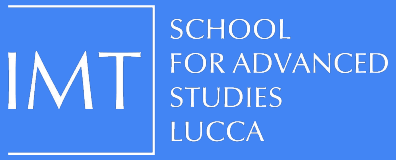
Behind the Screens: An MSC-Model of Digital Forensics in Crime Investigation

Mario Raciti

21st Workshop on Security Frameworks
"Intelligence rests on Knowledge"



19/12/23 – Catania

Agenda

1. Introduction
2. A Cybersecurity Perspective
3. The DF-ADF Dichotomy
4. The MSC-Model Approach
5. The DFCI Protocols
6. Conclusions

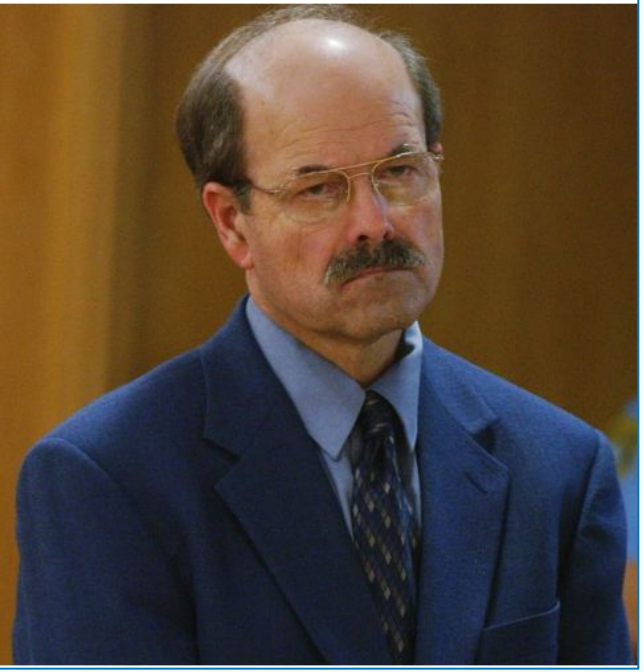
Agenda

1. **Introduction**
2. A Cybersecurity Perspective
3. The DF-ADF Dichotomy
4. The MSC-Model Approach
5. The DFCI Protocols
6. Conclusions

Dennis Rader

Known as the "BTK" Killer—which stands for bind, torture, and kill—Dennis Rader murdered 10 people in the Wichita, Kansas area from 1974 to 1991, often leaving clues to taunt authorities.

By Biography.Com Editors And Tyler Piccotti UPDATED: OCT 17, 2023



Silk Road review: The true story of the dark web's illegal drug market

The wild scheme of Ross Ulbricht, a young physics grad who set up a massive online illegal drugs market, keeps us hooked to the bitter end in *Silk Road*, a fictionalised version of his story

By Linda Marric

17 March 2021

Nick Robinson as Ross Ulbricht, founder of the dark web marketplace Silk Road
Vertigo Releasing

Colonial Pipeline ransomware attack: Everything you need to know

Updated: DarkSide has claimed responsibility for the catastrophic ransomware outbreak.

Written by **Charlie Osborne,** Contributing Writer

May 13, 2021 at 12:17 a.m. PT

"The use of *scientifically derived and proven methods* toward the **identification, collection, validation, examination, analysis, and presentation** of digital evidence while preserving the integrity of the information, including process repeatability, and maintaining a strict chain of custody for the data".

- Definition of Digital Forensics

The Role of Digital Evidence

A **digital evidence** is any probative information stored or transmitted in digital form.

Forensic evidence is *acceptable* only if it is obtained legally.

If the policies and procedures set by law are **violated** during the *Forensics Process*, the value of the evidence becomes null and void.

CySec and Privacy Concerns in DF

During crime investigation, various forms of **data processing** are conducted to gather evidence, analyse information, and support legal proceedings.

These acts have the potential to pose **threats** to the *suspect's rights*.

Guilty or not, privacy will always be there for you :)

“Attempts to **negatively** affect the existence, amount and/or quality of evidence from a crime scene, or make the analysis and examination of evidence difficult or impossible to conduct”.

- Definition of Anti-Digital Forensics

Classification of Anti-Forensics

Anti-Digital Forensics can be classified into **four categories**:

> Data hiding

> Artefact wiping

> Trail obfuscation

> Attacks against the forensic process and tool

So, who’s the actual villain?

Agenda

1. Introduction
2. **A Cybersecurity Perspective**
3. The DF-ADF Dichotomy
4. The MSC-Model Approach
5. The DFCI Protocols
6. Conclusions

Perspectives of (DF)CI

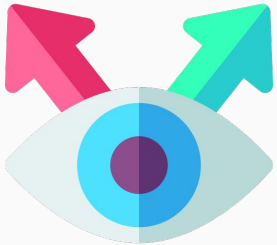
Typical perspective

Investigators are *always* **good**.

Suspects *may be* **guilty or not**.

Cybersecurity perspective

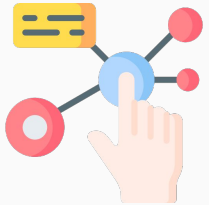
Anybody *may be* **bad**.



