Representing Recoverability of Unallocated Files using CASE/UCO

This document describes the approach, and associated property bundle, CASE uses for representing the recoverability of an unallocated file's name, metadata and content.

Decision: Although the File property bundle already has an *allocationStatus* property to indicate whether a file is allocated or unallocated, it is also necessary to represent three facets of recoverability of an unallocated file:

1. content (data)
2. file name (dirent)
3. metadata (e.g., NTFS MFT Standard Information Attribute, Unix inode).

Scope: This document covers unallocated files with recoverable filename and/or metadata. This document does not cover carved content, which is represented using the DataRange and ContentData property bundles as a range of data within any data source (see https://github.com/casework/case/blob/master/examples/reconstructed_file.json).

Property Bundle

The *UnallocatedRecoverability* property bundle is used to represent the recoverability of unallocated files using the following property names and associated values for representing recoverability status:

Property	**Values**
nameStatus	• recoverable • overwritten • unknown
metadataStatus	• recoverable • overwritten • unknown
contentStatus	• recoverable • potentially recoverable • overwritten • unknown

When using this property bundle, for completeness and clarity, it is recommended to specify values for all three properties.

Descriptive JSON-LD Examples

Illustrative examples are provided here to cover conditions commonly encountered when recovering unallocated files. These examples concentrate on NTFS, but can be translated to other files systems such as EXT.

When information is recoverable, it is represented explicitly in these examples. Recoverable metadata are represented using the File property bundle, including fileName and filePath, and additional file system metadata are represented using the MftRecord property bundle. In addition, the location of a recoverable file in a specific data source is represented using

the PathRelation property bundle on a “contained-within” Relationship (e.g., targeting a specified DiskPartition trace). Similarly, recoverable content is represented using the DataRange property bundle on a “contained-within” Relationship.

1) Fully Recoverable

The simplest case of representing an unallocated file that is fully recoverable. For example, a resident file on NTFS with the file name, metadata, and content all recoverable.


```
{
  "@id": "file-fullyrecoverable-38e5cd74-19b2-3f0c-b324-1c4b25a34f12",
  "@type": "Trace",
  "propertyBundle": [
   {
    "@type": "File",
    "createdTime": "2018-01-27T10:01:23.54Z",
    "extension": "jpg",
    "fileName": "IMG-425634.JPG",
    "fileSystemType": "NTFS",
    "filePath": "C:/SecretStash/IMG-425634.JPG",
    "isDirectory": false,
    "allocationStatus": "unallocated",
    "sizeInBytes": 4138616
   },
   {
    "@type": "UnallocatedRecoverability",
    "nameStatus": "recoverable",
    "metadataStatus": "recoverable",
    "contentStatus": "recoverable",
   },
   {
    "@type": "MftRecord",
    "mftFileID": "424356",
    "mftRecordChangeTime": "2018-01-27T10:01:23.54Z",
    "mftFileNameCreatedTime": "2018-01-27T10:01:23.54Z",
   },
   {
    "@type": "ContentData",
    "hash": [
     {
      "@type": "Hash",
      "hashMethod": "SHA256",
      "hashValue":
"ed1b9496953a9e9d2e797fb68fee7150cfb9e6d3ff97c0f64a35068264672918"
     }
    ],
    "sizeInBytes": 4138616
```

```
      }
     ]
  },
  {
    "@id": "datarange-relationship1",
    "@type": "Relationship",
    "source": "file-fullyrecoverable-38e5cd74-19b2-3f0c-b324-1c4b25a34f12",
    "target": "diskpartition1-46d3ae54-23a4-2e1a-a563-2c4b25a35d36",
    "kindOfRelationship": "contained-within",
    "isDirectional": true,
    "propertyBundle": [
     {
      "@type": "DataRange",
      "rangeOffset": 45156,
      "rangeSize": 4138616
     }
    ]
   },
  {
    "@id": "filepath-relationship1",
    "@type": "Relationship",
    "source": "file-fullyrecoverable-38e5cd74-19b2-3f0c-b324-1c4b25a34f12",
    "target": "diskpartition1-46d3ae54-23a4-2e1a-a563-2c4b25a35d36",
    "kindOfRelationship": "contained-within",
    "isDirectional": true,
    "propertyBundle": [
     {
      "@type": "PathRelation",
      "path": "C:/SecretStash/IMG-425634.JPG"
     }
    ]
   },
```


2) Potentially Recoverable Content

Representing an unallocated file with recoverable name and metadata, and the content potentially recoverable. For example, a non-resident file on NTFS with the file name and metadata recoverable, including which clusters were allocated to the file, with no indication that the content has been overwritten.

