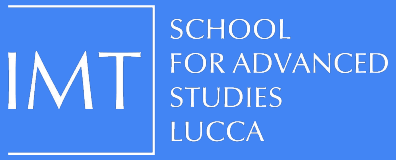
Behind the (Digital Crime) Scenes: An MSC-Model

Mario Raciti and Giampaolo Bella

ISDFS 2024



30/04/24 – San Antonio, TX

Agenda

1. **Introduction**
2. **The MSC-Model Approach**
3. **The DFCI Protocols**
4. **Conclusions**

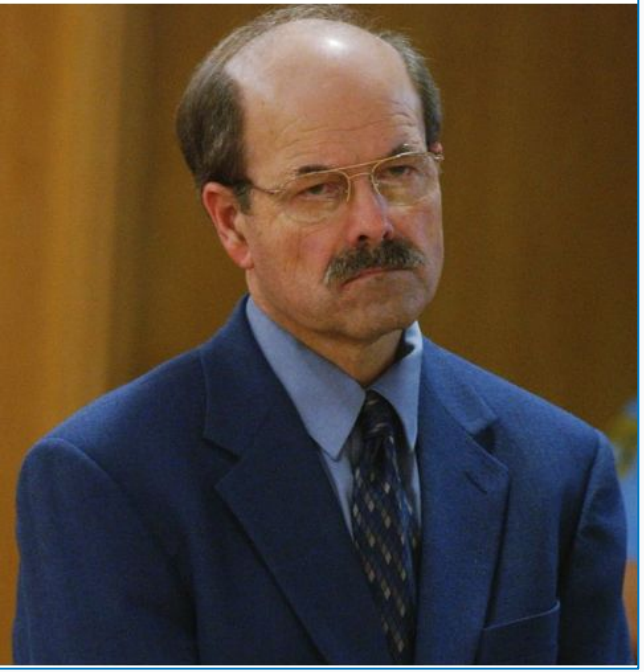
Agenda

1. **Introduction**
2. The MSC-Model Approach
3. The DFCI Protocols
4. 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 Right to Defence

The concept of a **fair and just defence** is an **essential right** enshrined within the principles of democratic legal system.

“Defence shall be an inviolable right at every stage and instance of legal proceedings.”
Article 24 of the Italian Constitution.

Concerns in DFCI

Cognitive biases, organisational traps, and *probability errors* may **affect** criminal investigations.

The **National Registry of Exonerations** has recorded *over 3,000 cases* of **wrongful convictions** in the United States as of 2023.

The **US vs. Ganias case** highlights **Fourth Amendment concerns** in digital data seizure.

The **US vs Comprehensive Drug Testing Inc. case** exemplifies **illegal data seizure** issues in criminal investigations.

A Cybersecurity Perspective on DFCI

A **fair and just** crime investigation **cannot be** an *arbitrary process*.

It must follow the **rules and laws** set by a given national or international authority to **ensure the defendants' rights**.

In a **cybersecurity fashion**, a crime investigation is a **protocol** where we can identify *actors* with roles, *interactions* with exchange of *messages*, and *requirements*.

RQ1: What are the available documents that explain how digital forensics in crime investigation works?

RQ2: Can we extrapolate a general MSC model for digital forensics in crime investigation from that knowledge base?

Agenda

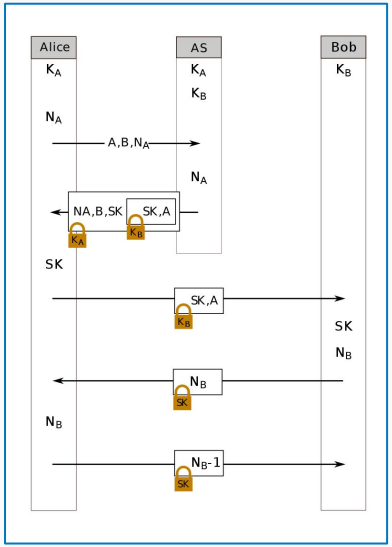
1. Introduction
2. **The MSC-Model Approach**
3. The DFCI Protocols
4. Conclusions

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*.