CySec Rules of Thumb

Rule 1

Any **interaction** *may involve* **malicious activity** within a protocol.



Rule 2

Assign **different roles** to the **same actor** to examine *all possibilities*.

That makes things intriguing…

Agenda

1. Introduction
2. A Cybersecurity Perspective
3. **The DF-ADF Dichotomy**
4. The MSC-Model Approach
5. The DFCI Protocols
6. Conclusions

The DF Scenario

The ADF Scenario

RQ: Can we formalise the DF and ADF scenarios?

Agenda

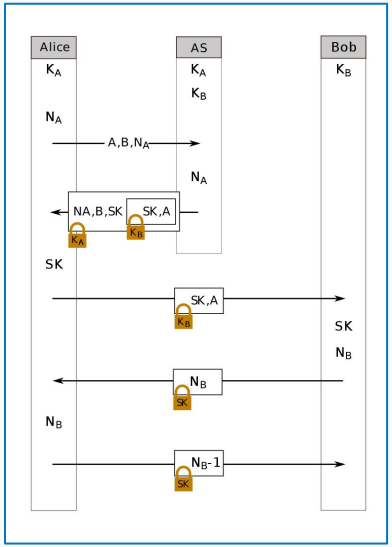
1. Introduction
2. A Cybersecurity Perspective
3. The DF-ADF Dichotomy
4. **The MSC-Model Approach**
5. The DFCI Protocols
6. Conclusions

MSCs – Old but Gold

Message Sequence Charts make up an attractive **visual formalism**.

They describe *patterns of interactions*.

Widely used to capture **system requirements** in the form of *"good" scenarios*.



Symmetric NS Protocol – *Source: Wikipedia*

Security protocols are often modelled through MSCs for their formal analysis.

The Approach in a Nutshell

1. Identify the key **actors**
2. Identify the **messages**
3. Model the **interactions**
4. Elicit the **functional requirements**
5. Set a **threat model**
6. Elicit the **non-functional requirements**
7. Identify potential **attacks**
8. Define appropriate **measures**

Alice → Bob: {"Hi!"}

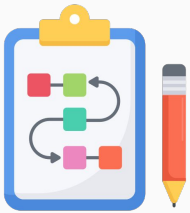
PO: Bob receives Alice's message.

Alice → Bob: {"Hi!"}

Confidentiality – DY – Charlie tries to intercept the message – Encryption.

An MSC-based Kill Chain

1. Identify the key **actors**
2. Identify the **messages**
3. Model the **interactions**
4. Elicit the **functional requirements**
5. Set a **threat model**
6. Elicit the **non-functional requirements**
7. Identify potential **attacks**
8. Define appropriate **measures**



Focusing on the *attacker's actions* in the MSC,

we can infer a Kill Chain!

Agenda

1. Introduction
2. A Cybersecurity Perspective
3. The DF-ADF Dichotomy
4. The MSC-Model Approach
5. **The DFCI Protocols**
6. Conclusions

Introducing the Key Actors

A typical *crime investigation* involving **digital elements** features the following **actors**:

DF Expert

Police

Prosecutor

Judge

Def Lawyer

Suspect/Defendant

The Key Actors in the Italian System

Italian *Code of Criminal Procedure* contains the rules governing **criminal procedure** in every court in Italy.

CT Informatico

Polizia Giudiziaria

Pubblico Ministero

GIP/Giudice del Dibatt.

Avv. Difesa

Indagato/Imputato

The Threat Model

Assumptions

We trust **Police**, **Prosecutor**, **Def Lawyer**, and **Judge** for simplicity (no *General Attacker*).

DF Scenario

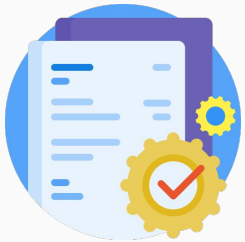
DF Expert a *TA*
Properties: *privacy, integrity, availability*

