DFAX: Digital Forensic Analysis eXpression

Leveraging CybOX™ to Standardize Representation and Exchange of Digital Forensic Information

Eoghan Casey, Greg Back, Sean Barnum

MITRE

Outline

- Motivation
- Related work
- DFAX ontology
- Introduce a Unified Cyber Ontology (UCO)
- Using CybOX to represent digital evidence
- Provenance
- Actions, Action Patterns, Action Lifecycle
- Next steps

Motivation

- **Share digital forensic information**
  - **Investigations involving 2+ jurisdictions/agencies**
- **Share digital forensic knowledge**
  - **Distinctive behavioral patterns to search for**
- **Combine results from multiple forensic tools**
- **Compare results from multiple forensic tools**
  - **Automate tool validation & verification**
- **Structured data enables more advanced analysis**
  - **high timelines, graph queries, behavioral analysis**

- **What is a Cyber Observable?**
  - **a *measurable event* or *stateful property* in the cyber domain**
  - **measurable events: registry key is created, file is deleted**
  - **stateful properties: MD5 hash of a file, value of a registry key**
- **How these observables relate (patterns)**
- **Actions (context and tool provenance)**
- **Already used in digital forensics (intrusions, malware, IoC)**
  - **Autopsy, Volatility**

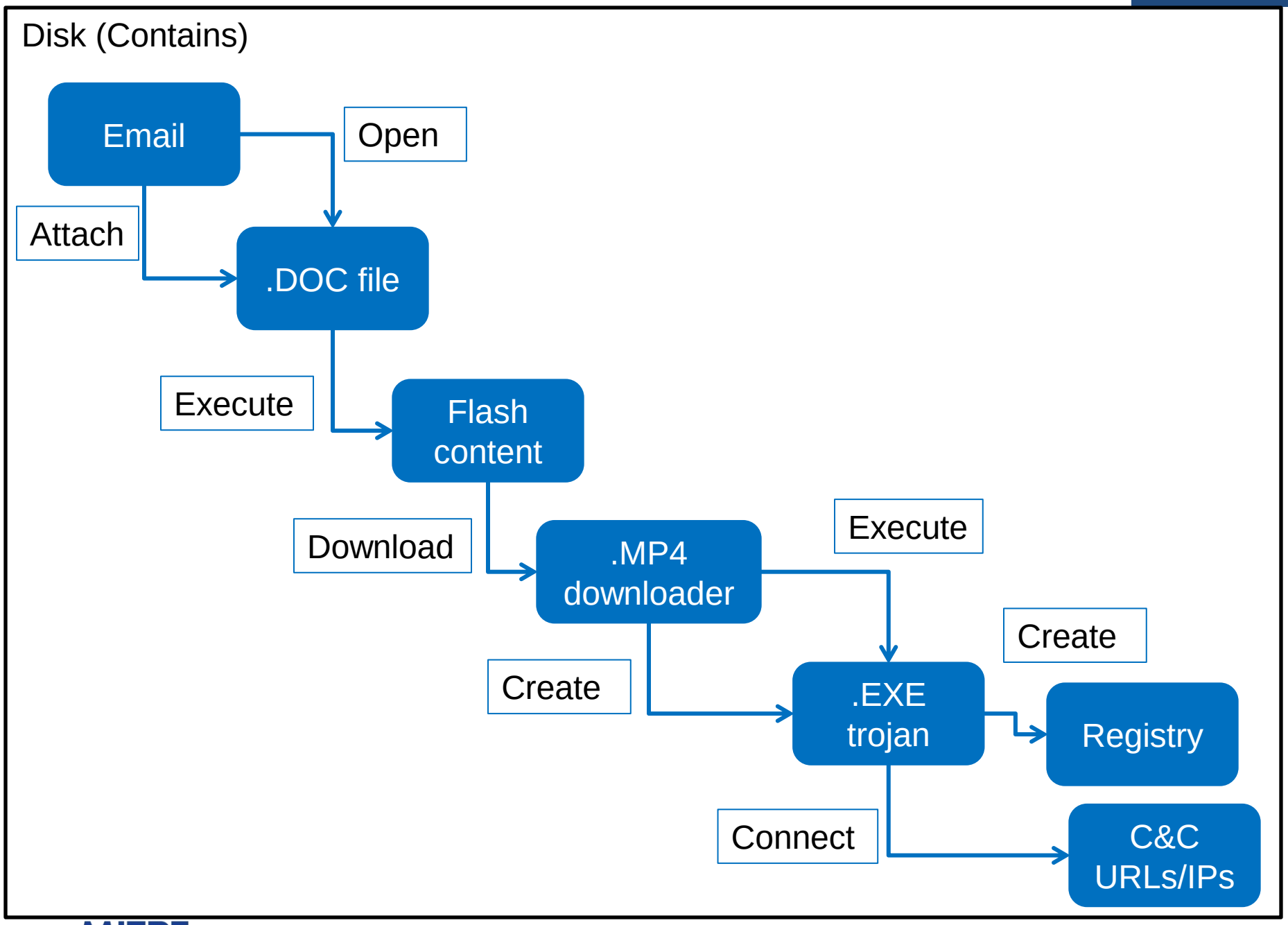
Various Defined Object Schemas

- Account
- Address
- API
- Code
- Device
- Disk
- Disk Partition
- DNS Cache
- DNS_Record
- Email Message
- File
- GUI
- GUI Dialog Box
- GUI Window
- Library
- Linux Package
- Memory
- Mutex
- Network Flow
- Network Packet
- Network Route Entry
- Network Route
- Network Subnet
- Pipe
- Port
- Process
- Product
- Semaphore
- Socket
- System
- Unix File
- Unix Network Route Entry
- Unix Pipe
- Unix Process
- Unix User Account
- Unix Volume
- URI
- User Account
- User Session
- Volume
- Win Computer Account
- Win Critical Section
- Win Driver
- Win Event
- Win Event Log
- Win Executable File
- Win File
- Win Kernel
- Win Kernel Hook
- Win Handle
- Win Mailslot
- Win Mutex
- Win Pipe
- Win Network Route Entry
- Win Network Share
- Win Pipe
- Win Prefetch
- Win Process
- Win Registry Key
- Win Semaphore
- Win Service
- Win System
- Win System Restore
- Win Task
- Win Thread
- Win User Account
- Win Volume
- Win Waitable Timer
- X509 Certificate

…

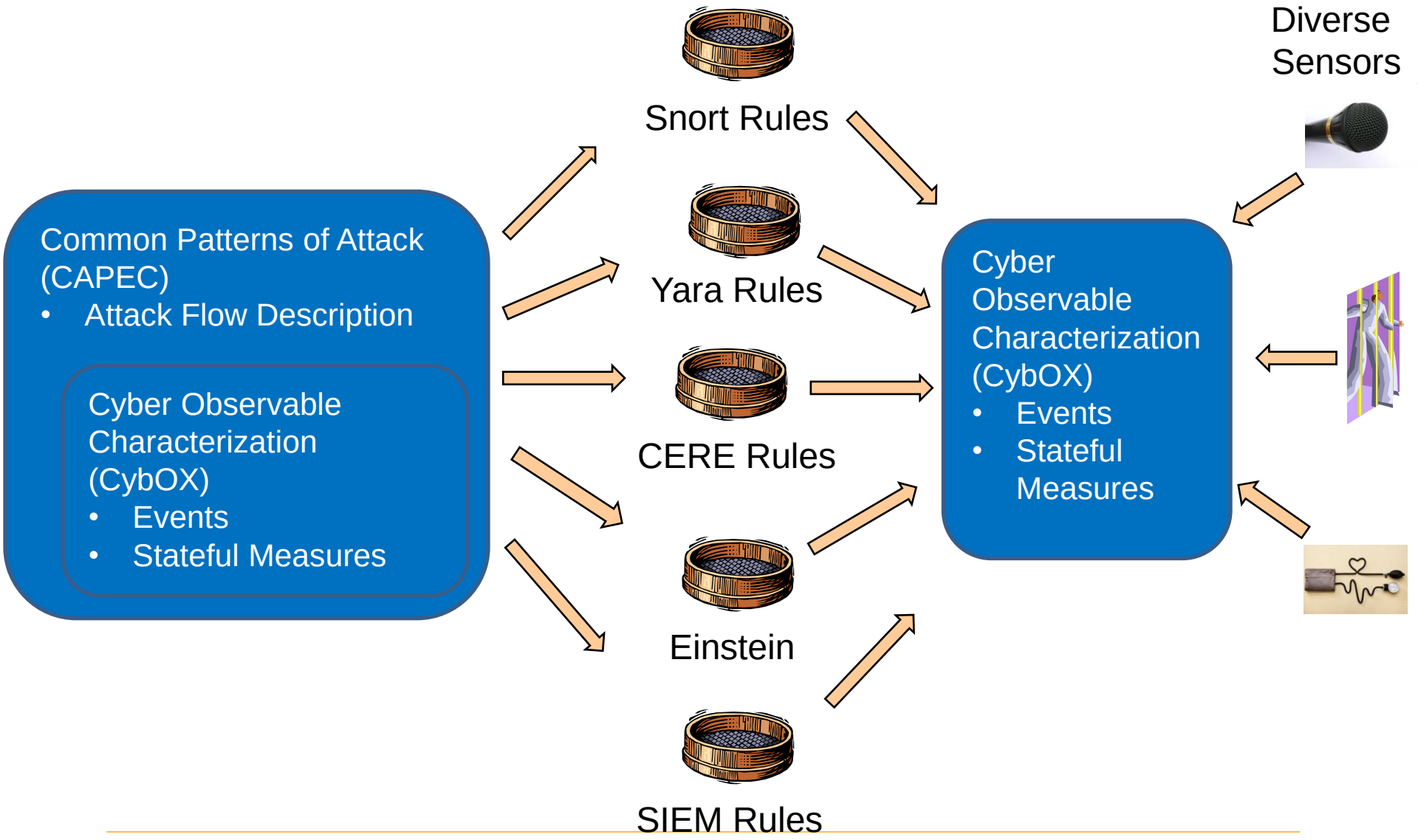
(more on the way)

