



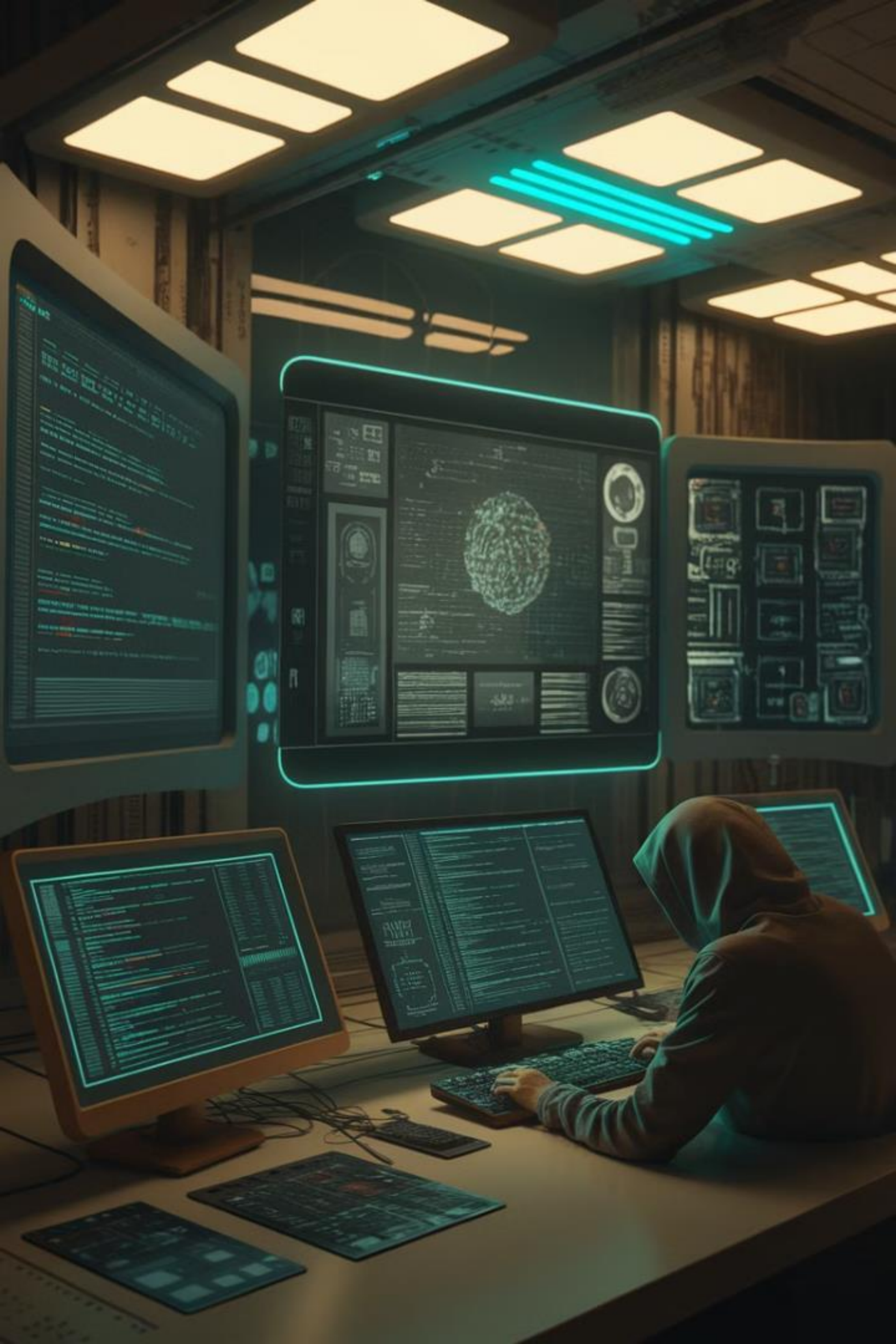
**Politecnico
di Torino**

Computer Forensics Class 2024/2025

Hacking Team Case



Background on Hacking Team



Hacking Team: Controversial Cybersecurity Firm

Hacking Team was an Italian technology company known for selling offensive intrusion and surveillance services to governments and law enforcement worldwide. Founded in 2003, it faced criticism for its controversial practices and clientele.



Company Overview

1

Founded

Established in 2003 by David Vincenzetti in Milan, Italy.

2

Business Model

Provided offensive hacking and surveillance software to governments and agencies.