ADF Scenario

Suspect/Defendant as TA
Properties: (*privacy*), *integrity, availability*

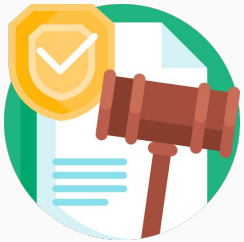
The Three Phases of DFCI

Protocol 1: Init



Protocol 2: Investigation

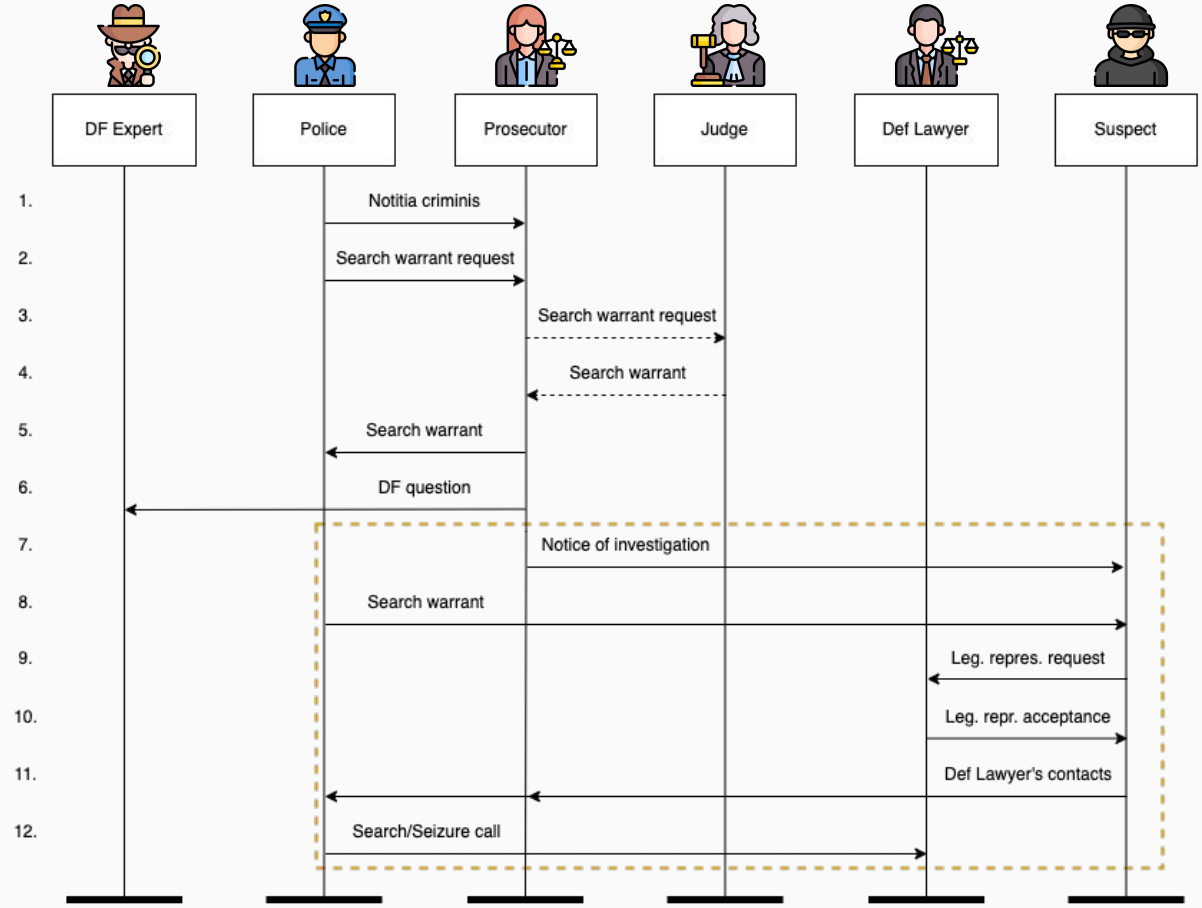
Protocol 3: Trial



Agenda

1. Introduction
2. A Cybersecurity Perspective
3. The DF-ADF Dichotomy
4. The MSC-Model Approach
5. **The DFCI Protocols → Init**
6. Conclusions

Protocol 1: Init

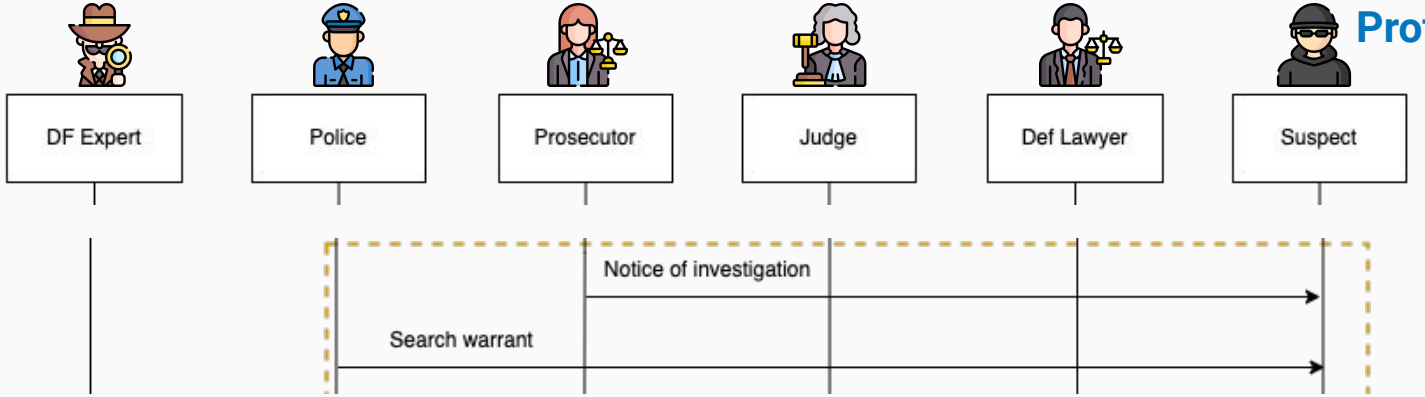


Legend	
Optional	----→
Crime Scene	

Protocol Functional Objectives
PO1: Police obtain search warrant and authorisation to proceed.