MITRE

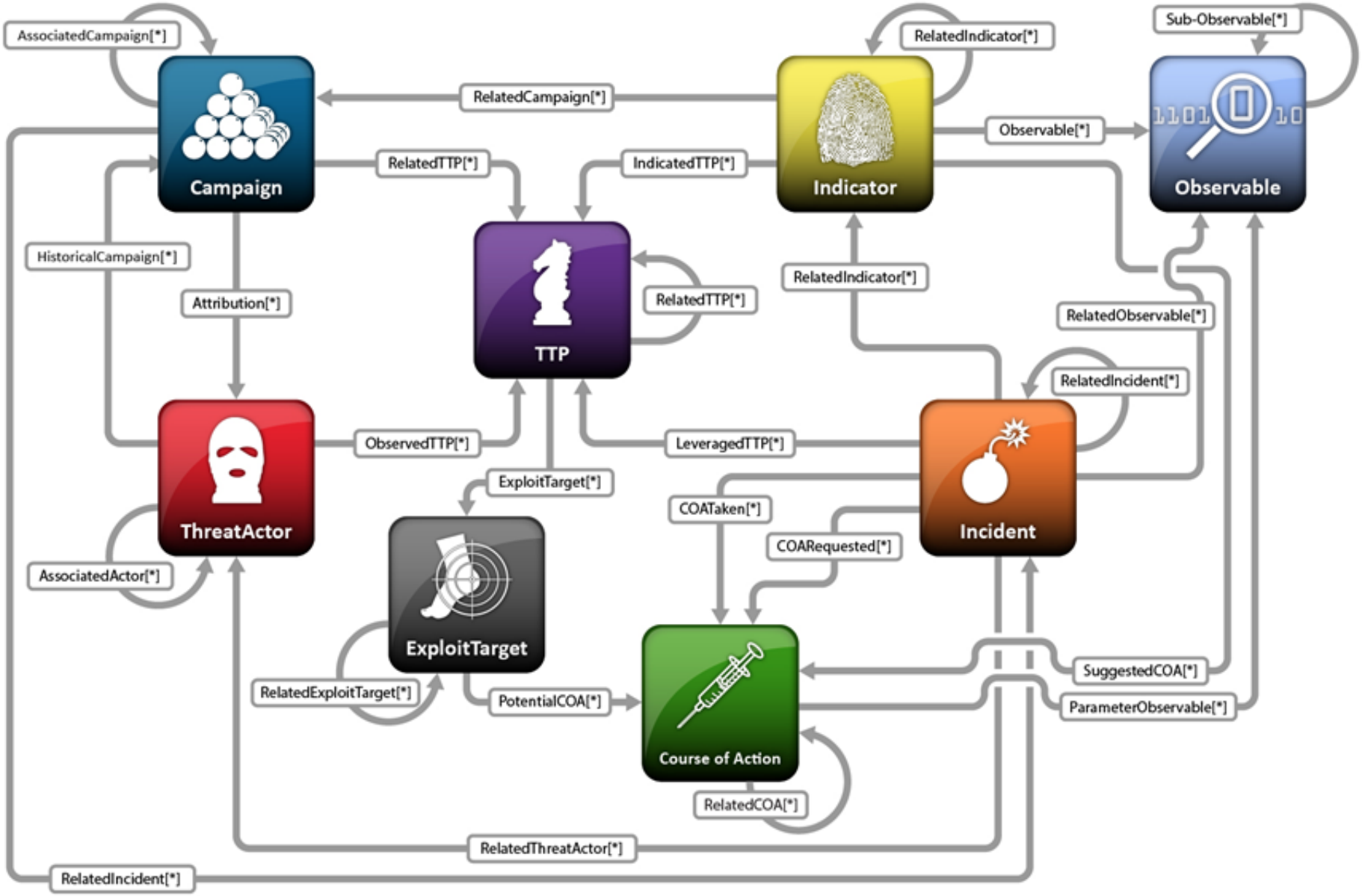


MITRE

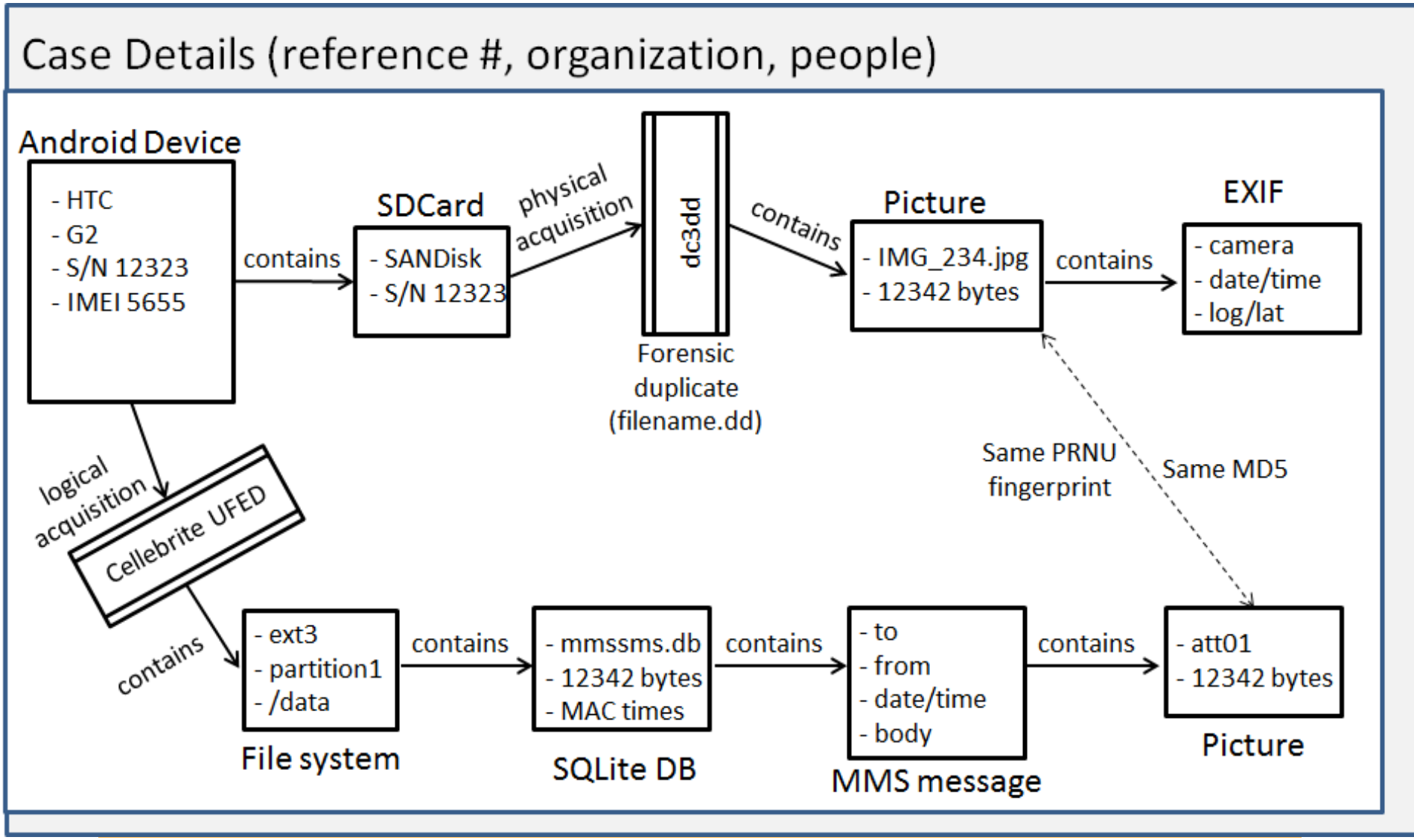
Use Case: Detect Malicious Activity



STIX: Structured Threat Information eXpressions



Android Example

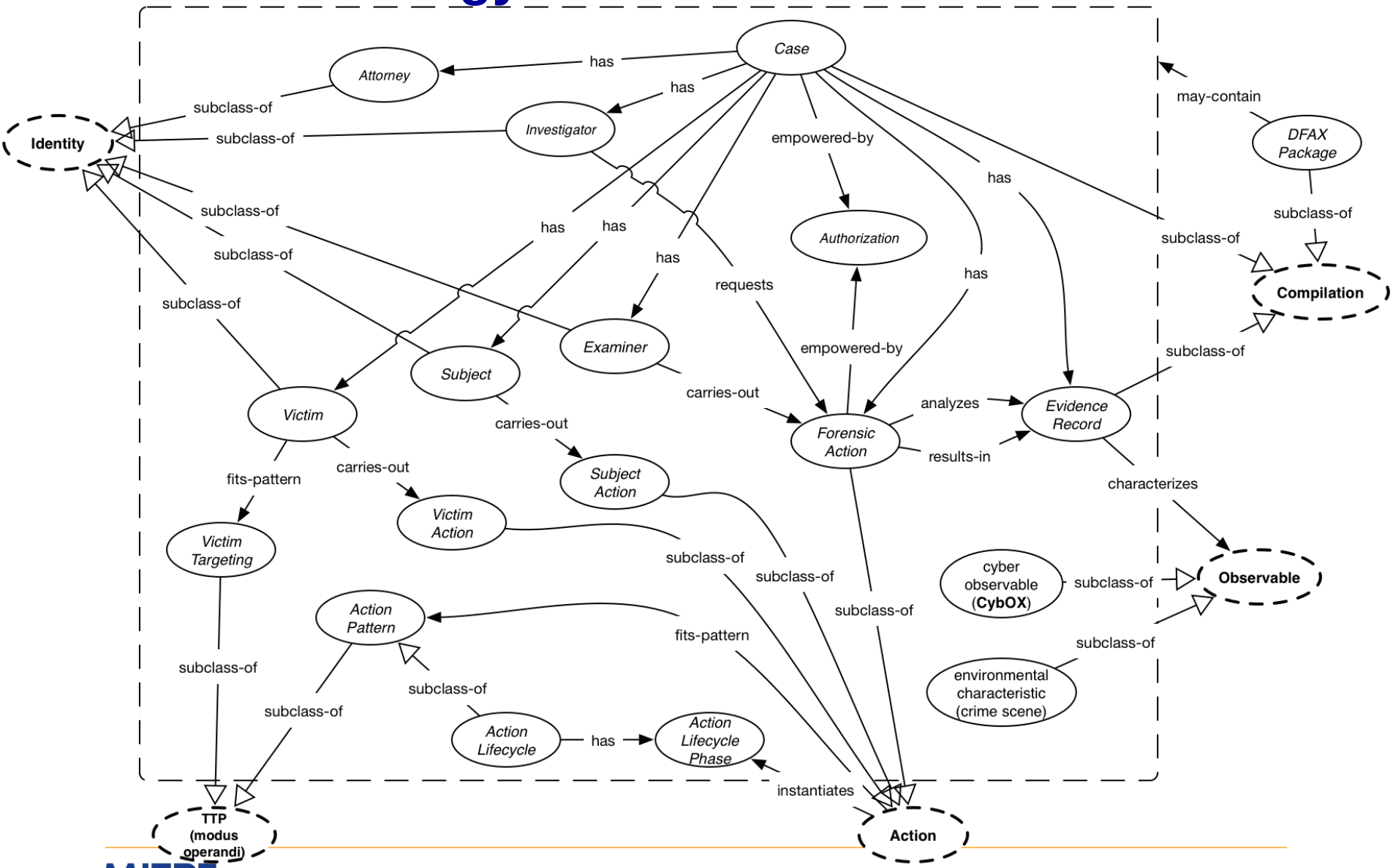


MITRE