3

Key Clients

Worked with NSA, CIA, FBI, and various international law enforcement agencies.

Core Technologies



Remote Control System

Software for monitoring Internet communications and decrypting files.



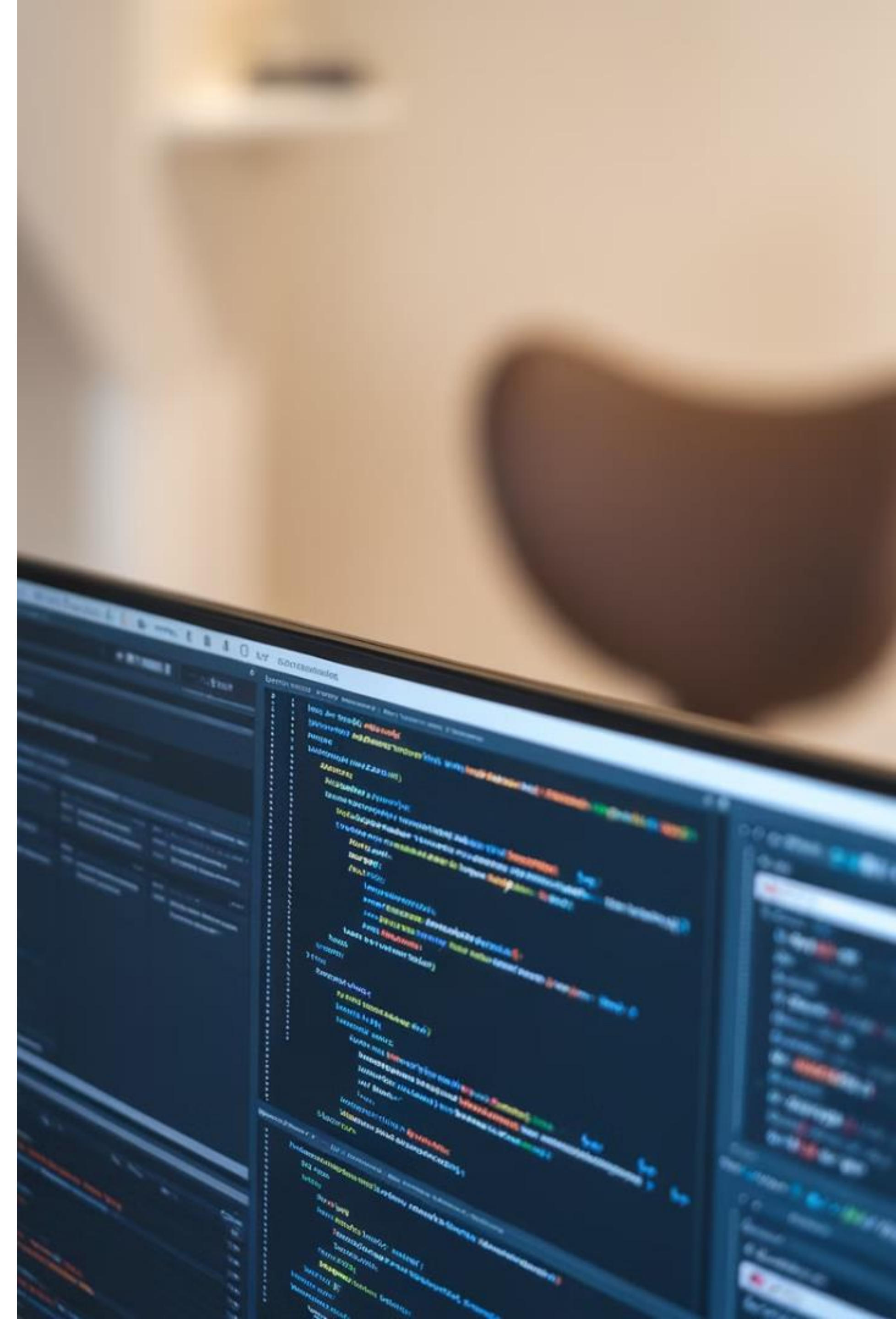
Mobile Surveillance

Tools for tracking cell phones, calls, and messages.



Remote Activation

Capability to remotely activate microphones and cameras on target devices and location tracking.



Advanced Surveillance Techniques

Battery Optimization

Techniques to avoid suspicious battery drain on monitored devices.

