CASE Ontology: Status and Future

EVIDENCE2E-CODEX / EXEC / E-EVIDENCE JOINT CONFERENCE

DIGITAL CROSS-BORDER COOPERATION IN CRIMINAL JUSTICE

Bruxelles, 22nd January 2020

Mattia Epifani, CNR-IGSG, Italy

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468
CASE is a community-developed specification language whose primary aim is the interoperability to enable the exchange of cyber-investigation information between tools and organisations and ultimately between countries:

- strengthening **admissibility** (authenticity, provenance)
- providing **trustworthy information**
- helping in **dual/multiple tools validation or results validation/comparison** (deduplication of results)
- enabling more **advanced and comprehensive correlation and analysis**.
Cyber-investigation Analysis Standard Expression

2015-03 Initial ideas presented (DI-12-1, 102-110)
2017-07 CASE introduction paper (DI-22, 14-45)
2018-04 specification workshop → first roadmap
2018-08 community formalization started:
    2018-11 bylaws
    2019-01 governance committee elected
    2019-01 code of conduct
    2019-02 ontology committee (charter)
    2019-04 caseontology.org
2019-06 specification workshop → roadmap to version 1.0
www.caseontology.org
CASE Committees

Governance Committee
- Secretary: Cory Hall
  - MITRE

Presiding Director: Eoghan Casey
  - University of Lausanne

Government Class Director: Ryan Griffith
  - DOD Cyber Crime Center

Commercial Class Director: Jessica Hyde
  - Magnet Forensics

Non-profit Class Director: Richard Brown
  - Project VIC

Academic Class Director: Sanjin Lee
  - Korea University

Chair: Alex Nelson
  - NIST

Co-chair: Ryan Hohimer
  - DarkLight

Ontology Committee: all classes: 2+ contributors
- Chair: Alex Nelson
  - NIST
- Co-chair: Ryan Hohimer
  - DarkLight

Adoption Committee: Vik Harichandran
  - MITRE
- Andrew Sovern
  - MITRE

Technical Director: Harm van Beek
  - Netherlands Forensic Institute

DIGITAL CROSS-BORDER COOPERATION IN CRIMINAL JUSTICE
Bruxelles, 22nd Jan 2020
Developed tools

- **Digital Forensics Tools Catalogue**
  - Catalogue of more than 1500 acquisition and analysis tools, categorized on features, license type and platform

- **CASE Generator**
  - Application useful to generate UCO/CASE language object

- **CASE Converter**
  - Intermediate software layer developed to convert the output of a forensic tool in UCO/CASE standard

- **EESP Application**
  - Platform to manage, import/export and prepare EP
Digital Forensics Tools Catalogue

- About **1500 tools mapped**
- Acquisition and Analysis tools
- Tools categorized based on
  - **Features** (Computer/Mobile/Network)
  - **License type** (Free/Commercial/Only LE)
  - **Platform** (Windows/Linux/MacOS)
Digital Forensics Tools Catalogue

10. Forensics Utilities

09. Forensics/E-Discovery Toolkit

- File Recovery/Carving
- Keyword search
- Timeline
- Password / Cracking Recovery
- Stego Analysis

08. Cross Analysis

07. Anti Forensics

06. Malware Forensics

05. Memory Forensics

04. Network Forensics

03. Mobile Forensics

02. File Analysis

- File Viewer
- File Metadata Extraction

01. Computer Forensics

- File System
- Operating System
- Application
- Virtualization Forensics
- Cloud Forensics
- Social Networking
- Windows
- Apple
- Linux
- Browser
- Chat/IM
- Email
- P2P
- CD / DVD

iOS
- Android
- Blackberry
- Symbian
- Chinese
- Others

Smartphone / Tablet

SIM Card
NAV
The Digital Forensics Tools Catalogue has been developed within the activity of the EVIDENCE project (funded by the European Union's Seventh Framework Programme, under the grant agreement No. 608185) by the Institute of Legal Information Theory and Technique of the National Research of Council of Italy. It contains the most relevant information about a huge number of digital forensics tools, concerning the Acquisition and Analysis phases. The collection has been organized using a specific categorization, both for the Analysis and the Acquisition.

Currently the Catalogue comprises information on the most significant digital forensics tools related to: Acquisition: 464 tools - Analysis: 1045 tools The total number of software tools collected so far is 1,509.