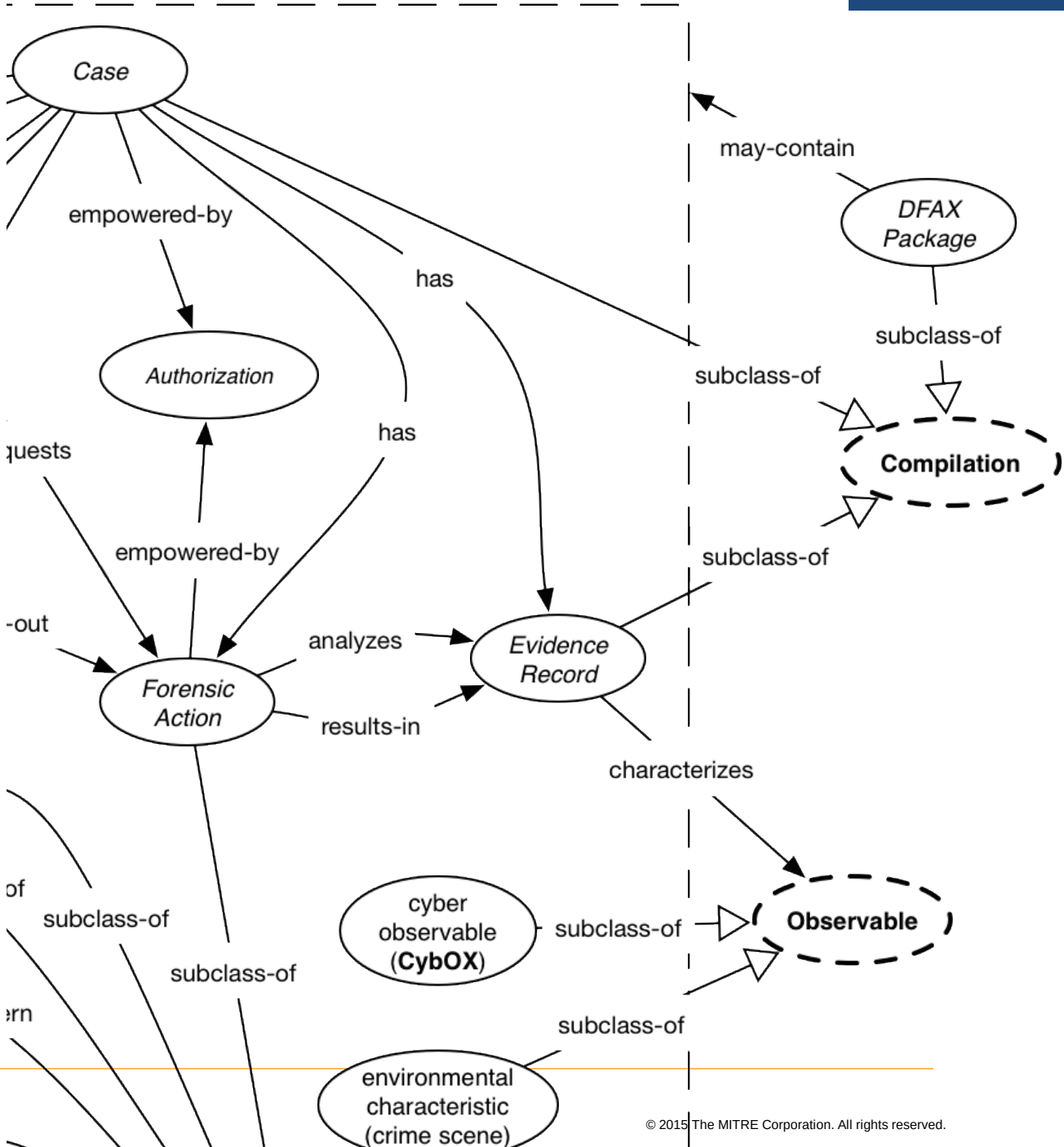
Related Work

	Digital Evidence Bags (DEB)	XIRAF	RDF	Digital Evidence Exchange (DEX)	Digital Forensic XML (DFXML)	AFF4	DFAX
	Turner, 2005	Alink et al, 2006	Schatz, 2007	Levine & Liberatore, 2009	Garfinkel, 2009	Cohen, et al 2009	Open Source (DHS/MITRE)
Open source	Y	N	N/A	Y	Y	Y	Y
Case Information	Y	Y	N	N	N	Y	Y
Integrity assurance	Y	Y	Y	Y	Y	Y	Y
Chain of custody	Y	N	P	N	N	Y	Y
Evidence details	Y	Y	Y	N	N	Y	Y
Tool details	Y	Y	Y	Y	Y	Y	Y
Storage media contents	Y	Y	Y	N	Y	Y	Y
Mobile device contents	Y	Y	N	N	N	N	Y
Assign object multiple types	Y	Y	Y	N	N	Y	Y
Parent-child relationships	Y	Y	Y	Y	Y	N	Y
Non-hierarchical relationships	N	N	Y	N	N	Y	Y
Actions	N	N	Y	N	N	N	Y
Action Lifecycles	N	N	N	N	N	N	Y
Action Patterns	N	N	N	N	N	N	Y

