Representing Network Connections in Captured Network Traffic using CASE/UCO

This document describes an approach, and associated property bundle, to use case in order to represent network connections in captured network traffic (e.g., PCAP).

Overview Diagram

The following diagram provides an overview of how a Relationship (StarttimeRelation) is used to link network connections with captured network traffic (e.g., PCAP file).

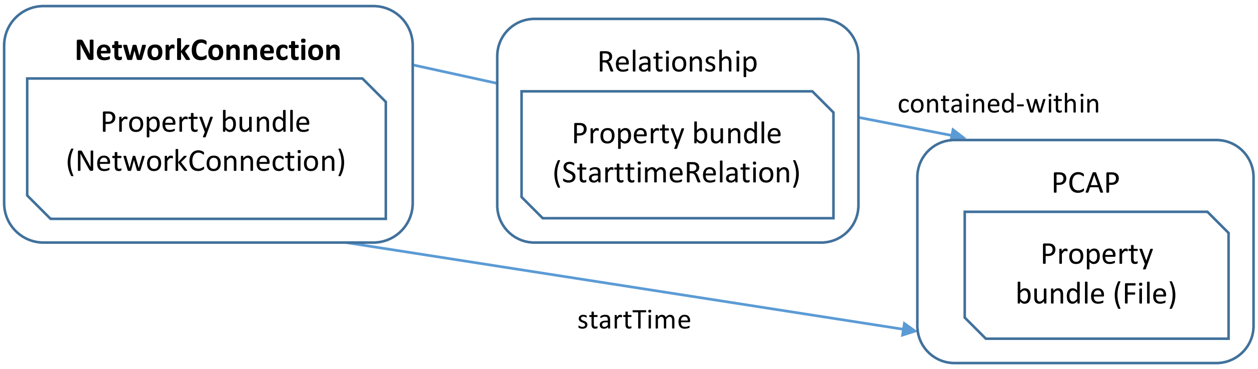

Figure: Depiction of a NetworkConnection contained within a PCAP file.

Property Bundles

The *NetworkConnection* property bundle is used to represent metadata for bi-directional connections within captured or live network traffic. A bi-directional TCP connection is represented using a single NetworkConnection object. Two new properties are proposed to represent the state of a network connection: overallState and connectionState.

Property	**Description**
src	Source of network connection
dst	Destination of network connection
sourcePort	Source port used in the network connection, as an integer in the range of 0 - 65535
destinationPort	Destination port used in the network connection, as an integer in the range of 0 - 65535
protocols	Protocols involved in the network connection
startTime	Start time of network connection
endTime	End time of network connection
overallState	Status of a network connection ESTABLISHED, LISTENING, CLOSED, UNKNOWN, etc.
connectionState	Aggregated TCP flags observed in any direction (RS = SYN and RST but no data, APSF = 3-way handshake with data and Fin-termination)

Descriptive JSON-LD Examples

This illustrative example is provided to show how CASE is used to represent network connections in captured traffic (e.g., PCAP file).

```
{
  "@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"
  ]
},
{
  "@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"
      ]
    },
```