Representing Content Extracted from Network Traffic using CASE/UCO

This document describes how CASE can be used to represent content extracted from captured network traffic and saved into files on storage media.

Overview Diagram

The following diagram proposes an approach to representing content extracted from network traffic and saved onto storage media. The direction of transfer is represented in the relationship between the extracted content and the associated network connection.

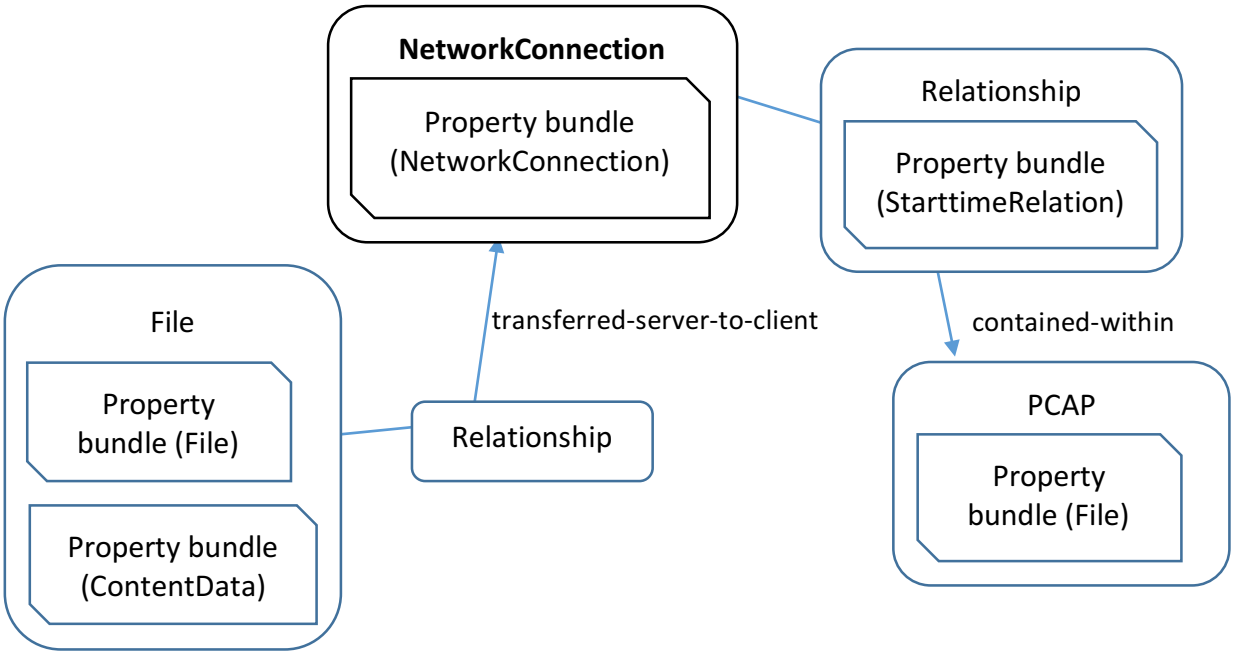

Figure: Depiction of content extracted from captured network traffic (contained within a PCAP file) and saved into files on storage media.