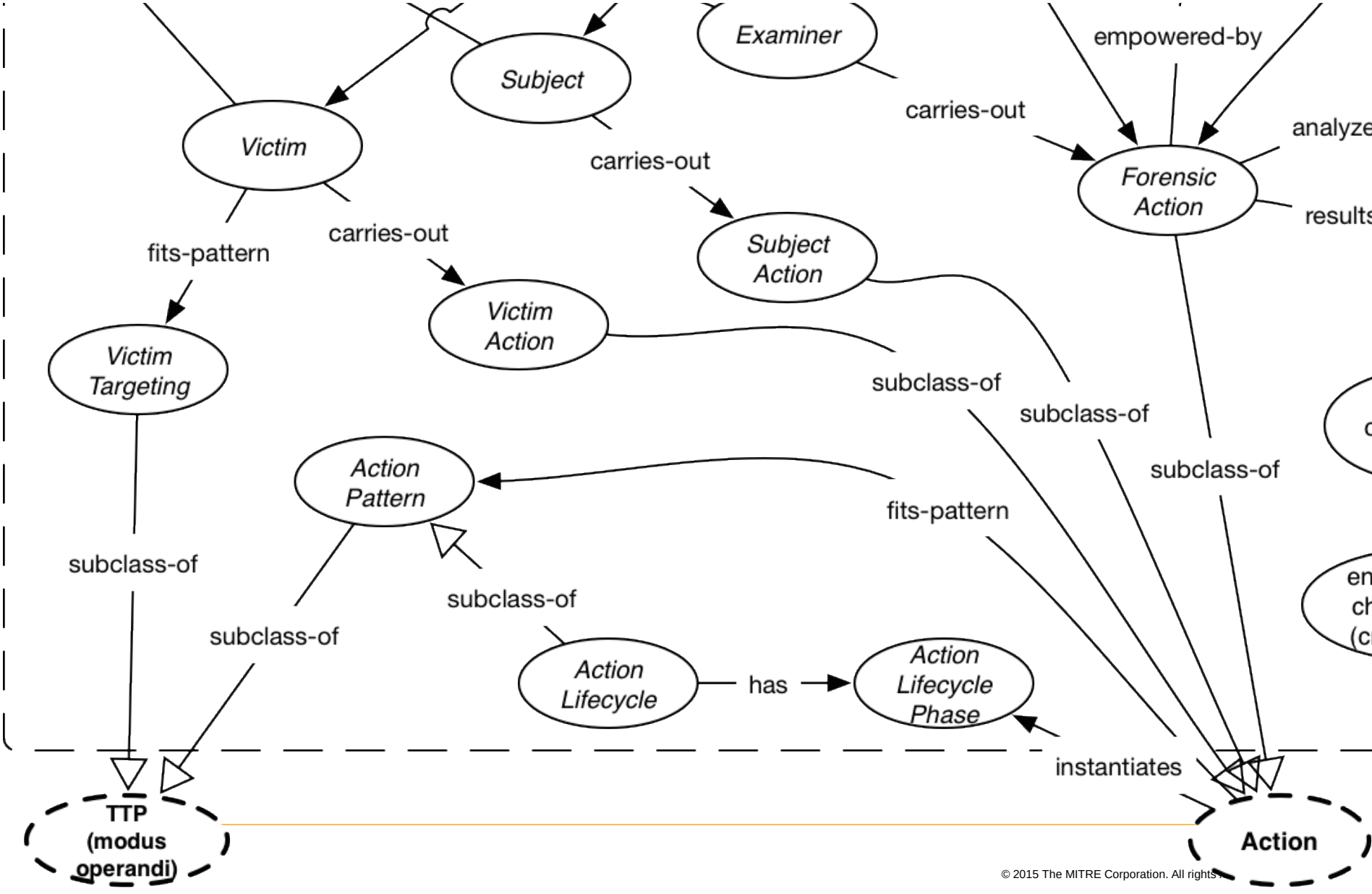
DFAX Ontology



DFAX Ontology



DFAX Ontology



Digital Evidence in CybOX

- **Traces of wiping (Observable or Pattern)**

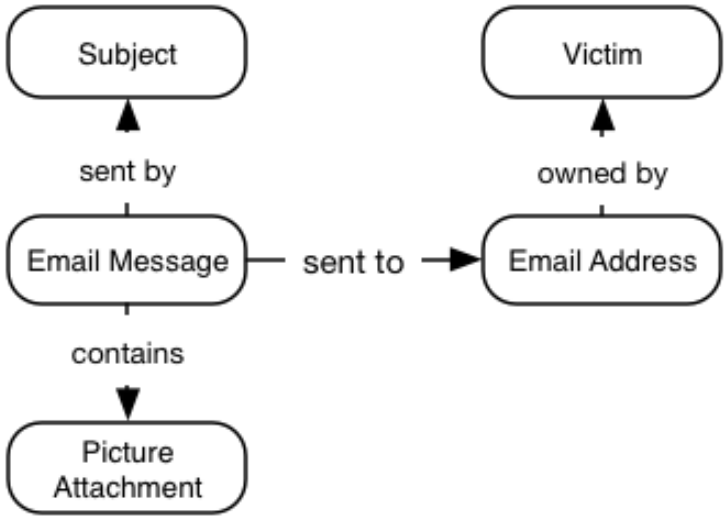
```
<ProductObj:Product>Secure Delete</ProductObj:Product>

<FileObj:File_Name>sdelete.exe</FileObj:File_Name>
<cybox:Relationship>Characterizes</cybox:Relationship>


<WinRegistryKeyObj:Key>Software\Sysinternal\SDelete</WinRegist
<cybox:Relationship>Created</cybox:Relationship>


<FileObj:File_Name
condition="FitsPattern">Z+.Z+</FileObj:File_Name>
<cybox:Relationship">Renamed_By</cybox:Relationship>
```

Provenance

- **Evidence source and handling**
  - **Continuity of possession / Chain of custody**
- **Evidence processing**
  - **Tools and transformations**
- **Evidence analysis**
  - **Evaluation of source**
  - **Need to expand CybOX (e.g., PRNU and ENF)**

Provenance in DFAX/CybOX

- **Evidence source and handling**
  - `dfax:Evidence Record`
  - `dfax:Forensic Action`
- **Evidence processing**
  - `cyboxCommon:Tool`
- **Evidence analysis**
  - **Defined relationships**



Action Lifecycle: Forensic Process

- **Different groups define process differently**

Forensic Process 1	Forensic Process 2	Forensic Process 3	Forensic Process 4
		Authorization	
	Planning	Planning	Preparation
Identification	Identification	Notification	
Preservation	Reconnaissance	Search	Incident Response
Collection	Transport & Storage	Collection	Data Collection
Examination		Transport	
Analysis	Analysis	Storage	Data Analysis
Presentation	Proof and Defense	Examination	Presentation of Findings
	Archive Storage	Presentation	
		Proof/defense	Incident Closure
		Dissemination	