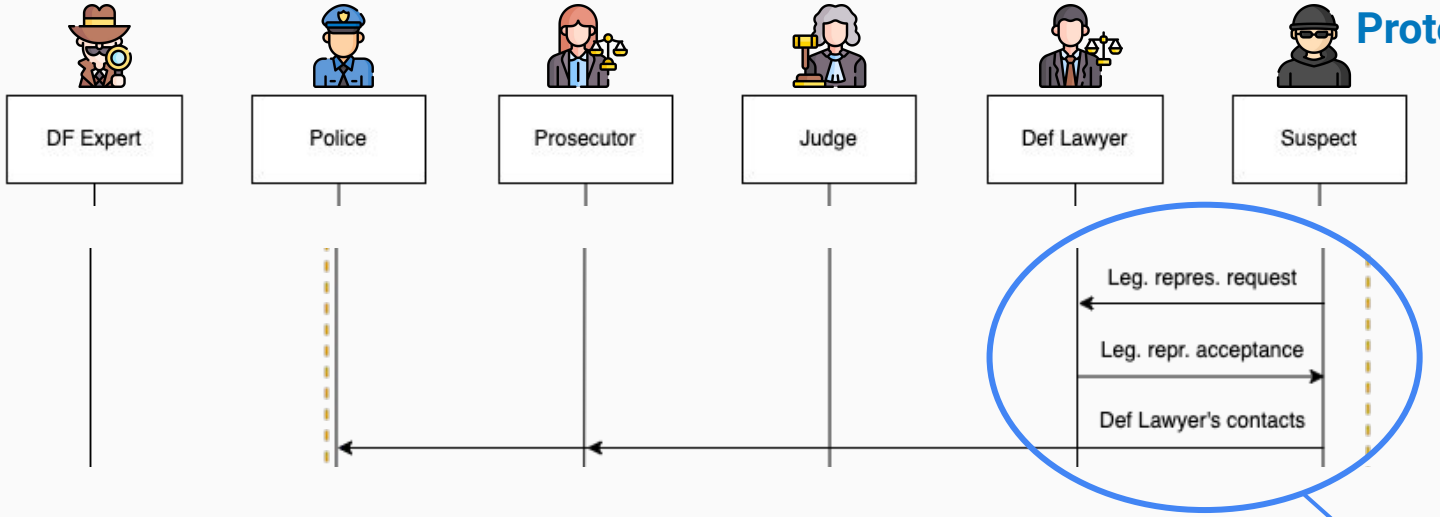
Go to **Protocol 2: Investigation**

Protocol 1: Init



ADF Scenario			
#	Property	Attack Attempt	Measure
7	Authentication	Suspect falsely denies Prosecutor's identity.	Auth verification
7	Integrity	Suspect argues on consistency of notice of investigation.	Digital signature
8	Authentication	Suspect falsely denies Police identity.	Auth verification
8	Integrity	Suspect argues on consistency of search warrant. Suspect questions consistency with notice of investigation.	Digital signature Cross verification