Choose your path

SEARCH
The Digital Forensics Tools Catalogue has been developed within the activity of the EVIDENCE project, funded by the European Union's Seventh Framework Programme, under the grant agreement No. 607777, and with the support of the Ministry of Legal Information Theory and Technique of the National Research Council of Italy. It contains relevant information about a huge number of digital forensics tools, concerning the Acquisition and Analysis phases. The collection has been organized using a specific categorization, both for the Acquisition and Analysis categories.

Currently the Catalogue comprises information on the most significant digital forensics tools. Acquisition: 464 tools - Analysis: 1045 tools. The total number of software tools collected amounts to 1,509.

Choose your path

[SEARCH]
The Digital Forensics Tools Catalogue has been developed within the activity of the EVIDENCE project, which is a three-year initiative under the European Union’s Seventh Framework Programme, under the grant agreement No. 257668. The project is coordinated by the National Research Council of Italy, Institute of Legal Information Theory and Technique of the National Research Council of Italy. The catalogue has been organized by a huge amount of digital forensics tools, concerning the Acquisition phase. The collection has been organized using a specific categorization, both for the Acquisition phase. The catalogue comprises information on the most significant digital forensics tools. The total number of software tools collected in the Catalogue is 1084.

Choose your path

SEARCH

01. Computer Forensics
   01.01. File System
   01.02. Operating System
   01.02.01. Windows
   01.02.02. Apple
   01.02.03. Linux
   01.03. Application
   01.03.01. Browser
   01.03.02. Chat
   01.03.03. Cloud Storage
   01.03.04. Email
   01.03.05. Peer To Peer
   01.03.06. Social Networking
   01.04. Virtualization
   01.05. CD/DVD
Case Generator

- Application useful to generate UCO / CASE language object

- It can be used by
  - LE / JA to describe non-technical actions
  - FL to describe technical actions

- For example a «Search and Seizure» action
  - Authorization (JA)
  - Performer (LE)
  - Location
  - Result
Example: digital evidence sharing

Provenance Chain

Device Acquisition

Extraction

Decoding

Parsed Content

Analysis ↔ Reporting

Sharing

- Request for Examination (scope)
- Tools & Versions
- Serial #s, Evidence Desc, Acquisition Hash
- Case & Scenario Descriptors, Organization that retain evidence
- Case name/repository

- Investigator Actors/Actions
- Device Owner Information
- Authorization (Consent, Authority, Scope, Banners, Warranties)
- Chain of Custody
- Temporal Metadata of actions

- Files/Traces
- Pictures
- Videos
- Audio Files
- Documents
- Database Files
- Emails
- Messages (SMS, MMS, 3rd party apps)
- Call logs

- Contacts
- Filesystems
- Location Info
- Installed Apps
- Passwords, Tokens, Credentials
- URLs, Browser History
- Network (Traffic, IPs, Domains, etc.)
- Device info parsed from filesystem
Example: digital evidence sharing
# Search and Seizure

<table>
<thead>
<tr>
<th>manufacturer</th>
<th>Samsung</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>SM-G900F</td>
</tr>
<tr>
<td>IMEI</td>
<td>356765064657669</td>
</tr>
<tr>
<td>Serial Number</td>
<td>FDG764192</td>
</tr>
<tr>
<td>Storage capacity</td>
<td>64 GB</td>
</tr>
<tr>
<td>Clock setting</td>
<td>2018-05-31 6:00</td>
</tr>
<tr>
<td>Mobile account</td>
<td>+393319420019</td>
</tr>
<tr>
<td>Item number</td>
<td>ITEM_00001</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Carrier</th>
<th>Telecom Italia</th>
</tr>
</thead>
<tbody>
<tr>
<td>SimType</td>
<td>SIM</td>
</tr>
<tr>
<td>SIMForm</td>
<td>Micro SIM</td>
</tr>
<tr>
<td>ICCID</td>
<td>89390100001847875453</td>
</tr>
<tr>
<td>IMSI</td>
<td>222014603559590</td>
</tr>
<tr>
<td>Phone Number</td>
<td>393319420019</td>
</tr>
<tr>
<td>PIN</td>
<td>7571</td>
</tr>
<tr>
<td>PUK</td>
<td>86245177</td>
</tr>
</tbody>
</table>
Search and Seizure

