OpenIOC Scanner**
- **Cuckoo Sandbox Interface**

What we loved

- **Open Source**
- **Extensible by design**
- **Provides a broad base**

What we missed

- **Documentation coverage is low**
- **No dynamic workflow possible**
 - Not possible to run modules over set of data/file
- **Content is not indexed properly**

Q & A