Note: In certain contexts, there may not be a way to definitively authenticate that the actual, original content is recoverable. However, it might be possible to raise the confidence level of a non-resident file from potentially recoverable to recoverable. For instance, if the content contains traits (e.g., header signature + content size value in the header + creation timestamp in the header) that are all compatible with the metadata, then a forensic tool or forensic examiner might be confident enough to assert that the content is recoverable, as represented in Example 1 above.

```
{
   "@id": "file-potentiallyrecoverable-38e5cd74-19b2-3f0c-b324-1c4b25a34f12",
   "@type": "Trace",
   "propertyBundle": [
    {
     "@type": "File",
     "createdTime": "2018-01-27T10:00:19.32Z",
     "extension": "jpg",
     "fileName": "IMG-416451.JPG",
     "fileSystemType": "NTFS",
     "filePath": "C:/SecretStash/IMG-416451.JPG",
     "isDirectory": false,
     "allocationStatus": "unallocated",
     "sizeInBytes": 4021529
    },
    {
     "@type": "UnallocatedRecoverability",
     "nameStatus": "recoverable",
     "metadataStatus": "recoverable",
     "contentStatus": "potentially recoverable",
    },
    {
     "@type": "MftRecord",
     "mftFileID": "532552",
     "mftRecordChangeTime": "2018-01-27T10:00:19.32Z",
     "mftFileNameCreatedTime": "2018-01-27T10:00:19.32Z",
    },
    {
     "@type": "ContentData",
     "hash": [
      {
       "@type": "Hash",
       "hashMethod": "SHA256",
       "hashValue":
"5f635be55c83a3dff3c771f4b4b36202f79d4bc0c109bd83d9609cf45a47b23c"
      }
     ],
     "sizeInBytes": 4021529
    }
   ]
 },
 {
   "@id": "datarange-relationship2",
   "@type": "Relationship",
   "source": "file-potentiallyrecoverable-38e5cd74-19b2-3f0c-b324-1c4b25a34f12",
```

```
    "target": "diskpartition1-46d3ae54-23a4-2e1a-a563-2c4b25a35d36",
    "kindOfRelationship": "contained-within",
    "isDirectional": true,
    "propertyBundle": [
     {
      "@type": "DataRange",
      "rangeOffset": 5635584,
      "rangeSize": 4021529
     }
    ]
   },
  {
    "@id": "filepath-relationship2",
    "@type": "Relationship",
    "source": "file-potentiallyrecoverable-38e5cd74-19b2-3f0c-b324-1c4b25a34f12",
    "target": "diskpartition1-46d3ae54-23a4-2e1a-a563-2c4b25a35d36",
    "kindOfRelationship": "contained-within",
    "isDirectional": true,
    "propertyBundle": [
     {
      "@type": "PathRelation",
      "path": "C:/SecretStash/IMG-416451.JPG"
     }
    ]
   },
```


3) Overwritten Content

Representing an unallocated file with recoverable name and metadata, but the content has been overwritten by a more recent file.


```
  {
    "@id": "file-contentoverwritten-38e5cd74-19b2-3f0c-b324-1c4b25a34f12",
    "@type": "Trace",
    "propertyBundle": [
     {
      "@type": "File",
      "createdTime": "2018-01-27T10:11:45.19Z",
      "extension": "jpg",
      "fileName": "IMG-436357.JPG",
      "fileSystemType": "NTFS",
      "filePath": "C:/SecretStash/IMG-436357.JPG",
      "isDirectory": false,
      "allocationStatus": "unallocated",
      "sizeInBytes": 4142567
     },
```

```
      {
       "@type": "UnallocatedRecoverability",
       "nameStatus": "recoverable",
       "metadataStatus": "recoverable",
       "contentStatus": "overwritten",
      },
      {
       "@type": "MftRecord",
       "mftFileID": "646210",
       "mftRecordChangeTime": "2018-01-27T10:11:45.19Z",
       "mftFileNameCreatedTime": "2018-01-27T10:11:45.19Z",
      },
      {
       "@type": "ContentData",
       "hash": [
        {
         "@type": "Hash",
         " numberHashes": "0",
        }
       ],
       "sizeInBytes": 0
      }
    ]
  },
  {
    "@id": "datarange-relationship3",
    "@type": "Relationship",
    "source": "file-contentoverwritten-38e5cd74-19b2-3f0c-b324-1c4b25a34f12",
    "target": "diskpartition1-46d3ae54-23a4-2e1a-a563-2c4b25a35d36",
    "kindOfRelationship": "contained-within",
    "isDirectional": true,
    "propertyBundle": [
     {
      "@type": "DataRange",
      "rangeOffset": 8931840,
      "rangeSize": 4142567
     }
    ]
   },
  {
    "@id": "filepath-relationship3",
    "@type": "Relationship",
    "source": "file-contentoverwritten-38e5cd74-19b2-3f0c-b324-1c4b25a34f12",
    "target": "diskpartition1-46d3ae54-23a4-2e1a-a563-2c4b25a35d36",
    "kindOfRelationship": "contained-within",
    "isDirectional": true,
    "propertyBundle": [
```

```
    {
     "@type": "PathRelation",
     "path": "C:/SecretStash/IMG-436357.JPG"
    }
   ]
  },
```