**Investigative Action**

- **Name**: Search and Seizure
- **Instrument**: Authorization 20181002@[79D6AB]
- **Description**: Search and seizure

**Tool Arguments**

- **Name**: 
- **Value**: 

**Performer**: Anton Grubitz@[B1C22D51-4A3F-4353-84FB-E210B5EFDA48]

**Location**: Heinrich-Grüber-Straße 118 Berlin Germany@[582CAF46-0F32-4A77-9A5F-3D576F994011]

**Select source (Trace or Provenance Record)**

**Object**: 

**Result**

- **Provenance Record**: Samsung SM-G900F of Maria Sieland voluntarily handed over to the LEA IT_2018_00150 @[A2C173]
- **Provenance Record**: Samsung SM-G900F of Maria Sieland voluntarily handed over to the LEA IT_2018_00150 @[A2C17345]

**Add provenance record**
**Modify provenance record**
**Remove provenance record**

**List Provenance Records**

- Samsung SM-G900F of Maria Sieland voluntarily handed over to the LEA IT_2018_00150 @[A2C173]
- Samsung SM-G900F of Maria Sieland voluntarily handed over to the LEA IT_2018_00150 @[A2C17345]
Search and Seizure

- **Performer**: Anton Grubitz@{B1C22D51-4A3F-4353-84FB-E210B5EFDA48}
- **Location**: Heinrich-Grüber-Straße 118 Berlin Germany@{582CAF46-0F32-4A77-9A5F-3D576F994011}

**Result**

- **Provenance Record**: Samsung SM-G900F of Maria Sieland voluntarily handed over to the LEA IT_2018_00150@{A2C173-5}

**List Provenance Records**

- Samsung SM-G900F of Maria Sieland voluntarily handed over to the LEA IT_2018_00150@{A2C17345-1}
Search and Seizure

Investigative Action

Name: Search and Seizure

Instrument: Authorization 20181002@[79D6AB]

Description: Search and seizure

Tool Arguments

Name:
Value:

Add  Modify  Remove

Performer: Anton Grubitz@[B1C22D51-4A3F-4353-84FB-E21085EFDA48]

Location: Heinrich-Grüber-Straße 118 Berlin Germany@[582CAF46-0F32-4A77-9A5F-3D576F994011]

Select source (Trace or Provenance Record)

Object:

Result

Provenance Record: Samsung SM-G900F of Maria Sieland voluntarily handed over to the LEA IT_2018_00150 @A2C173-

Add provenance record  Modify provenance record  Remove provenance record

List Provenance Records

Samsung SM-G900F of Maria Sieland voluntarily handed over to the LEA IT_2018_00150 @A2C17345K
### Search and Seizure

#### Trace Mobile Device

<table>
<thead>
<tr>
<th>Device</th>
<th>Mobile Device</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Manufacturer</strong></td>
<td>Samsung</td>
</tr>
<tr>
<td><strong>Model</strong></td>
<td>SM-G900F</td>
</tr>
<tr>
<td><strong>Serial no.</strong></td>
<td>FDG764192</td>
</tr>
<tr>
<td><strong>IMEI</strong></td>
<td>356765064657669</td>
</tr>
<tr>
<td><strong>Storage capacity</strong></td>
<td>64 GB</td>
</tr>
<tr>
<td><strong>Clock setting</strong></td>
<td>10 06 2018 08:30:14</td>
</tr>
</tbody>
</table>

#### iPhone Device

| **Unique ID**  |  |
| **Owner name** |  |

#### Mobile Account

| **MSISDN**    | +393319420019 |

#### Mobile traces

```json
{"@id":"FF3B5D29-F5DF-4599-801B-C13ED606B428","@type":"Trace","propertyBundle":[]}
```
### Search and Seizure

**Trace Mobile Device**

<table>
<thead>
<tr>
<th>Device</th>
<th>Mobile Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Samsung</td>
</tr>
<tr>
<td>Model</td>
<td>SM-G900F</td>
</tr>
<tr>
<td>Serial no.</td>
<td>FDG764192</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### iPhone Device

<table>
<thead>
<tr>
<th>Unique ID</th>
<th>Owner name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Mobile Account