Protocol 1: Init



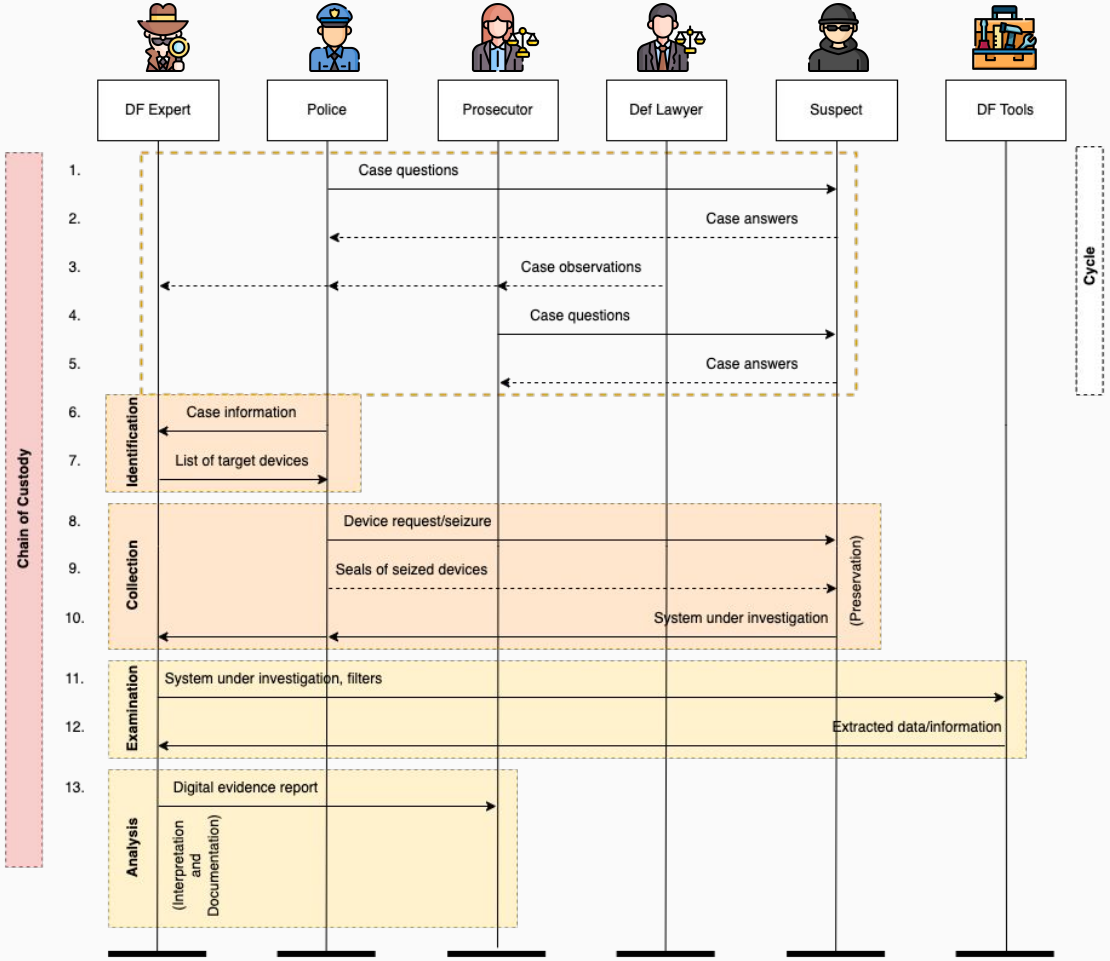
ADF Scenario			
#	Property	Attack Attempt	Measure
7	Authentication	Suspect falsely denies Prosecutor's identity.	Auth verification
7	Integrity	Suspect argues on consistency of notice of investigation.	Digital signature
8	Authentication	Suspect falsely denies Police identity.	Auth verification
8	Integrity	Suspect argues on consistency of search warrant. Suspect questions consistency with notice of investigation.	Digital signature Cross verification

Suspect could *cheat* on **Def Lawyer's availability..** *(additional threat?)*

Agenda

1. Introduction
2. A Cybersecurity Perspective
3. The DF-ADF Dichotomy
4. The MSC-Model Approach
5. **The DFCI Protocols → Investigation**
6. Conclusions

Protocol 2: Investigation

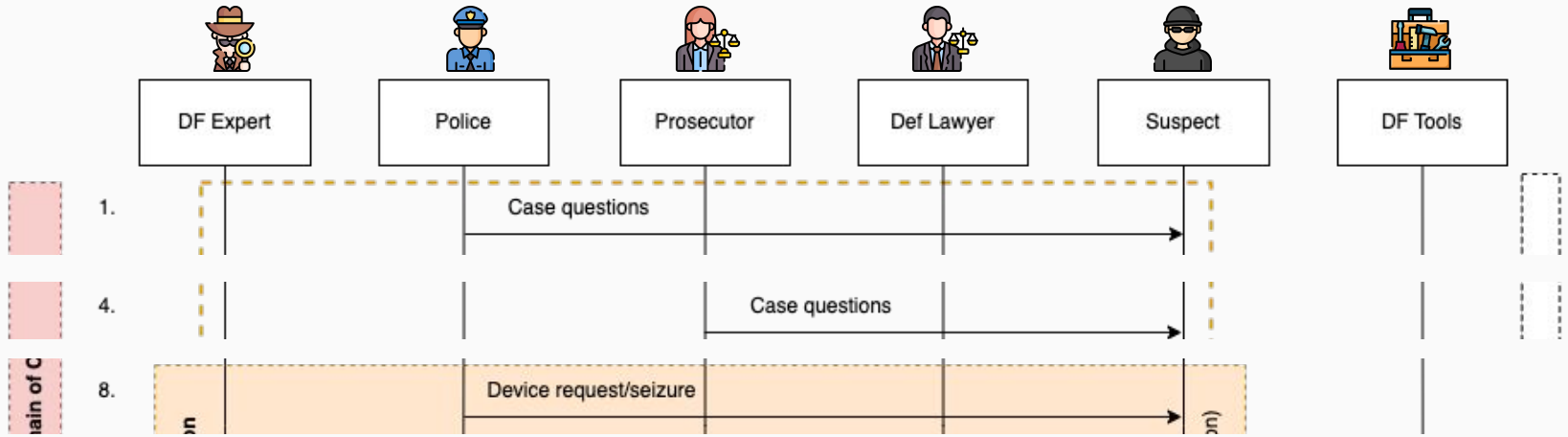


Legend	
Optional	⇢
Crime Scene	
DF Lab	

Protocol Functional Objectives
PO1: Police and Prosecutor obtain set of information to prove or confute charges.