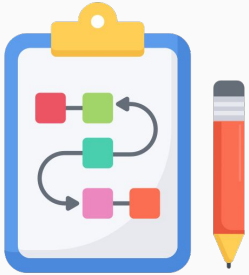


Symmetric NS Protocol – *Source: Wikipedia*

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**



Alice → Bob: {“Hi!”}

PO: Bob receives Alice’s message.

Looking for Sources (1)

> **Criminal Procedure** by **Wikipedia**

> **Comparative Criminal Procedure** by the **US Federal Judicial Center**

> **Rights of Defendants** (criminal proceedings) by the **European Commission**

> **Italian Code of Criminal Procedure**

> **How a Criminal Case Works** by the **UK Crown Prosecution Service**

> **Steps in the Federal Criminal Process** by the **US Department of Justice**

Looking for Sources (2)

> **The Budapest Convention** (ETS No. 185) by the **European Council**

> **ISO 27037**, **ISO 27043**

> **Standard Operating Procedures for the collection, analysis and presentation of electronic evidence** by the **Council of Europe**

> **Electronic Evidence Guide Version 3.0** by the **Council of Europe**

> **Best Practice Manual for the Forensic Examination of Digital Technology** by **ENFSI**

Agenda

1. Introduction
2. The MSC-Model Approach
3. **The DFCI Protocols**
4. Conclusions

Introducing the Key Actors

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

DF Expert

Prosecutor

Judge

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

Pubblico Ministero

Giudice del Dibatt.