<table>
<thead>
<tr>
<th>MSISDN</th>
</tr>
</thead>
<tbody>
<tr>
<td>+393319420019</td>
</tr>
</tbody>
</table>

#### Operating System

<table>
<thead>
<tr>
<th>Name</th>
<th>Manufacturer</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Clock setting

- 10:06:2018 08:30:14

---

**Note:**

The image includes a screenshot of a software interface for tracing mobile devices, with specific details about a Samsung device's IMEI, storage capacity, and clock setting. The MSISDN is also provided.
### Search and Seizure

**Trace Mobile Device**

<table>
<thead>
<tr>
<th><strong>Device</strong></th>
<th><strong>Mobile Device</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Samsung</td>
</tr>
<tr>
<td>Model</td>
<td>SM-G900F</td>
</tr>
<tr>
<td>Serial no.</td>
<td>FDG764192</td>
</tr>
<tr>
<td>IMEI</td>
<td>356765064657669</td>
</tr>
<tr>
<td>Storage capacity</td>
<td>64 GB</td>
</tr>
<tr>
<td>Clock setting</td>
<td>10:06:2018 08:30:14</td>
</tr>
</tbody>
</table>

**iPhone Device**

- **Unique ID**: 
- **Owner name**: 

**Mobile Account**

- **MSISDN**: +393319420019

**Mobile traces**

```
{
    "@id": "FF3B5D29-F5DF-4599-801B-C13ED606B428",
    "@type": "Trace",
    "propertyBundle": {
        "@type": "Device",
        "manufacturer": "Samsung",
        "model": "SM-G900F"
    }
}
```
Representing a “Mobile Device”

```json
{
  "@type": "suspect-device-uuid",
  "@type": "Trace",
  "propertyBundle": [
    {
      "@type": "Device",
      "manufacturer": "iPhone",
      "model": "MG552",
      "serialNumber": "F18Q4LGRG5MD"
    },
    {
      "@type": "MobileDevice",
      "keypadUnlockCode": "123789",
      "IMEI": "359305065690067",
      "MSISDN": "suspect-mobileaccount-uuid",
      "clockSetting": "2019-03-30T22:36:24.35Z",
      "localeLanguage": "en",
      "phoneActivationTime": "2018-05-09T07:36:24.35Z",
      "storageCapacity": "16 GB"
    }
  ],
  "@type": "iPhoneDevice",
  "uniqueID": "B3858A69A29375E6C706226B3633A3A11EBD2A774",
  "ownerName": "Loki iPhone"
}
```
Forensic Acquisition

SELECT EXTRACTION TYPE

Advanced Logical
Disable/Re-Enable User Lock
File system
Physical

Camera
Screenshot

Lock Bypass
Lock Bypass
Lock Bypass
Lock Bypass

ABORT
BACK
Forensic Acquisition

- Mobile devices (1)
  - SM-G900F Samsung (+393319420019)
- SIMs (1)
  - Micro SIM Vodafone Italia
- FILES (8)
  - Samsung GSM_SM-G900F_Galaxy_S5.zip (234567890018)
  - Samsung GSM_SM-G900F_Galaxy_S5_Logical.ufd (3096)
  - Report.xml (102400)
  - blk0_mmcblk0.bin (16985678911)
  - blk32_mmcblk0rpmb.bin (4912670)
  - procdat.zip (10784652)
  - log.txt (1024)
  - Samsung GSM_SM-G900F_Galaxy_S5_Physical.ufd (1024)
Forensic Acquisition

**Investigative Action**

<table>
<thead>
<tr>
<th>Name</th>
<th>Forensic Acquisition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Instrument</strong></td>
<td>UFED 4PC (Physical A.)#Extraction 7</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Mobile device physical acquisition</td>
</tr>
</tbody>
</table>

**Tool Arguments**

```
"ExtractionType":"Physical"
"UFEDExtractionMethod":"ADB_Rooted"
```

**Performer**

Investigator @ {CC5F1E8B-9B80-4D41-AE7A-9A5343368106}

**Location**

Piazza Navona Rome Italy@ {309BC178-1836-4787-AA15-94EA3A2C7401}

**Select source (Trace or Provenance Record)**

Object

Samsung SM-G900F of Lamberto Laudisi transferred to FEG IT_2018_FEGeeks_00192 @ {96398C01-778B-4F8}`
Forensic Acquisition