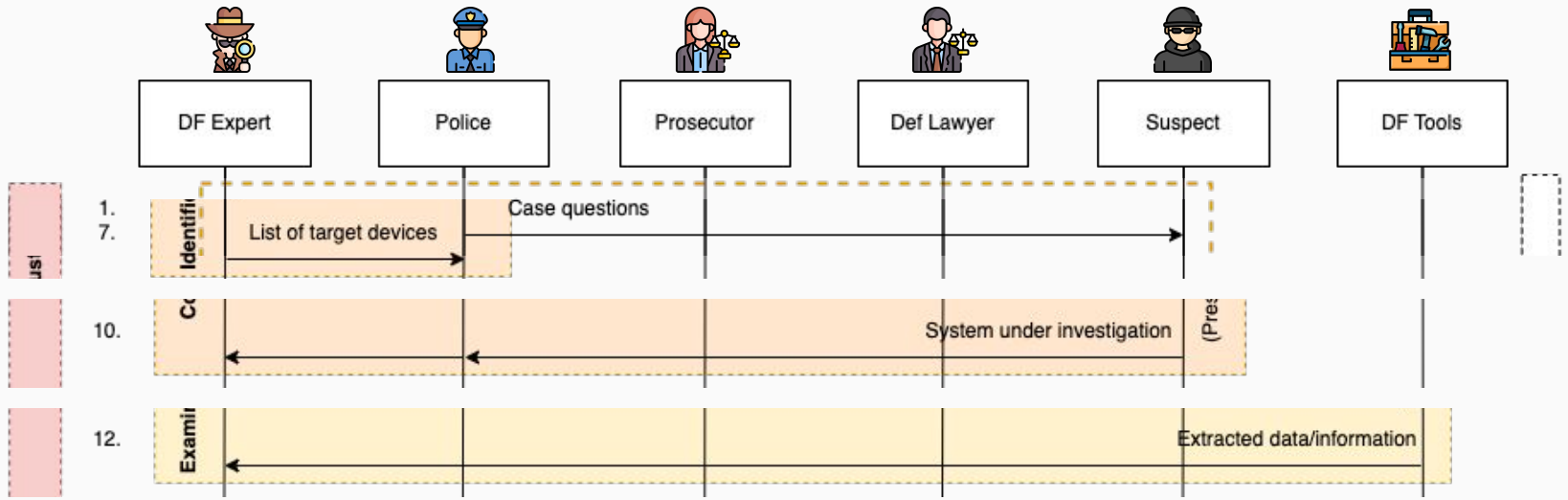
Go to **Protocol 3: Trial**

Protocol 2: Investigation



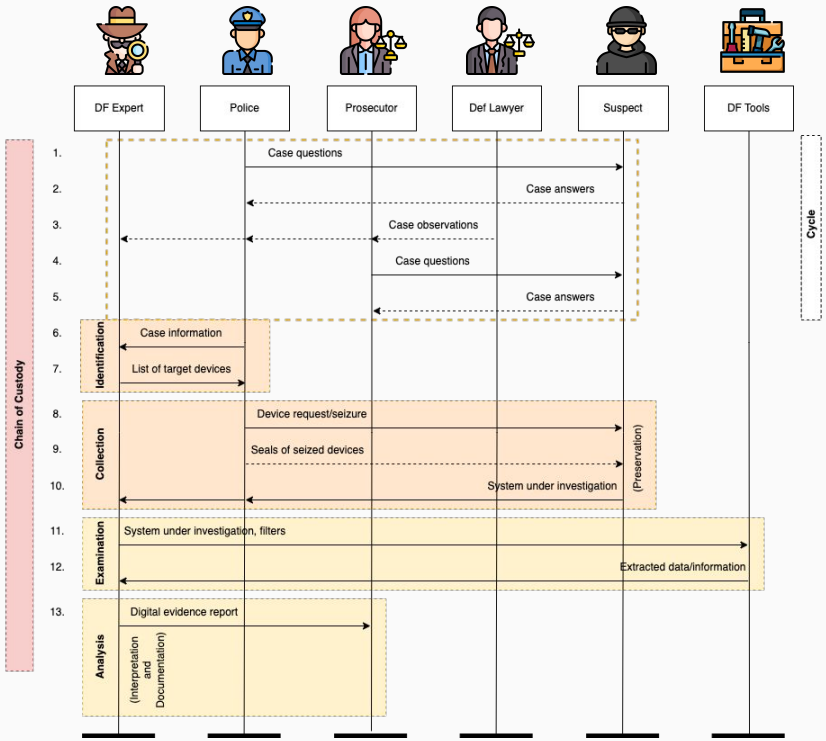
ADF Scenario			
#	Property	Attack Attempt(s)	Measure
1	Integrity	Suspect argues on consistency of case questions.	Cross verification
4	Integrity	Suspect argues on consistency of case questions.	Cross verification
8	Integrity	Suspect argues on insufficiency of measures. Suspect operates hacking, wiping, hiding, etc.	Forensic readiness Anti-Anti-Forensics