Stealth Operations

Methods to make surveillance difficult to detect.

Data Extraction

Sophisticated tools for extracting and analyzing target information.



Founding and Early Years

1

2003

Founded by David Vincenzetti and Valeriano Bedeschi.

2

2007

Received 8 millions in funding from Italian venture capital firms.

3

Early Success

Software purchased by Milan police, becoming first commercial hacking software provider.



Applications of Technology

1

Counter-Terrorism

Used to monitor and track potential terrorist activities.

2

Drug Trafficking

Employed in international efforts to combat narcotics trade.

3

Organized Crime

Utilized to gather intelligence on mafia and criminal organizations.





High-Level Connections

Booz Allen Hamilton

Established relations with Mike McConnell, former NSA director and intelligence advisor.

US Intelligence

Connections to NSA, CIA, and FBI.

Global Reach

Worked with intelligence agencies worldwide.

Saudi Arabia Acquisition Attempt

1

2013

Negotiations began with Saudi Arabian government for acquisition.

2

Valuation

Company valued at \$2 billion, Saudi offer around \$140 million.

3

Mediators

Wafic Said involved, third wealthiest Arab billionaire in Britain.





Controversial Clients

1

Sudan

Sold software to Sudan despite UN arms embargo.

2

Bahrain

Provided surveillance tools to Bahraini government.

3

Saudi Arabia

Supplied spyware to Saudi Arabian authorities.



UN Investigation

1

June 2014

UN commission inquired about software sales to Sudan.

2

January 2015

Hacking Team denied current sales to Sudan.

3

March 2015

UN insisted software could be classified as military equipment.



Italian Export Ban

1

Autumn 2014

Italian government froze Hacking Team's exports.

2

Lobbying Efforts

Company engaged in lobbying to overturn the ban.

3

Ban Lifted

Hacking Team regained right to sell products abroad.

Ethical Concerns

Human Rights

Criticized for enabling surveillance in countries with poor human rights records.

Privacy Violations

Tools potentially used to violate citizens' privacy rights.

Democratic Concerns

Accusations of compromising democracy in some nations.



Legal Challenges

UN Sanctions

Questioned about potential violations of UN arms embargo.

1

Italian Export Laws

Faced temporary ban on exports from Italian government.

2

Privacy Lawsuits

Subject to legal actions related to privacy violations in multiple countries.

3



The investigation



2015 Data Breach

Event

Hacking Team itself became victim of a cyber attack.

1

Aftermath

Exposed internal operations and client list of the company.

3

2

Consequence

400 gigabytes of confidential data leaked to the public.



Client List and Revenue

Client Types

Primarily military, police, governments, and intelligence agencies.

Corporate Clients

Partnerships with multinational corporations, including Boeing.

Revenue

Reported revenue over €40 million, with suggestions of larger offshore contracts.



Milan Prosecutor's Investigation

1

Trigger

Suspicious payment from a Saudi company to SoftHack Srl.

2

Action

Prosecutor Alessandro Gobbis ordered a search of the Turin-based company.