Investigative Action

Name: Forensic Acquisition
Instrument: UFED 4PC (Physical A.)#Extraction 7
Description: Mobile device physical acquisition

Start time: 19 06 2018 12:17:31
End time: 19 05 2018 12:47:32

Tool Arguments:
"ExtractionType":"Physical"
"UFEDExtractionMethod":"ADB_Rooted"

Performer: Investigator @{CC5F1E8B-9B80-4D41-AE7A-9A5343368106}
Location: piazza Navona Rome Italy@{309BC178-1836-47B7-AA15-94EA3A2C7401}

Object: Samsung SM-G900F of Lamberto Laudisi transferred to FEG IT_2018_FEGeeks_00192 @{96398C01-778B-4F8}
Forensic Acquisition

Investigative Action

Name: Forensic Acquisition
Instrument: UFED 4PC (Physical A.)#Extraction 7
Description: Mobile device physical acquisition

Tool Arguments:
"ExtractionType":"Physical"
"UFEDExtractionMethod":"ADB_ROOTED"

Performer: Investigator @{CC5F1E8B-9B80-4D41-AE7A-9A5343368106}
Location: piazza Navona Rome Italy@{309BC178-1836-47B7-AA15-94EA3A2C7401}

Object: Samsung SM-G900F of Lamberto Laudisi transferred to FEG IT_2018_FEGeeks_00192 @{96398C01-778B-4F8}
Forensic Acquisition

<table>
<thead>
<tr>
<th>Provenance Record</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Acquisition (dump blk0.bin) EFGGeeks_00192_004 @90F73123-DB7E-41E5-B6CA-493B96E4E</td>
<td></td>
</tr>
</tbody>
</table>

**List Provenance Records**

- Physical Acquisition (dump blk0.bin) EFGGeeks_00192_004 @90F73123-DB7E-41E5-B6CA-493B96E4E
- Physical Acquisition (dumprpmb.bin) EFGGeeks_00192_005 @97C74753-FCEB-49C8-A611-7A70EF46
- Physical Acquisition (procdata.zip) EFGGeeks_00192_006 @EBAB06EE-7522-42D6-96EA-E3121D67E3
- Physical Acquisition (log.txt) EFGGeeks_00192_007 @48C0F0B8-9A63-45EE-99BE-23CC354C3252
Representing a “Forensic Acquisition”

INVESTIGATIVE ACTION
Representing a “Forensic Acquisition” TOOL

```
{
    "@id": "tool-embeddedextractor1-uid",
    "@type": "Tool",
    "name": "Embedded Device Extractor",
    "toolType": "Extraction",
    "creator": "Harald",
    "version": "1.2.0",
    "propertyBundle": {
        "@type": "ToolConfiguration",
        "configurationSetting": [
            {
                "@type": "ConfigurationSetting",
                "itemName": "ExtractionMethod",
                "itemValue": "iOS Backup"
            },
            {
                "@type": "ConfigurationSetting",
                "itemName": "ExtractionType",
                "itemValue": "File System"
            }
        ]
    }
}
```
Representing a “Forensic Acquisition” RESULT
Example: digital evidence sharing
Examples of “Traces”

- Files
  - Pictures
  - Videos
  - Audios
  - Documents
  - Databases
- Email
- Contacts
- Messages (SMS, MMS, WhatsApp, Telegram, ecc.)
- Call Logs
- Browser History
- Location Info
- Network (IP, Domains, traffic)
Digital Forensics Tools Supporting CASE