Protocol 2: Investigation



DF Scenario			
#	Property	Attack Attempt(s)	Measure
7	Integrity	DF Expert argues on consistency of devices.	Individual verification
7	Privacy	DF Expert collects more devices than necessary.	Data minimisation law
10	Integrity	DF Expert argues on manipulation/forgery of devices. DF Expert operates hacking, tampering with, etc.	Device hardening
12	Integrity	DF Expert argues on extracted data/info. DF Expert fine-tunes DF Tools to extract false data/info.	Individual verification

Protocol 2: Investigation



Go to **Protocol 3: Trial**

ADF Scenario

#	Property	Attack Attempt(s)	Measure
1	Integrity	Suspect argues on consistency of case questions.	Cross verification
4	Integrity	Suspect argues on consistency of case questions.	Cross verification
8	Integrity	Suspect argues on insufficiency of measures. Suspect operates hacking, wiping, hiding, etc.	Forensic readiness Anti-Anti-Forensics

DF Scenario

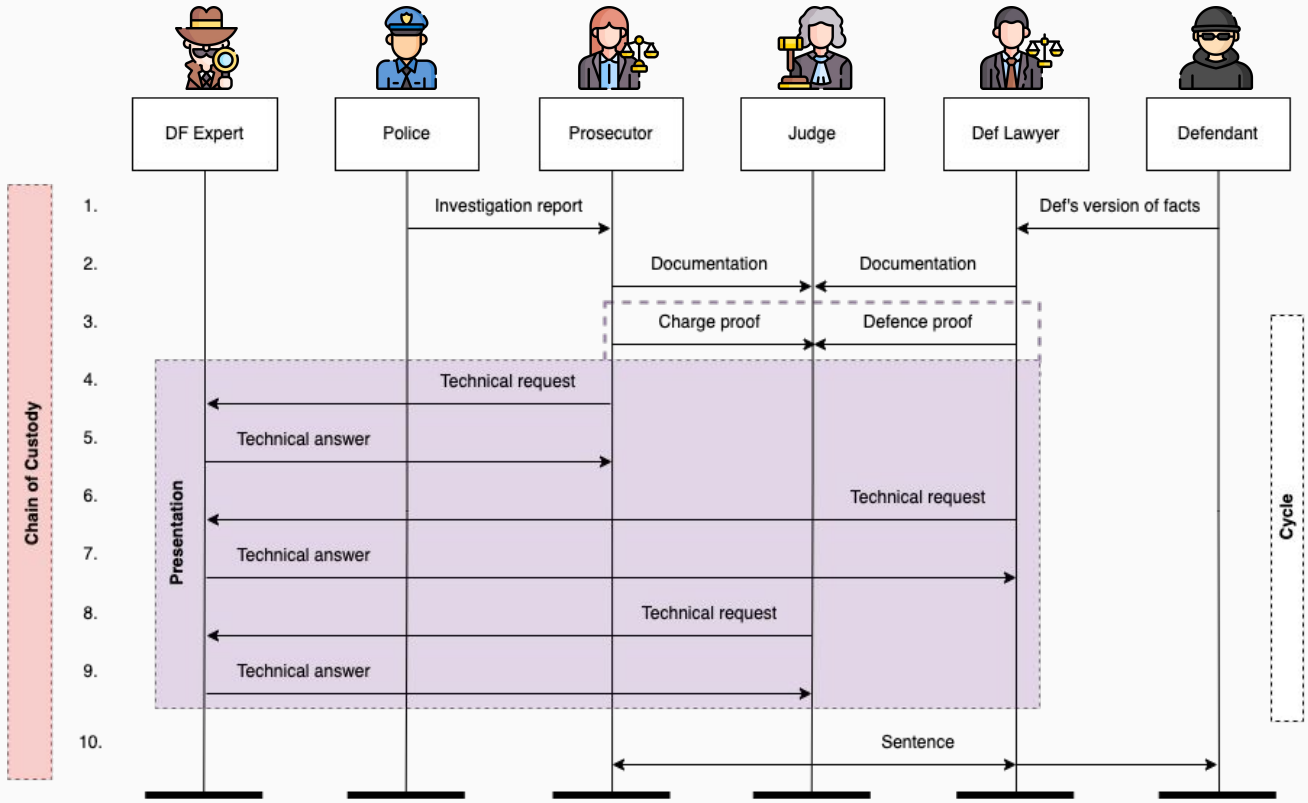
#	Property	Attack Attempt(s)	Measure
7	Integrity	DF Expert argues on consistency of devices.	Individual verification
7	Privacy	DF Expert collects more devices than necessary.	Data minimisation law
10	Integrity	DF Expert argues on manipulation/forgery of devices. DF Expert operates hacking, tampering with, etc.	Device hardening
12	Integrity	DF Expert argues on extracted data/info. DF Expert fine-tunes DF Tools to extract false data/info.	Individual verification

Is **privacy** only *threatened* in the **DF scenario**?