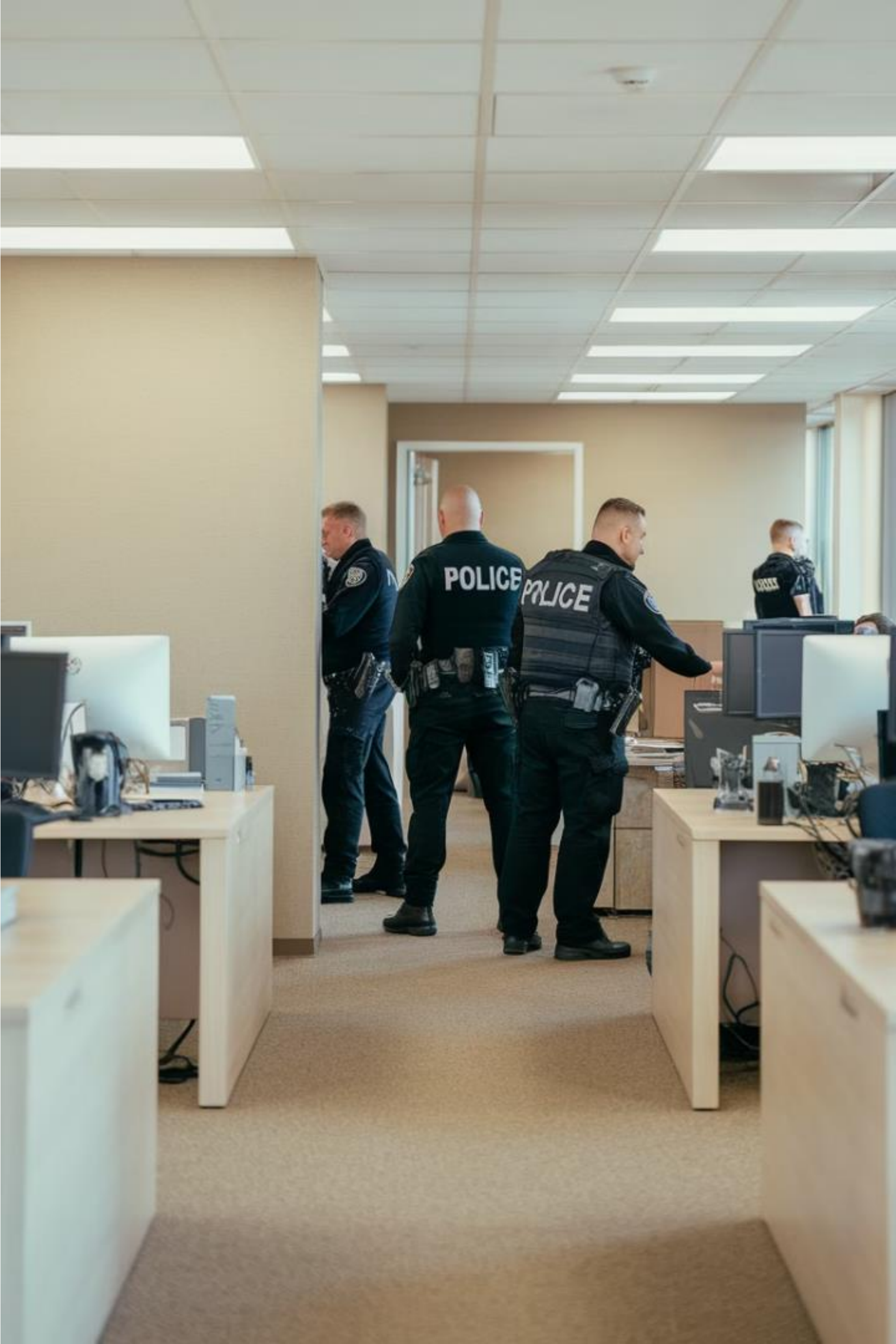
3

Suspicion

Possible sale of Galileo spyware source code to unauthorized parties.

SoftHack Srl Investigation

Company	SoftHack Srl (Turin)
Individual	Luca Spector (developer)
Charges	Unauthorized system access, industrial secret disclosure





Suspicious Transaction Details

Date	Amount
November 20, 2014	300,000 euros
Sender	Recipient
Saudi Technology Development Inv	SoftHack Srl



Prosecutor's Suspicions

1

Cover Story

Payment claimed to be for professional training services.

2

Real Purpose

Suspected sale of Galileo spyware source code.

3

Potential Misuse

Concerns that the software could be used by terrorist groups.

Saudi Technology Development Inv



Investigation Focus

Examining company's shareholders and potential jihadist connections.



Intermediary Role

Suspected to be a mediator for an unknown client.



Unknown Motives

Reasons for acquiring the software remain unclear.





SoftHack's Defense

1

Denial

Lawyer claims accusations are false rumors spread by Hacking Team.

2

Clarification

No explicit mention of selling services to Arabs or terrorists in search warrant.

3

Transparency

Willingness to cooperate with investigations to prove innocence.



Ongoing Investigation

1

Current Focus

Examining Saudi Technology Development Inv's background and connections.

2

Key Question

Determining if spyware reached terrorist groups.

3

Next Steps

Further interrogations and analysis of financial transactions.



Search and Seizure



Subject: Search and Seizure of Electronic Devices

Italian Cybercrime Unit

Location to be Searched:


- SoftHack Srl Headquarters, Turin

Items to be Seized:

- Laptop computers
- Smartphones
- CCTV cameras
- Tablets (including iPads)
- Other electronic devices that may contain digital evidence relevant to the investigation.