- Autopsy
- Network Miner
AUTOPSY
AUTOPSY
AUTOPSY
Representing a forensic image

```json
{
    "@id": "data-source-1",
    "@type": "Trace",
    "propertyBundle": [ {
        "@type": "File",
        "filePath": "X:/CORPORA/pen02.E01"
    }, {
        "@type": "ContentData",
        "sizeInBytes": "2014314496"
    } ]
}
```
AUTOPSY
Representing a file

```
{
    "@id": "file-136",
    "@type": "Trace",
    "propertyBundle": [ {
        "@type": "File",
        "createdTime": "2013-04-03T18:00:21Z",
        "accessedTime": "2013-04-03T22:00:00Z",
        "modifiedTime": "2013-04-04T09:39:28Z",
        "extension": "docx",
        "fileName": "Carbonara.docx",
        "filePath": "/Sito/Carbonara.docx",
        "isDirectory": false,
        "sizeInBytes": "3039590"
    }, {
        "@type": "ContentData",
        "mimeType": "application/vnd.openxmlformats-officedocument.wordprocessingml.document",
        "hash": [ {
            "@type": "Hash",
            "hashMethod": "MD5",
            "hashValue": "1378f29e249ddada396a295b2d969a40"
        } ],
        "sizeInBytes": "3039590"
    } ]
}
```
AUTOPSY

Relationship between a file and a device

```json
{
    "@id" : "relationship-136",
    "@type" : "Relationship",
    "source" : "file-136",
    "target" : "data-source-1",
    "kindOfRelationship" : "contained-within",
    "isDirectional" : true,
    "propertyBundle" : [ {
        "@type" : "PathRelation",
        "path" : "/Sito/Carbonara.docx"
    } ]
}
```
NETWORK MINER Hosts

![Image of Network Miner tool displaying host details]

- IP: 174.143.213.184 [packetlife.net]
- IP: 192.168.1.140 (Linux)
  - MAC: 001D60B30184
  - NIC Vendor: ASUSTeK COMPUTER INC.
  - MAC Age: 18/08/2007
  - Hostname:
  - OS: Linux
    - TTL: 64 (distance: 0)
    - Open TCP Ports:
      - Sent: 21 packets (1.234 Bytes), 0.00% cleartext (0 of 0 Bytes)
      - Received: 19 packets (23.041 Bytes), 0.00% cleartext (0 of 0 Bytes)
    - Incoming sessions: 0
    - Outgoing sessions: 1
      - Host Details
        - Web Browser User-Agent: Wget/1.12 (linux-gnu)
        - Device Category: Linux

DIGITAL CROSS-BORDER COOPERATION IN CRIMINAL JUSTICE

Bruxelles, 22\textsuperscript{nd} Jan 2020
NETWORK MINER
Representing a host (IP)

{  
"@type": "Trace",
"@id": "https://www.netresec.com/3ea96fca-c70e-4269-9ca0-c24c1f5be026",
"createdBy": "https://www.netresec.com/8c00bb13-40b4-5a1e-aeb3-a65366a4c616",
"propertyBundle": [  
{  
"@type": "IPv4Address",
"value": "192.168.1.140"
  
},
],
}
NETWORK MINER

Representing a host (IP and Domain)

```json
{
    "@type": "Trace",
    "@id": "https://www.netresec.com/4558f129-df48-4bcf-b34f-c3b74549c251",
    "createdBy": "https://www.netresec.com/8c00bb13-40b4-5a1e-aeb3-a65366a4c616",
    "propertyBundle": [
        {
            "@type": "IPv4Address",
            "value": "174.143.213.184"
        },
        {
            "@type": "DomainName",
            "value": "packetlife.net"
        }
    ]
}
```
NETWORK MINER
Network Connection (Session)
NETWORK MINER

Representing a “Network Connection”

```
{
  "@type": "Trace",
  "@id": "https://www.netresec.com/cb19467c-0d18-42bc-92b8-d38a6b0127b3",
  "createdBy": "https://www.netresec.com/8c00bb13-40b4-5a1e-aeb3-a65366a4c616",
  "propertyBundle": [
    {
      "@type": "NetworkConnection",
      "destinationPort": 80,
      "dst": "https://www.netresec.com/4558f129-df48-4bfc-b34f-c3b74549c251",
      "endTime": "2011-03-01T20:45:13.5136310Z",
      "protocols": "TCP, HTTP",
      "sourcePort": 57678,
      "src": "https://www.netresec.com/3ea95fca-c70e-4269-9ca0-c24c1f5be026",
      "startTime": "2011-03-01T20:45:13.2668210Z"
    }
  ]
},
```
NETWORK MINER
Representing a “Network Connection”

```
{
    "@type": "Trace",
    "@id": "https://www.netresec.com/cb19467c-0d18-42bc-92b8-d38a6b0127b3",
    "createdBy": "https://www.netresec.com/8c00bb13-40b4-5a1e-aeb3-a65366a4c616",
    "propertyBundle": [
        {
            "@type": "NetworkConnection",
            "destinationPort": 80,
            "dst": "https://www.netresec.com/4558f129-df48-4bcf-b34f-c3b74549c251",
            "endTime": "2011-03-01T20:45:13.5136310Z",
            "protocols": "TCP, HTTP",
            "sourcePort": 57678,
            "src": "https://www.netresec.com/3ea95fca-c70e-4269-9ca0-c24c1f5be026",
            "startTime": "2011-03-01T20:45:13.2668210Z"
        }
    ]
}
```
NETWORK MINER