Descriptive JSON-LD Examples

This illustrative example is provided to show how CASE is used to represent payload content extracted from captured network traffic and saved into files on storage media.

```
{
 "@type": "Tool",
 "@id": "pcap-tool-uuid",
 "creator": "PCAPAnalyser",
 "toolType": " PCAParser",
 "version": "3.5"
},
{
 "@type": "InvestigativeAction",
 "@id": "extraction-action-uuid",
```

```
  "createdBy": "investigator1-uuid",
  "createdTime": "2017-09-29T11:47:54.2889922Z",
  "propertyBundle": [
   {
    "@type": "ActionReferences",
    "instrument": "pcap-tool-uuid",
    "object": [
     "pcap-provenancerecord-uuid"
    ],
    "result": [
     "extracted-connections-provenancerecord-uuid"
    ]
   }
  ],
  "endTime": "2017-09-29T11:47:54.2889922Z",
  "name": "extracted"
 },
 {
  "@type": "ProvenanceRecord",
  "@id": "pcap-provenancerecord-uuid",
  "createdBy": "81ee357b-5fc1-5aa8-b932-ff29ace0f65b",
  "createdTime": "2017-09-29T11:47:54.2889922Z",
  "description": "Parsed packet capture files",
  "object": [
   "pcap-file-uuid"
  ]
 },
 {
  "@type": "Trace",
  "@id": "pcap-file-uuid",
  "createdBy": "81ee357b-5fc1-5aa8-b932-ff29ace0f65b",
  "createdTime": "2017-09-29T11:47:54.2889922Z",
  "propertyBundle": [
   {
    "@type": "File",
    "createdTime": "2009-04-03T02:28:42.0086110Z",
    "extension": "pcap",
    "fileName": "20090402-scenario.pcap",
    "isDirectory": false,
    "modifiedTime": "2009-04-03T03:31:26.0521980Z",
    "sizeInBytes": 6337357
   },
   {
    "@type": "ContentData",
    "dataPayloadReferenceURL": "E:\\Traffic\\20090402-scenario.pcap",
    "hash": [
     {
```

```
        "@type": "Hash",
        "hashMethod": "MD5",
        "hashValue": "dd7558b16eae4d582d7b4608e85d862a"
       }
     ],
    }
  ]
},
{
  "@type": "ProvenanceRecord",
  "@id": "extracted-connections-provenancerecord-uuid",
  "createdBy": "investigator1-uuid",
  "createdTime": "2017-09-29T11:47:54.2889922Z",
  "description": "Network connections and files parsed with PCAParser",
  "object": [
    "network-connection1-uuid",
    "network-connection2-uuid",
    "network-connection3-uuid",
    "file1-uuid",
    "file2-uuid",
    "file3-uuid"
  ]
},
{
  "@type": "Trace",
  "@id": "source-host-uuid",
  "createdBy": "investigator1-uuid",
  "createdTime": "2017-09-29T11:47:54.2889922Z",
  "propertyBundle": [
    {
      "@type": "IPv4Address",
      "value": "10.10.10.2"
    },
    {
      "@type": "DomainName",
      "value": "EOGHANMACBOOK"
    }
  ]
},
{
  "@type": "Trace",
  "@id": "destination-host-uuid",
  "createdBy": "investigator1-uuid",
  "createdTime": "2017-09-29T11:47:54.2889922Z",
  "propertyBundle": [
    {
      "@type": "IPv4Address",
```

```
      "value": "10.10.10.50"
     },
     {
      "@type": "DomainName",
      "value": "JHL-IDNOLHYSVIA"
     }
    ]
   },
   {
    "@type": "Trace",
    "@id": "network-connection1-uuid",
    "createdBy": "investigator1-uuid",
    "createdTime": "2017-09-29T11:47:54.2889922Z",
    "propertyBundle": [
     {
      "@type": "NetworkConnection",
      "startTime": "2009-04-03T02:29:25.6256260Z",
      "endTime": "2009-04-03T02:29:25.6365510Z",
      "dst": "destination-host-uuid",
      "destinationPort": 139,
      "src": "source-host-uuid",
      "sourcePort": 52960,
      "protocols": "TCP, NETBIOSSESSIONSERVICE",
      "connectionState": "APSF"
     }
    ]
   },
   {
    "@type": "Trace",
    "@id": "network-connection2-uuid",
    "createdBy": "investigator1-uuid",
    "createdTime": "2017-09-29T11:47:54.2889922Z",
    "propertyBundle": [
     {
      "@type": "NetworkConnection",
      "startTime": "2009-04-03T02:29:25.6264620Z",
      "endTime": "2009-04-03T02:29:25.6369450Z",
      "dst": "destination-host-uuid",
      "destinationPort": 139,
      "src": "source-host-uuid",
      "sourcePort": 52961,
      "protocols": "TCP, NETBIOSSESSIONSERVICE",
      "connectionState": "APSF"
     }
    ]
   },
   {
```

```
 "@type": "Trace",
 "@id": "network-connection3-uuid",
 "createdBy": "investigator1-uuid",
 "createdTime": "2017-09-29T11:47:54.2889922Z",
 "propertyBundle": [
  {
   "@type": "NetworkConnection",
   "startTime": "2009-04-03T02:29:25.6370540Z",
   "endTime": "2009-04-03T02:29:25.6475500Z",
   "dst": "destination-host-uuid",
   "destinationPort": 139,
   "src": "source-host-uuid",
   "sourcePort": 52962,
   "protocols": "TCP, NETBIOSSESSIONSERVICE",
   "connectionState": "APSF"
  },
  }
 ]
},
{