Purpose of Warrant

This warrant is issued as part of an investigation by the Prosecutor's Office of Milan into unauthorized access to the proprietary software source code of Hacking Team, a Milan-based company specializing in intelligence software. Evidence indicates that on [specific date], SoftHack Srl, based in Turin and associated with former Hacking Team employees Red and White, may have received a substantial payment from the Saudi company Saudi Technology Development Inv. under potentially false pretenses of professional training. It is suspected that the payment was instead compensation for transferring sensitive source code and other proprietary information.


PROCURA DELLA REPUBBLICA
Presso il Tribunale di Roma
* Piazzale Clodio - Città Giudiziaria - Palazzina C - piano 2° - stanza 253 *
Tel. 06.38703933 - fax 06.38703934

OGGETTO: Procedimento Penale [REDACTED]

AL COMANDO COMPAGNIA CARABINIERI
Nucleo Operativo
ROMA TRIONFALE

In relazione al procedimento penale in oggetto indicato, trasmetto per l'immediata esecuzione - in 6 copie conformi all'originale - il DECRETO DI PERQUISIZIONE LOCALE - PERSONALE E SEQUESTRO - INFORMAZIONE DI GARANZIA - INFORMAZIONE SUL DIRITTO DI DIFESA, nr. 31579/17 R.G. NOTI emesso in data 18.07.2017 a carico dei nominati in oggetto

Si chiede inoltre di redigere nei confronti dei succitati Verbale d'identificazione, elezione di domicilio e nomina del difensore di fiducia ai sensi dell'art. 161 C.P.P.

Si resta in attesa di sollecito riscontro

Roma, 18.07.2017

[REDACTED]

Subject: Search and Seizure of Electronic Devices

Italian Cybercrime Unit

Justification for Immediate Seizure

The presence of specific electronic devices at SoftHack Srl is suspected to contain evidence crucial for resolving the case and preventing tampering, destruction, or concealment of data. Immediate seizure is ordered to ensure digital evidence is preserved in its original form, thereby maintaining integrity according to digital forensics protocols.

Digital Forensics Standards

The execution of this search and seizure is to adhere to strict digital forensics principles to ensure evidence integrity and legal admissibility:

1. Integrity of Evidence

All electronic devices must be handled to prevent any alteration of data. Forensic experts should manage and secure the devices in a controlled environment, using write-blocking tools and creating forensic images of all data before examination.

2. Documentation and Chain of Custody

A detailed log of each device must be maintained, including device serial numbers, types, and any identifying marks. The chain of custody for each piece of evidence must be recorded from seizure to examination to safeguard transparency and traceability.

3. Impartiality and Accuracy

Compliance with digital forensics standards is mandatory to avoid contamination or bias. Write-protecting technology and forensic imaging will be used to maintain original evidence unaltered.

PROCURA DELLA REPUBBLICA
Presso il Tribunale di Roma
* Piazzale Clodio - Città Giudiziaria - Palazzina C - piano 2° - stanza 253 *
Tel. 06.38703933 - fax 06.38703934

OGGETTO: - Procedimento Penale - [Redacted]
[Redacted]
[Redacted]

AL COMANDO COMPAGNIA CARABINIERI
Nucleo Operativo
ROMA TRIONFALE

In relazione al procedimento penale in oggetto indicato, trasmetto per l'immediata esecuzione - in 6 copie conformi all'originale - il DECRETO DI PERQUISIZIONE LOCALE - PERSONALE E SEQUESTRO - INFORMAZIONE DI GARANZIA - INFORMAZIONE SUL DIRITTO DI DIFESA, nr. 31579/17 R.G. NOTI emesso in data 18.07.2017 a carico dei nominati in oggetto

Si chiede inoltre di redigere nei confronti dei succitati Verbale d'identificazione, elezione di domicilio e nomina del difensore di fiducia ai sensi dell'art. 161 C.P.P.