Agenda

1. Introduction
2. A Cybersecurity Perspective
3. The DF-ADF Dichotomy
4. The MSC-Model Approach
5. **The DFCI Protocols → Trial**
6. Conclusions

Protocol 3: Trial



Legend

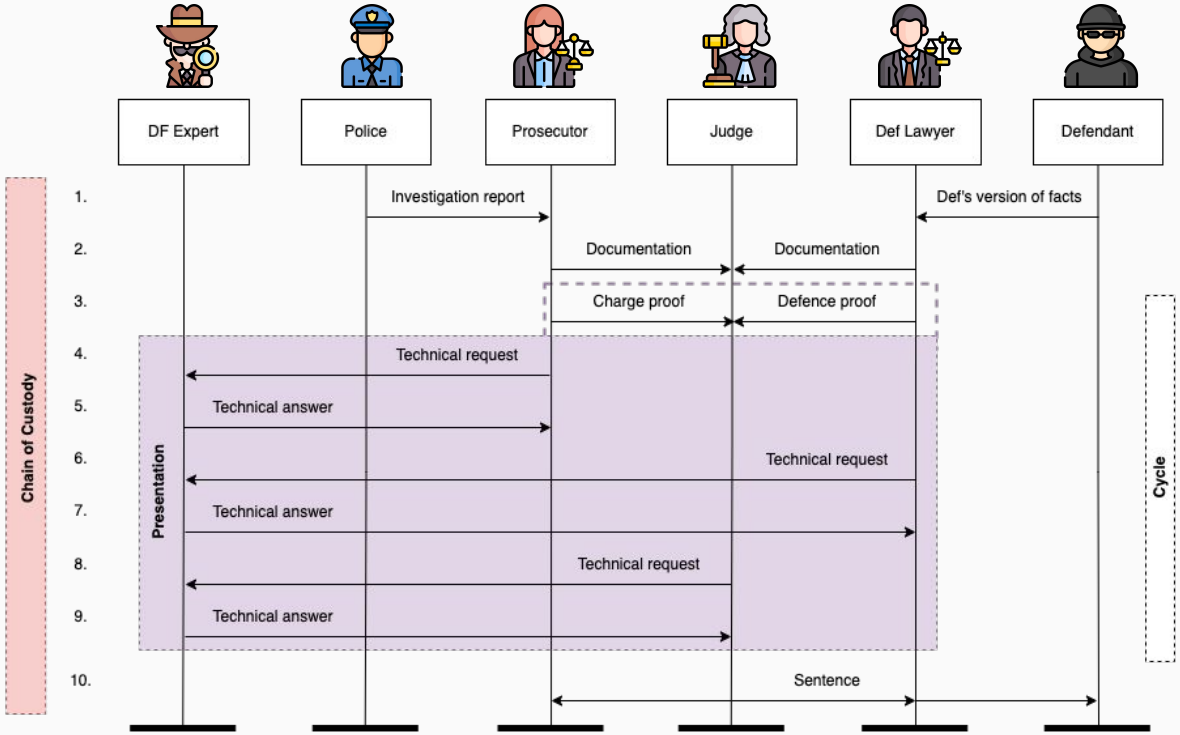
Court

Protocol Functional Objectives

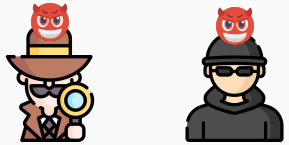
PO1: Defendant obtains a fair process.

PO2: (At least) Defendant and Def Lawyer obtain sentence.

Protocol 3: Trial



The **DF** and **ADF** scenarios are **symmetrical** here!



Takeaways

- DF-ADF in terms of CySec
- Two villains with a model

Agenda

1. Introduction
2. A Cybersecurity Perspective
3. The DF-ADF Dichotomy
4. The MSC-Model Approach
5. The DFCI Protocols
6. **Conclusions**

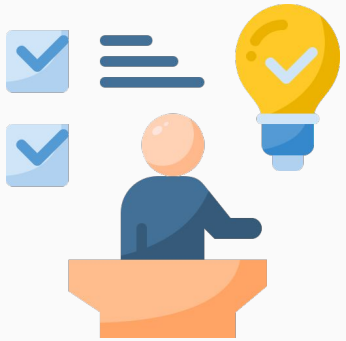
Conclusions

We employed **MSCs** to formalise *Digital Forensics in Crime Investigation*.

The **three protocols** provided a better understanding of the **DF-ADF dichotomy**.

Future work:

- Extract a *Kill Chain* for each threat agent
- Analyse other *threat model variants*
- Consider other *EU/Extra-EU systems*



References

Harel D., Thiagarajan P.S. (2003). Message Sequence Charts. In: Lavagno L., Martin G., Selic B. (eds) UML for Real. Springer, Boston, MA. https://doi.org/10.1007/0-306-48738-1_4

Conlan K. & Baggili I. & Breitinger F. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. Digital Investigation. http://dx.doi.org/10.1016/j.diin.2016.04.006

Paolo Tonini - Carlotta Conti, Manuale di procedura penale, XXIV ed., Giuffré, Torino, 2023

Thanks for your attention!

For more information or questions:

mario.raciti@imtlucca.it - mario.raciti@phd.unict.it

https://tsumarios.github.io/

@tsumarios

https://linkedin.com/in/marioraciti

Non-malicious QR (maybe)