



MINISTERIO
DEL INTERIOR



FIGHTING CYBERCRIME THE NEW CHALLENGE



César Lorenzana González

Cpt. Guardia Civil

Cybercrime Unit (U.C.O.)

CoE Regional Workshop

Tbilisi, 13th May 2010



MINISTERIO
DEL INTERIOR



GUARDIA CIVIL

AGENDA

CYBERCRIME UNIT PROFILE

- Technicians.
- Investigators.
- «Hackers»??

CYBER - INVESTIGATION

- Facts Rating
- Gathering Hints
- Prosecution

INVESTIGATION DIFFICULTIES

- Data retention
- User identification
- Electronic evidences





MINISTERIO
DEL INTERIOR



CYBERCRIME



CONVENTION ON CYBERCRIME
Budapest, 23rd november 2001



Those crimes, that
affect data or
computer systems.



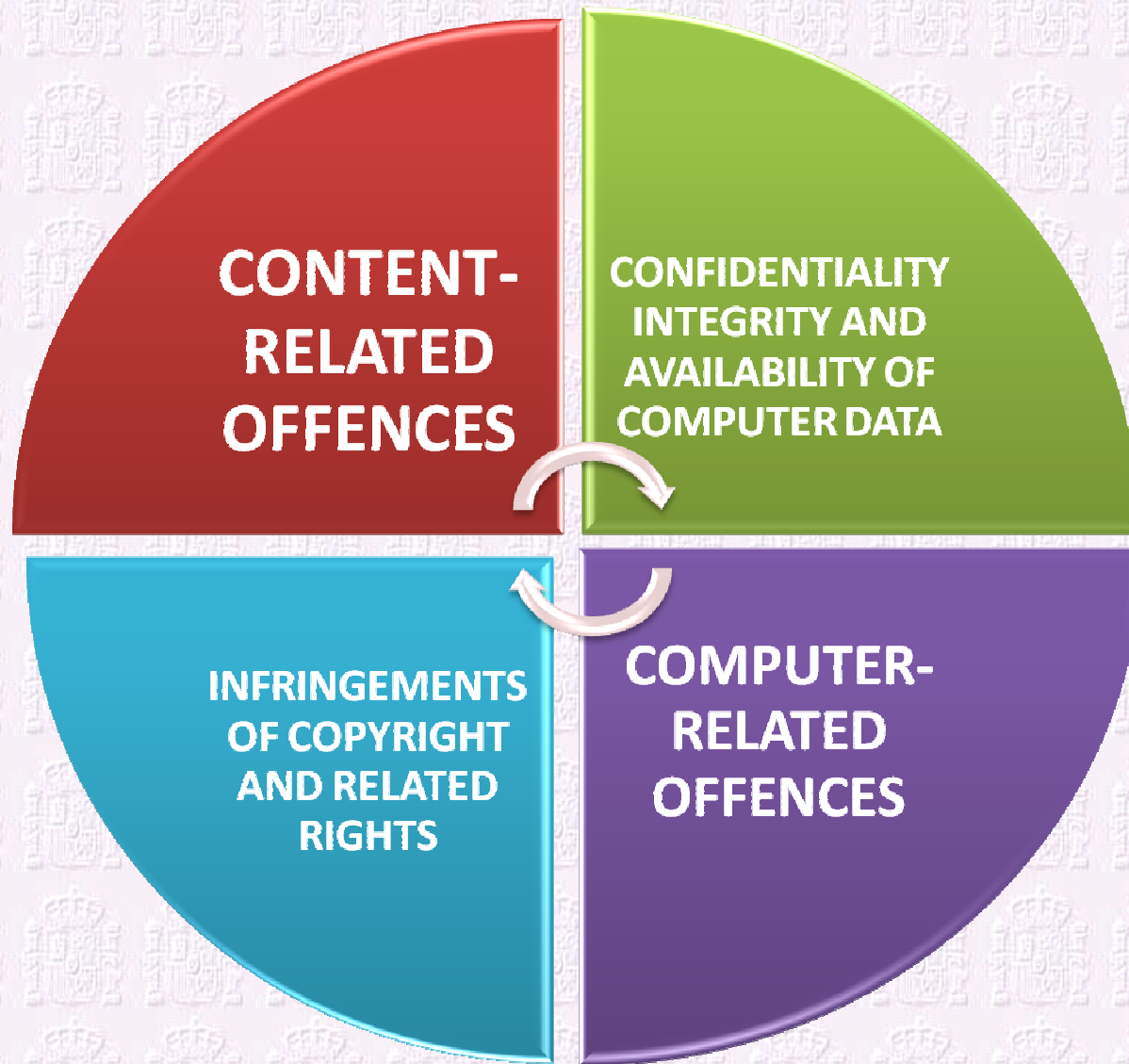


MINISTERIO
DEL INTERIOR



GUARDIA CIVIL

TYPES OF CYBERCRIME



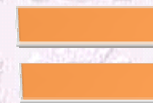


MINISTERIO
DEL INTERIOR



GUARDIA CIVIL

Investigators - PROFILE



**POLICE
PROFILE**

**TECHNICIAN
PROFILE**

Instinct

BINARY Translators

Investigative Tactics

Techincal Resources

Legal knowledge

Developer Abilities

Social Abilities

**Computers
Knowledge**





MINISTERIO
DEL INTERIOR



GUARDIA CIVIL

CRIME

EFFECTS

SUCCESS

PLANNING

SECURING

INVESTIGATOR

OFFENDER



YOU HAVE BEEN
HACKED !





MINISTERIO
DEL INTERIOR



GUARDIA CIVIL



Gathering Data

System
Logs

Police
DB

PC's

Public
DB

ISP's

ex Seleccionar Símbolo del sistema (2)

Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\YK>ping www.tinkebell.com

Haciendo ping a www.tinkebell.com [82.192.68.18] con 32 bytes:

Respuesta desde 82.192.68.18: bytes=32 tiempo=74ms TTL=54

Respuesta desde 82.192.68.18: bytes=32 tiempo=117ms TTL=54

Respuesta desde 82.192.68.18: bytes=32 tiempo=75ms TTL=54

Respuesta desde 82.192.68.18: bytes=32 tiempo=111ms TTL=54

Estadísticas de ping para 82.192.68.18:

Paquetes: enviados = 4, recibidos = 4, perdidos = 0

(0% perdidos).

Tiempos aproximados de ida y vuelta en milisegundos:

Mínimo = 74ms, Máximo = 117ms, Media = 94ms

C:\Documents and Settings\YK>





MINISTERIO
DEL INTERIOR



GUARDIA CIVIL

PROSECUTION





MINISTERIO
DEL INTERIOR



GOALS FOR HOUSE SEARCHES



**Electronic
Devices
Seizure**



**Try to link
User&Computer**





MINISTERIO
DEL INTERIOR



POLICE TECHNICAL REPORT



Seized Electronic Devices



Backups or System images



Thumbdrives, storing devices



Documments & Manuals





MINISTERIO
DEL INTERIOR



PRESENTING THE CASE TO COURT

Description
of evidences



**ELECTRONIC
EVIDENCE**

Non-
technical
language

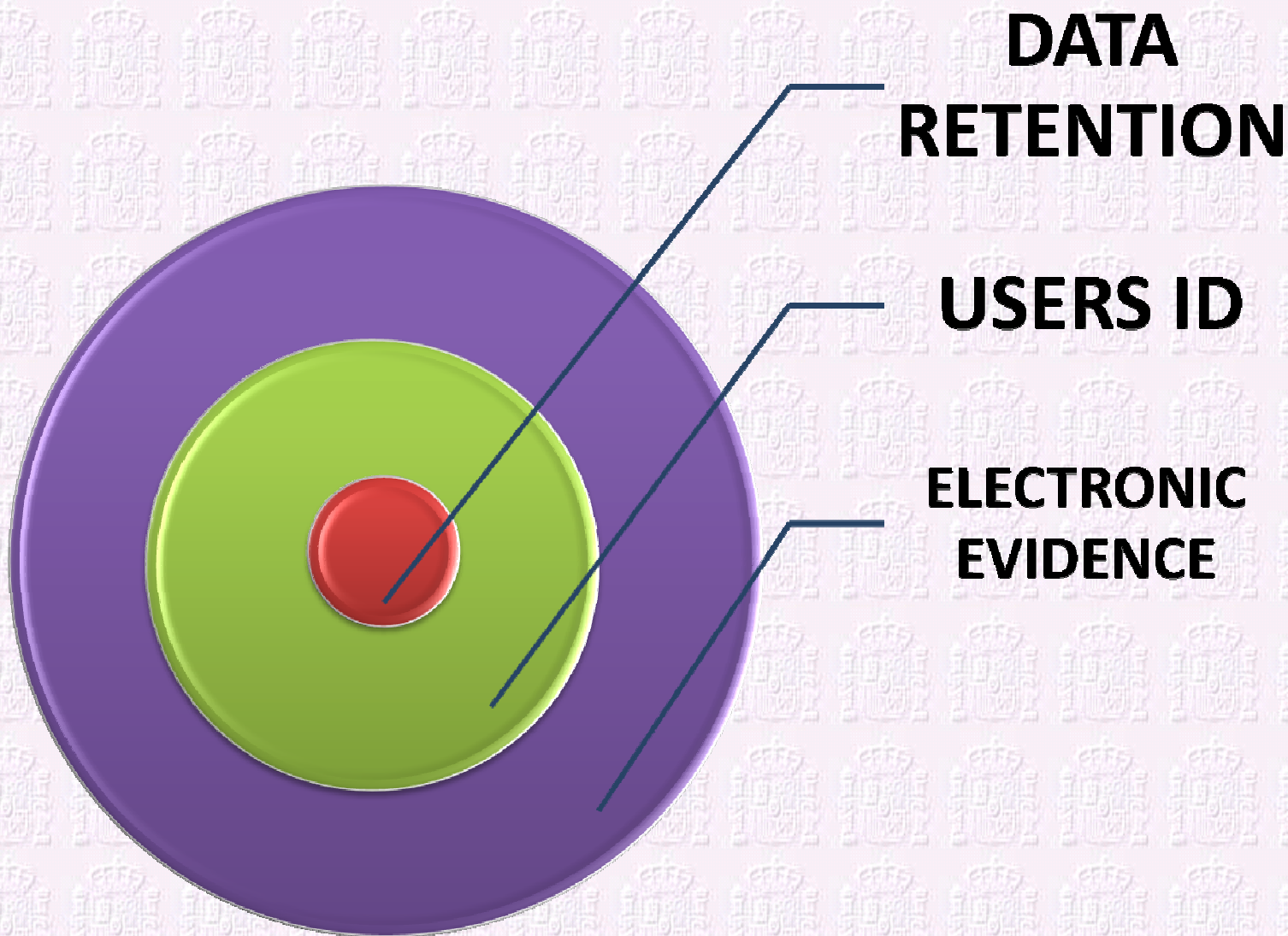




MINISTERIO
DEL INTERIOR



INVESTIGATION DIFFICULTIES

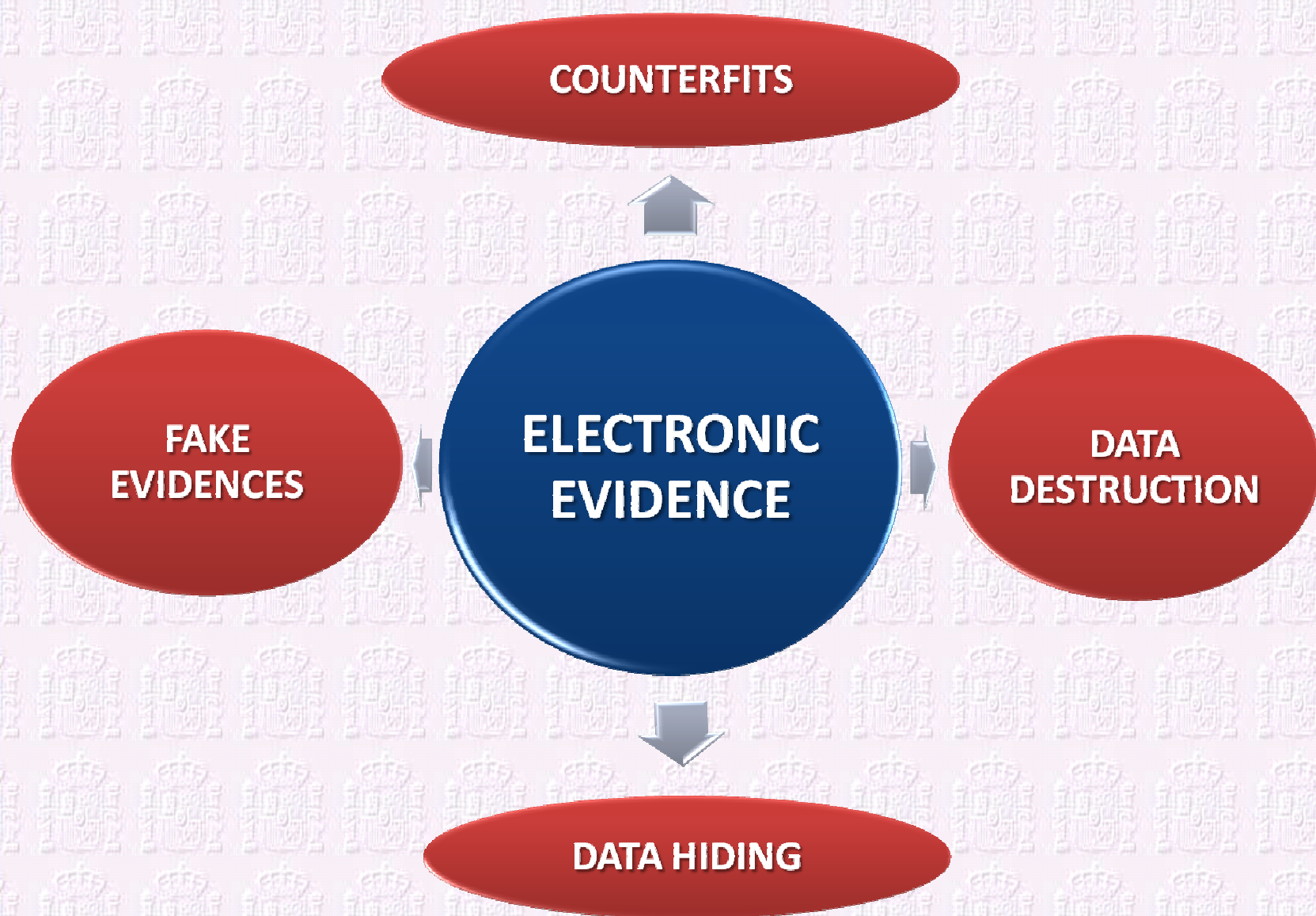




MINISTERIO
DEL INTERIOR



GUARDIA CIVIL





MINISTERIO
DEL INTERIOR



GUARDIA CIVIL



POLICE
EFFORTS

LIVE ANALYSIS

EFFICENCY



POLICE
TECHNICAL
REPORT

FORENSIC
ANALYSIS





MINISTERIO
DEL INTERIOR



GUARDIA CIVIL

High Tech Crime Group

Guardia Civil



delitostelematicos@guardiacivil.org



www.gdt.guardiacivil.es



Calle Salinas del Rosio 33-35;
28042 Madrid (Spain)



+34 91 503 1300



+34 91 503 14 37