"@id": "trace-relationship1-uuid",
"@type": "Relationship",
"source": "network-connection1-uuid",
"target": "pcap-file-uuid",
"kindOfRelationship": "contained-within",
"isDirectional": "true"
 "propertyBundle": [
  "@type": "StarttimeRelation",
  "startTime": "2009-04-03T02:29:25.6256260Z"
 ]
}
{
"@id": "trace-relationship2-uuid",
"@type": "Relationship",
"source": "network-connection3-uuid",
"target": "pcap-file-uuid",
"kindOfRelationship": "contained-within",
"isDirectional": "true"
 "propertyBundle": [
  "@type": "StarttimeRelation",
  "startTime": "2009-04-03T02:29:25.6264620Z"
 ]
}
{
"@id": "trace-relationship3-uuid",
"@type": "Relationship",
"source": "network-connection3-uuid",
```

```
      "target": "pcap-file-uuid",
      "kindOfRelationship": "contained-within",
      "isDirectional": "true"
       "propertyBundle": [
        "@type": "StarttimeRelation",
        "startTime": "2009-04-03T02:29:25.6370540Z"
       ]
      },
      {
       "@type": "Trace",
       "@id": "file1-uuid",
       "createdBy": "investigator1-uuid",
       "createdTime": "2017-09-29T11:47:54.2889922Z",
       "propertyBundle": [
        {
         "@type": "File",
         "accessedTime": "2009-04-03T02:40:15.2790160Z",
         "extension": "html",
         "fileName": "index.html",
         "isDirectory": false,
         "sizeInBytes": 1009
        },
        {
         "@type": "ContentData",
         "dataPayloadReferenceURL":
"C:\\Users\\formation\\Desktop\\NMP2_12217597\\AssembledFiles\\10.10.10.50\\TCP-
80\\index.html",
          "hash": [
           {
            "@type": "Hash",
            "hashMethod": "MD5",
            "hashValue": "49e69aa023559898c6be330972eeb9d7"
           }
          ],
          "sizeInBytes": 1009
        }
       ]
      },
      {
       "@type": "Relationship",
       "@id": "trace-relationship4-uuid",
       "createdBy": "investigator1-uuid",
       "createdTime": "2017-09-29T11:47:54.2889922Z",
       "isDirectional": true,
       "kindOfRelationship": "transferred-server-to-client",
       "source": "file1-uuid",
       "target": "network-connection1-uuid"
```

```
    },
    {
     "@type": "Trace",
     "@id": "file2-uuid",
     "createdBy": "investigator1-uuid",
     "createdTime": "2017-09-29T11:47:54.2889922Z",
     "propertyBundle": [
      {
       "@type": "File",
       "accessedTime": "2009-04-03T02:40:15.4869790Z",
       "extension": "jpg",
       "fileName": "snakeoil1.jpg",
       "isDirectory": false,
       "sizeInBytes": 49327
      },
      {
       "@type": "ContentData",
       "dataPayloadReferenceURL":
"C:\\Users\\formation\\Desktop\\NMP2_12217597\\AssembledFiles\\10.10.10.50\\TCP-
80\\images\\snakeoil1.jpg",
       "hash": [
        {
         "@type": "Hash",
         "hashMethod": "MD5",
         "hashValue": "05726c7d9a10e8de26b89911e3e8f094"
        }
       ],
       "sizeInBytes": 49327
      }
     ]
    },
    {
     "@type": "Relationship",
     "@id": "trace-relationship5-uuid",
     "createdBy": "investigator1-uuid",
     "createdTime": "2017-09-29T11:47:54.3045922Z",
     "isDirectional": true,
     "kindOfRelationship": "transferred-server-to-client",
     "source": "file2-uuid",
     "target": "network-connection2-uuid"
    },
    {
     "@type": "Trace",
     "@id": "file3-uuid",
     "createdBy": "investigator1-uuid",
     "createdTime": "2017-09-29T11:47:54.3045922Z",
     "propertyBundle": [
```

```
        {
         "@type": "File",
         "accessedTime": "2009-04-03T02:40:15.4839730Z",
         "extension": "jpg",
         "fileName": "snakeoil2.jpg",
         "isDirectory": false,
         "sizeInBytes": 115674
        },
        {
         "@type": "ContentData",
         "dataPayloadReferenceURL": "C:\\Users\\formation\\Desktop\\NMP2_12217597
\\AssembledFiles\\10.10.10.50\\TCP-80\\images\\snakeoil2.jpg",
          "hash": [
           {
            "@type": "Hash",
            "hashMethod": "MD5",
            "hashValue": "441994ff99d6e4bb68cd12bda18d4422"
           }
          ],
          "sizeInBytes": 115674
        }
       ]
      },
      {
       "@type": "Relationship",
       "@id": "trace-relationship5-uuid",
       "createdBy": "investigator1-uuid",
       "createdTime": "2017-09-29T11:47:54.3045922Z",
       "isDirectional": true,
       "kindOfRelationship": "transferred-server-to-client",
       "source": "file3-uuid",
       "target": "network-connection3-uuid"
      },
```