4) Unknown Content

Representing an unallocated file with recoverable name and metadata, but the status of content is unknown. For example, an entry in the $LogFile on NTFS includes filename and metadata, but does not contain information about where the content was allocated.


```
{
   "@id": "file-contentunknown-38e5cd74-19b2-3f0c-b324-1c4b25a34f12",
   "@type": "Trace",
   "propertyBundle": [
    {
     "@type": "File",
     "createdTime": "2018-01-27T10:38:34.02Z",
     "extension": "jpg",
     "fileName": "IMG-445138.JPG",
     "fileSystemType": "NTFS",
     "filePath": "C:/SecretStash/IMG-445138.JPG",
     "isDirectory": false,
     "allocationStatus": "unallocated",
     "sizeInBytes": 4031432
    },
    {
     "@type": "UnallocatedRecoverability",
     "nameStatus": "recoverable",
     "metadataStatus": "recoverable",
     "contentStatus": "unknown",
    },
    {
     "@type": "MftRecord",
     "mftFileID": "732615",
     "mftRecordChangeTime": "2018-01-27T10:38:34.02Z",
     "mftFileNameCreatedTime": "2018-01-27T10:38:34.02Z",
    }
   ]
},
{
   "@id": "filepath-relationship4",
   "@type": "Relationship",
   "source": "file-contentunknown-38e5cd74-19b2-3f0c-b324-1c4b25a34f12",
   "target": "diskpartition1-46d3ae54-23a4-2e1a-a563-2c4b25a35d36",
```

```
    "kindOfRelationship": "contained-within",
    "isDirectional": true,
    "propertyBundle": [
     {
      "@type": "PathRelation",
      "path": "C:/SecretStash/IMG-445138.JPG"
     }
    ]
   },
```


5) Filename Overwritten

Representing an unallocated file with recoverable metadata and content, but the filename is unrecoverable. For example, an EXT inode is recoverable but the associated dirent has been overwritten.


```
  {
    "@id": "file-nameoverwritten-38e5cd74-19b2-3f0c-b324-1c4b25a34f12",
    "@type": "Trace",
    "propertyBundle": [
     {
      "@type": "File",
      "createdTime": "2018-01-27T10:41:54.15Z",
      "fileSystemType": "NTFS",
      "isDirectory": false,
      "allocationStatus": "unallocated",
      "sizeInBytes": 4111296
     },
     {
      "@type": "UnallocatedRecoverability",
      "nameStatus": "overwritten",
      "metadataStatus": "recoverable",
      "contentStatus": "recoverable",
     },
     {
      "@type": "MftRecord",
      "mftFileID": "835267",
      "mftRecordChangeTime": "2018-01-27T10:41:54.15Z",
      "mftFileNameCreatedTime": "2018-01-27T10:41:54.15Z",
     },
     {
      "@type": "ContentData",
      "hash": [
       {
        "@type": "Hash",
        "hashMethod": "SHA256",
        "hashValue":
"b372b227b118112f1f31070d6844a4c3872cb4a6cbe34ddaa625b719986c7a40"
```

```
        }
       ],
       "sizeInBytes": 4111296
     }
    ]
  },
  {
    "@id": "relationship4",
    "@type": "Relationship",
    "source": "file-nameoverwritten-38e5cd74-19b2-3f0c-b324-1c4b25a34f12",
    "target": "diskpartition1-46d3ae54-23a4-2e1a-a563-2c4b25a35d36",
    "kindOfRelationship": "contained-within",
    "isDirectional": true,
    "propertyBundle": [
     {
      "@type": "DataRange",
      "rangeOffset": 9931776,
      "rangeSize": 4111296
     }
    ]
   },
```