File

<table>
<thead>
<tr>
<th>Frame nr.</th>
<th>Filename</th>
<th>Extension</th>
<th>Size</th>
<th>Source host</th>
<th>S. port</th>
<th>Destination host</th>
<th>D. port</th>
<th>Protocol</th>
<th>Timestamp</th>
</tr>
</thead>
</table>

DIGITAL CROSS-BORDER COOPERATION IN CRIMINAL JUSTICE

Bruxelles, 22\textsuperscript{nd} Jan 2020
NETWORK MINER

Representing a “File”

{ "@type": "Trace",
 "@id": "https://www.netresec.com/bfe2e4da-97b4-4677-9439-d37592ca33fd",
 "createdBy": "https://www.netresec.com/8c00bb13-40b4-5a1e-aeb3-a65366a4c616",
 "propertyBundle": [
 {
 "@type": "File",
 "accessedTime": "2011-03-01T20:45:3138890Z",
 "extension": "png",
 "fileName": "logo.png",
 "isDirectory": false,
 "sizeInBytes": 21684
 },
 {
 "@type": "ContentData",
 "dataPayloadReferenceURL": "D:\case-export\AssembledFiles\174.143.213.184\TCP-80\images\layout\logo.png",
 "hash": {
 "@type": "Hash",
 "hashMethod": "MD5",
 "hashValue": "966007c476e0c200fba8b28b250a6379"
 }
 },
 "sizeInBytes": 21684
 }
}
Case Converter

- PoC intermediate software layer developed to convert the output of a forensic tool in UCO/CASE standard

- As an example we used the XML report generated by the Cellebrite UFED and by the Logicube Falcon hardware duplicator
Representing a “Call Log”

```
{
  "@id": "phone_call1",
  "@type": "Trace",
  "propertyBundle": [
    {
      "@type": "PhoneCall",
      "callType": "mobile",
      "startTime": "2010-01-15T17:59:43.25Z",
      "endTime": "2010-01-15T18:30:41.25Z",
      "from": "phone_account1",
      "to": "phone_account2",
      "duration": "1858"
    }
  ]
}
```
Representing a “Message”

```json
{
    "@id": "sms_message1",
    "@type": "Trace",
    "propertyBundle": [
        {
            "@type": "Message",
            "application": "sms_application1",
            "messageText": "Yo dude! This is my new number."
        },
        {
            "@type": "Message",
            "application": "sms_application1",
            "messageText": "Yo dude! This is my new number."
        },
        {
            "@type": "Message",
            "application": "sms_application1",
            "messageText": "Yo dude! This is my new number."
        }
    ],
    "sentTime": "2010-01-15T17:59:43.25Z"
}
```
CASE Roadmap and Future

- Support the development of UCO / CASE language in forensic tools
- Develop tools to map/convert the output produced by DF software to UCO / CASE
- Work with software developers and cloud providers to facilitate the native adoption of UCO / CASE language
Conversion and parsing tools

**OXYGEN FORENSICS**

Oxygen Forensic® Analyst and Oxygen Forensic® Detective
GENERAL REQUIREMENTS FOR XML EXPORT

**UFED Physical Analyzer**

Extraction report fields
August 2019 | Version 7.23

**ARTIFACT REFERENCE**

3.5
Obtaining Cloud Provider data

https://www.facebook.com/records/login/

Law Enforcement Online Requests

Request Secure Access to the Law Enforcement Online Request System

We disclose account records solely in accordance with our terms of service and applicable law.

If you are a law enforcement agent or emergency responder who is authorized to gather evidence in connection with an official investigation or in order to investigate an emergency involving the danger of serious physical injury or death, you may request records from Facebook through this system.