Action Lifecycle: Subject

Grooming (Sexual Assault)	Kill Chain (Intrusion)
Victim selection	Reconnaissance
Establish trust	Development
Desensitization to sexual activity/abuse	Delivery
Maintain secrecy (persuasion/threats)	Exploitation
Arrange meeting	Configuration
Conceal evidence	Beaconing and C2

Actions {Subject, Victim, System}

- **Action = `USB Device Connected`**
- **Represent & search structured characteristics**

```
FileObj:File_Name = setupapi.log
IN
FileObj:File_Path = C:\Windows\setupapi.log
CONTAINS
cyboxCommon:String_Value =
"\DISK&VEN_KINGSTON&PROD_DATATRAVELER_3.0&REV_PMAP\8606E6D418ABE6077179
FAE&0]
OR
WinRegistryKeyObj:Name = HardwareID
IN
WinRegistryKeyObj:Hive = HKEY_LOCAL_MACHINE
WinRegistryKeyObj:Key = "\SYSTEM\CurrentControlSet\Enum\USBSTOR\
Disk&Ven_Kingston&Prod_DataTraveler_3.0&Rev_PMAP\08606E6D418ABE6077179F
AE&0"
CONTAINS
WinRegistryKeyObj:Data = "USBSTOR\DiskKingstonDataTraveler_3.0PMAP"
```

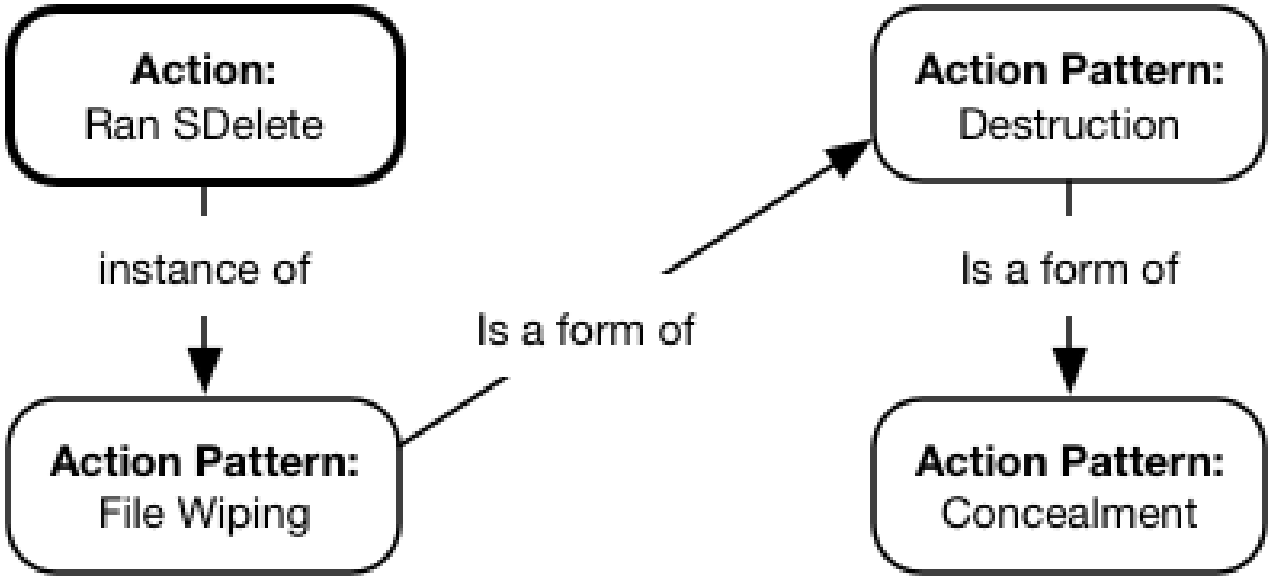
MITRE

Note: Plaso

- Categorizes related “events” using “tags”
  - Plaso events map to cybOX:Observables
  - Plaso tags map to dfax:Actions
- Plaso “Application Execution” tag includes:
  - windows:prefetch:execution
  - windows:lnk AND path contains ‘.exe’
  - winreg AND userassist or mru
  - winevt source = Security AND eventID = 592

Action Patterns

- **Higher level, human understandable terms**
  - **Reflect behaviors and objectives**
  - **Assist in establishing modus operandi (a.k.a. TTP)**



Representing Changes

NIST Diskprint (before and after comparison)

http://www.nsrl.nist.gov/dskprt/DPexample.html

- **CybOX Actions**
  - **Install program**
  - **Execute program**
  - **Use program**
  - **Uninstall program**

Next steps

- Community involvement
  - https://github.com/dfax/dfax
- DFAX/CybOX Python library
- Periodic Mobile Forensics
- Plaso
- Abstract concepts common across cyber domains
  - Tools
  - Actions & Action Lifecycle