Indagato/Imputato

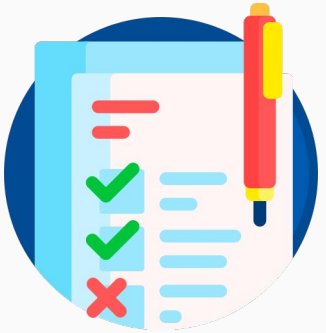
Some Assumptions

The **Need** for **Digital Forensics**

The **Retention** of the **DF Expert**

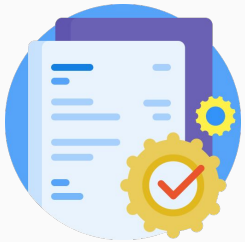
The **Phases** of **Digital Forensics**

The **Variety** of **Trials**



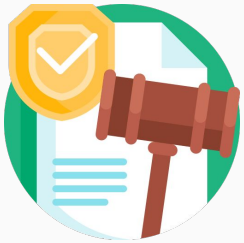
The Three Protocols of DFCI

Protocol 1: Init



Protocol 2: Investigation

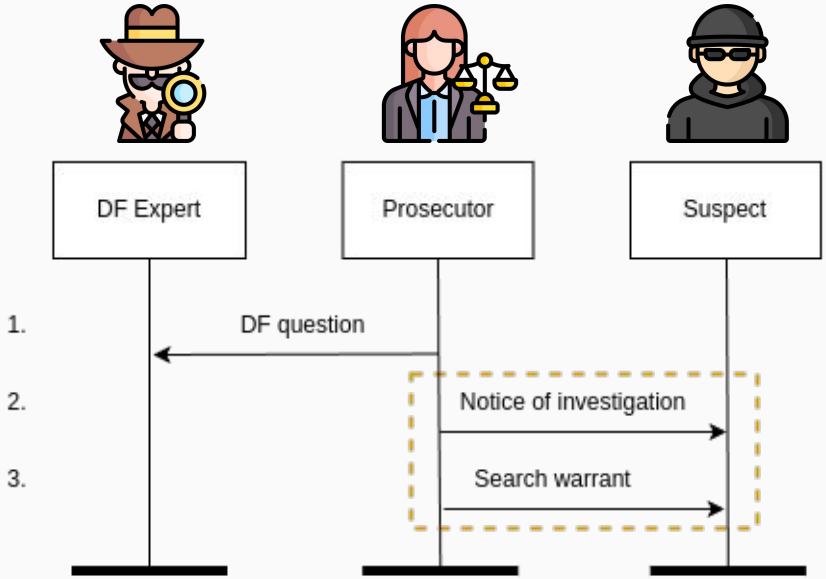
Protocol 3: Trial



Agenda

1. Introduction
2. The MSC-Model Approach
3. **The DFCI Protocols → Init**
4. Conclusions

Protocol 1: Init



Legend	
Crime Scene	

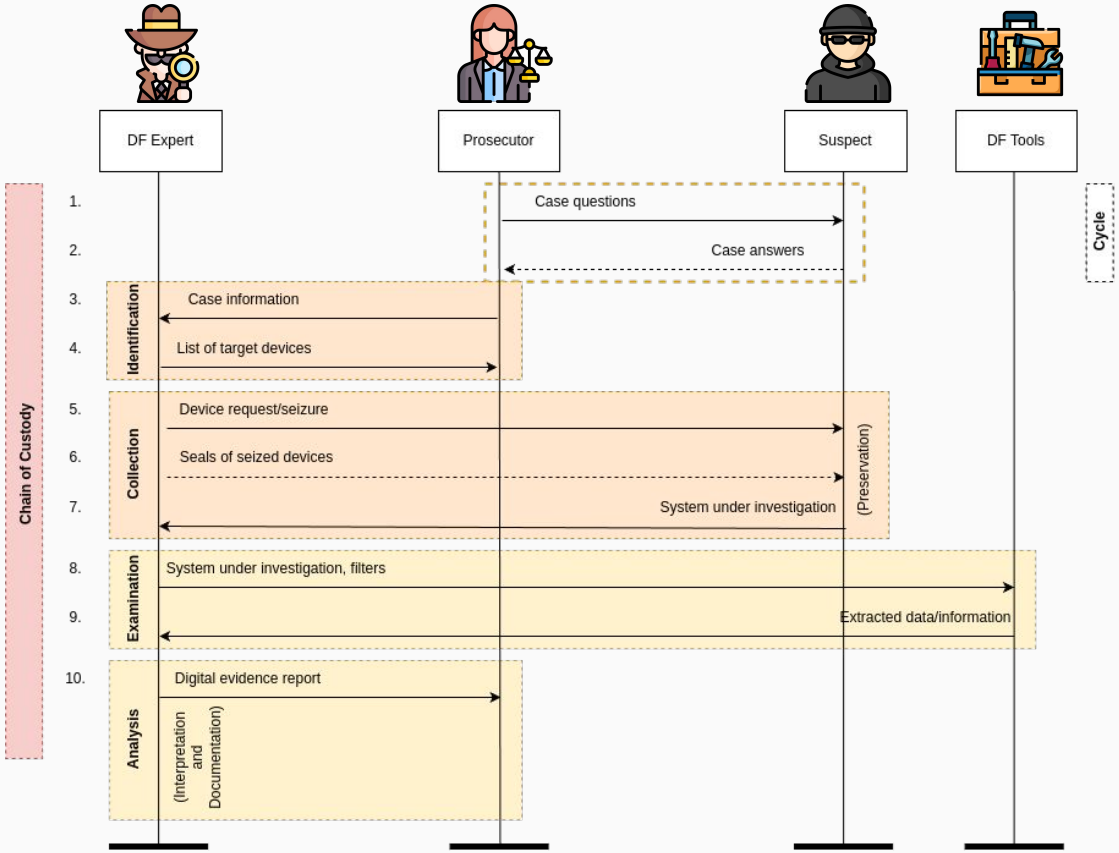
Protocol Functional Objectives
PO1: Suspect gets search warrant.