☐ I am an authorized law enforcement agent or government employee investigating an emergency, and this is an official request

Request Access

Warning: Requests to Facebook through this system may be made only by governmental entities authorized to obtain evidence in connection with official legal proceedings pursuant to Title 18, United States Code, Sections 2703 and 2711. Unauthorized requests will be subject to prosecution. By requesting access you are acknowledging that you are a government official making a request in official capacity. For further information please review the Law Enforcement Guidelines.
Obtaining Cloud Provider data
https://legalrequests.twitter.com/
Analyzing Cloud Provider data

Folder: facebook-mattiaep

- about_you
- ads
- apps_and_websites
- comments
  - comments.html
  - no-data.txt
- events
- following_and_followers
- friends
- groups
- index.html
- likes_and_reactions
- location
- marketplace
- messages
- other_activity
- pages
- payment_history
- photos_and_videos
- posts
- profile_information
- saved_items_and_collections
- search_history
  - no-data.txt
  - your_search_history.html
- security_and_login_information
- stories
- your_places

File list:
- no-data.txt: 30 byte, Solo testo
- comments.html: 1,6 MB, HTML...ocument
- index.html: 54 KB, HTML...ocument
- your_search_history.html: 28 KB, HTML...ocument

Folder sizes:
- Cartella
Analyzing Cloud Provider data
Analyzing Cloud Provider data

<table>
<thead>
<tr>
<th>File Name</th>
<th>Modification Date</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>account-creation-ip.js</td>
<td>oggi 09:38</td>
<td>149 byte</td>
</tr>
<tr>
<td>account-suspension.js</td>
<td>oggi 09:38</td>
<td>40 byte</td>
</tr>
<tr>
<td>account-timezone.js</td>
<td>oggi 09:38</td>
<td>127 byte</td>
</tr>
<tr>
<td>account.js</td>
<td>oggi 09:38</td>
<td>324 byte</td>
</tr>
<tr>
<td>ad-engagements.js</td>
<td>oggi 09:38</td>
<td>827 KB</td>
</tr>
<tr>
<td>ad-impressions.js</td>
<td>oggi 09:38</td>
<td>1.5 MB</td>
</tr>
<tr>
<td>ad-mobile-conversions-attributed.js</td>
<td>oggi 09:38</td>
<td>54 byte</td>
</tr>
<tr>
<td>ad-mobile-conversions-unattributed.js</td>
<td>oggi 09:38</td>
<td>12 KB</td>
</tr>
<tr>
<td>ad-online-conversions-attributed.js</td>
<td>oggi 09:38</td>
<td>4 KB</td>
</tr>
<tr>
<td>ad-online-conversions-unattributed.js</td>
<td>oggi 09:38</td>
<td>4 KB</td>
</tr>
<tr>
<td>ageinfo.js</td>
<td>oggi 09:38</td>
<td>135 byte</td>
</tr>
<tr>
<td>block.js</td>
<td>oggi 09:38</td>
<td>151 byte</td>
</tr>
<tr>
<td>connected-application.js</td>
<td>oggi 09:38</td>
<td>3 KB</td>
</tr>
<tr>
<td>contact.js</td>
<td>oggi 09:38</td>
<td>29 byte</td>
</tr>
<tr>
<td>device-token.js</td>
<td>oggi 09:38</td>
<td>566 byte</td>
</tr>
<tr>
<td>direct_message_group_media</td>
<td>oggi 09:38</td>
<td>--</td>
</tr>
<tr>
<td>direct_message_media</td>
<td>oggi 09:38</td>
<td>--</td>
</tr>
<tr>
<td>direct-message-group-headers.js</td>
<td>oggi 09:38</td>
<td>24 KB</td>
</tr>
<tr>
<td>direct-message-group.js</td>
<td>oggi 09:38</td>
<td>40 KB</td>
</tr>
<tr>
<td>direct-message-group-headers.js</td>
<td>oggi 09:38</td>
<td>57 KB</td>
</tr>
</tbody>
</table>
Analyzing Cloud Provider data...
Conversion and parsing
Cloud Provider data
Thanks for your attention!

Questions?

Mattia Epifani, CNR-IGSG
mattia.epifani@igsg.cnr.it