Si resta in attesa di sollecito riscontro

Roma, 18.07.2017

PER RICEVUTA
[Signature]

Subject: Search and Seizure of Electronic Devices

Italian Cybercrime Unit

Execution of the Warrant

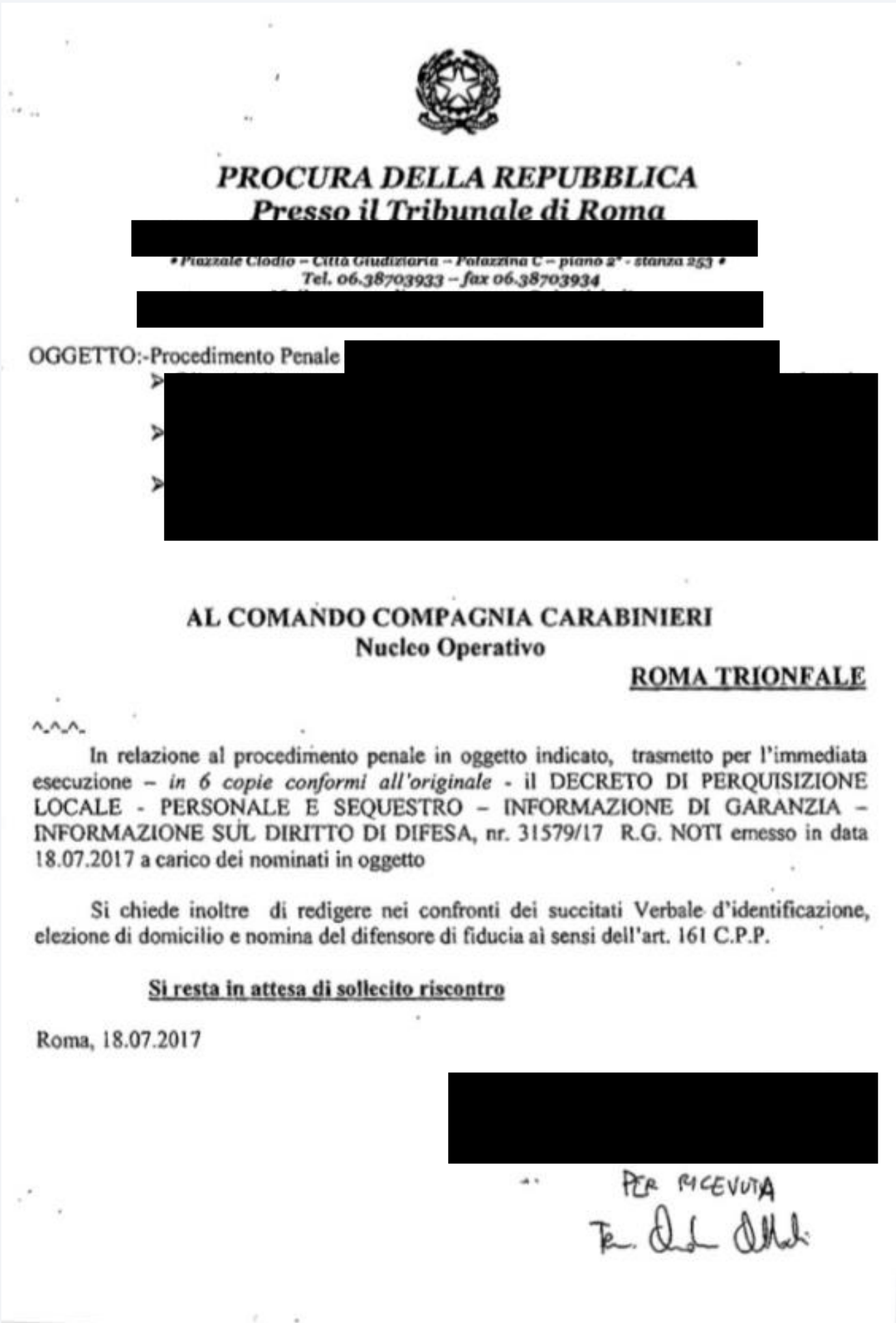
This warrant authorizes entry and search of the premises at SoftHack Srl, Turin, with a specific focus on the electronic devices listed above. The warrant shall be executed within [timeframe], after which all seized devices will be transferred securely to [designated forensic lab or appropriate authority].

Additional Provisions

The warrant does not authorize access to private data unrelated to the case. All procedures must comply with applicable data protection laws to respect the privacy of unrelated individuals or data.

Order

The Prosecutor’s Office of Milan hereby issues this search and seizure warrant on this day, [Insert Date], to be executed per the standards outlined above, ensuring preservation and forensic reliability of all digital evidence.





What Prosecutor and Law Enforcement Officers Should do to respect digital forensics principle during the investigation?

What is the most effective strategy to demonstrate the liability of the investigated/suspected person?



What the defendant's attorney should do during the investigation to respect the fundamental right of the defendants?

What the attorney should do give to the Judge evidences of the innocence of his Client?