Go to **Protocol 2: Investigation**

Agenda

1. Introduction
2. The MSC-Model Approach
3. **The DFCI Protocols → Investigation**
4. Conclusions

Protocol 2: Investigation



Go to **Protocol 3: Trial**

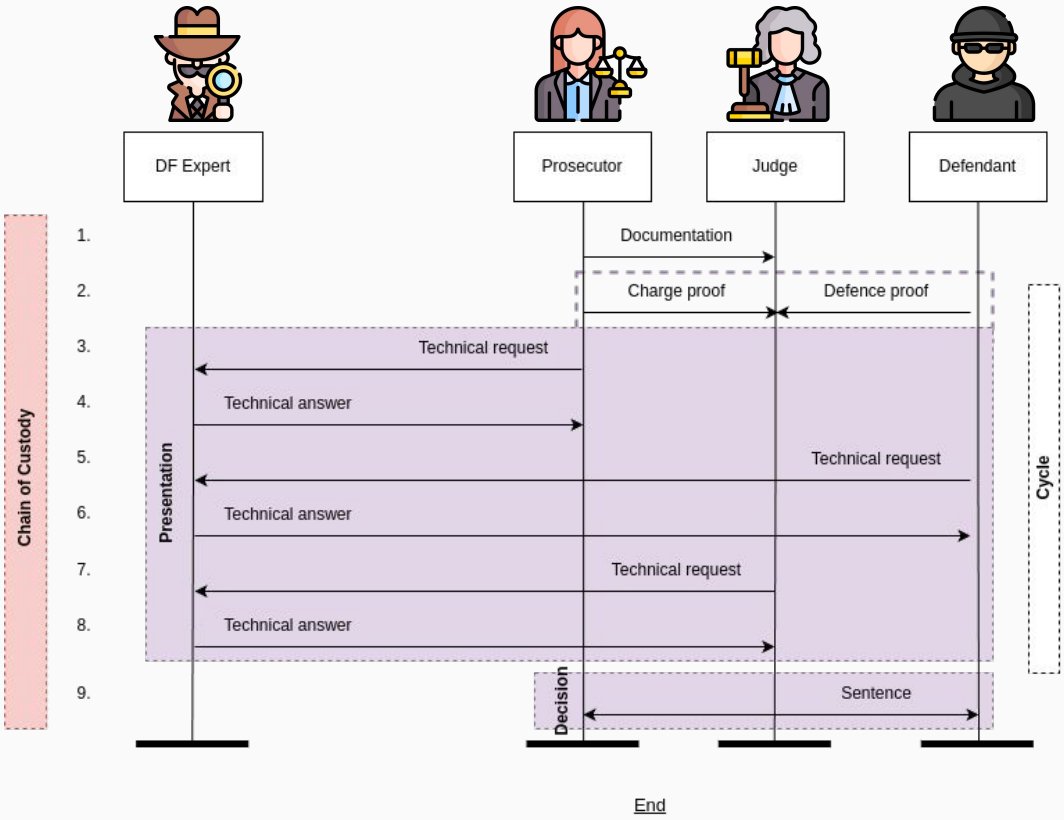
Legend	
Optional	⇢
Crime Scene	
DF Lab	

Protocol Functional Objectives
PO1: Prosecutor obtains set of information to prove or confute charges.

Agenda

1. Introduction
2. The MSC-Model Approach
3. **The DFCI Protocols → Trial**
4. Conclusions

Protocol 3: Trial



Legend	
Court	

Protocol Functional Objectives
PO1: Defendant obtains a fair process.
PO2: (At least) Defendant obtains sentence.

Takeaways

- More clarity on DFCI
- Reference model for CySec

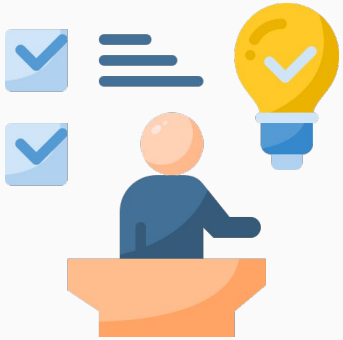
Agenda

1. Introduction
2. The MSC-Model Approach
3. The DFCI Protocols
4. **Conclusions**

Conclusions

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

The **three protocols** provide a better understanding of **DFCI**.



Future work looks at refining the MSC model on:

- variations of **threat models**
- elicitation of **non-functional requirements**
- identification of **potential attacks** against the *investigative process* and/or the *defendant's rights*
- definition of **measures** to mitigate those attacks

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)