Documentation

THE LIFE CYCLE OF E-EVIDENCE

THE RISE OF EVIDENCE ON MOBILE DEVICES

317DT61 Madrid, 23-24 May 2017

Co-funded by the Criminal Justice Programme of the European Union 2014-2020

Objective of the seminar

Mobile devices such as smartphones and tablets contain personal information such as call history, text messages, e-mails, digital photographs, videos, calendar items, address books, passwords and credit card numbers. They can be useful as sources of digital evidence to be examined when criminal activities occur.

This seminar aims to share advanced knowledge and the exchange of experience and best practice between judges, prosecutors and lawyers in private practice who deal with criminal proceedings involving e-evidence on mobile devices.

Key topics of the seminar

- Definition of 'e-evidence': practical examples of analogue and digital evidence
- Legal implications of e-evidence (collection, evaluation and admissibility)
- The rise of evidence on mobile devices
- Insights into different national criminal justice systems regarding the handling of e-evidence in court

Who should attend?

Judges, prosecutors and lawyers in private practice.

About the project

This seminar is part of a training project, sponsored by the European Commission, which consists of four more events to take place in Athens, Trier, Prague and Tallinn.

Each seminar will have a specific focus:

- Handling e-evidence in online fraud cases (Athens, 7-8 November 2017)
- Handling e-evidence in child sex abuse material (Trier, February 2018)
- The challenges posed by "Cloud Computing" (Prague, May 2018)
- Acquisition of e-evidence and jurisdictional issues (Tallinn, September 2018)

Speakers and Chairs

Laviero Buono, Head of Section, European Criminal Law, ERA, Trier

Cormac Callanan, CEO, Aconite Internet Solutions, Dublin

Tais Deus Ramos, Prosecutor, Mataró Prosecutor Office, Barcelona

Hein Dries-Ziekenheiner, CEO, Vigilo Consult, Leiden

Damir Kahvedžić, Digital Forensic and eDiscovery Consultant, Espion, Dublin

Stephen Mason, Barrister and Associate Research Fellow, Institute of Advanced Legal Studies, London

Tõnu Mets, Attorney at Law, IT Law Programme, University of Tartu

Abraham Pasamar, CEO, Incide Digital Data, Member of the Spanish Cybercrime Centre of Excellence, Barcelona

Israel Pastor Sainz-Pardo, Director, Centre for Legal Studies (CEJ), Madrid

Lodewijk van Zwieten, National Prosecutor for High Tech Crime, Rotterdam; Seconded National Expert on Cybercrime, Eurojust, The Hague

This publication has been produced with the financial support of the Justice Programme 2014-2020 of the European Union. The content of this publication reflects only ERA's view and the Commission is not responsible for any use that may be made of the information it contains.

For further information

Liz Klopocki
Tel. +49 (0) 651 937 37 322
Fax. +49 (0) 651 937 37 791
E-mail: eklopocki@era.int
Online application: www.era.int/?126363&en

GOBIERNO DE ESPAÑA MINISTERIO DE JUSTICIA

ERA
Europäische Rechtsakademie
Academy of European Law
Académie de Droit Européen
Accademia di Diritto Europeo

THE LIFE CYCLE OF E-EVIDENCE

THE RISE OF EVIDENCE ON MOBILE DEVICES

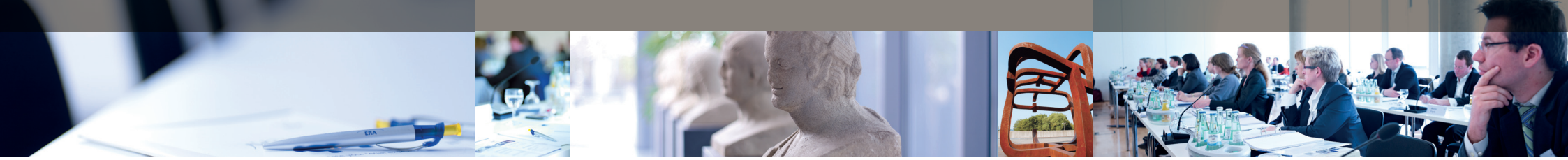
Madrid, 23-24 May 2017
Centro de Estudios Jurídicos,
Calle de Juan del Rosal, 2
Madrid

Organiser:
ERA (Laviero Buono) in cooperation with the Centro de Estudios Jurídicos (Ministry of Justice), Spain

Language:
English

Event number: 317DT61

With the support of the Justice Programme 2014-2020 of the European Union



Tuesday 23 May 2017

08:30 Arrival and registration of participants

09:00 **Welcome and introduction to the programme**
- *Israel Pastor Sainz-Pardo*
- *Laviero Buono*

SESSION I – FUNDAMENTALS OF ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS (WITH FOCUS ON MOBILE DEVICES)

09:15 **Electronic evidence and computer forensics in criminal cases: an introduction**
Stephen Mason

09:45 **How legal practitioners (prosecutors, defence lawyers and judges) deal with electronic evidence in criminal proceedings: an overview with sample cases where mobile devices are involved**
Stephen Mason

10:30 Discussion

11:00 Break

Chair: Stephen Mason

11:30 **The challenges of dealing with electronic evidence on mobile devices**
- Handling mobile devices as sources of evidence
- Common procedures for handling evidence on mobile devices
- Legal issues related to the collection of traffic/subscriber data and its admissibility in court

Tõnu Mets

12:45 Discussion and lunch (13:00)

SESSION II – COLLECTION, EVALUATION AND ADMISSIBILITY OF ELECTRONIC EVIDENCE ON MOBILE DEVICES

Chair: Laviero Buono

14:00 **Investigating and gathering evidence against hidden web / darkweb services: alternatives and options**
Lodewijk van Zwieten

14:45 **Electronic evidence on mobile phone devices and the Cloud**
- Handling mobile devices as sources of evidence
- Forensic preservation of mobile devices
- Investigative reconstruction using mobile devices
- Electronic evidence and cloud computing in the light of the CJEU *Safe Harbour* ruling

Damir Kahvedžić

15:30 Discussion

15:45 Break

SESSION III – WORKSHOP

Chair: Laviero Buono

16:15 **Demo session to introduce participants to the supporting tools for online investigation/research**
The demos will make participants aware of the sources of evidence available to them in online investigations. The exercise will improve their ability to work with the current Internet technologies
Abraham Pasamar

17:15 Discussion

17:30 End of the first day

20:00 Dinner

Wednesday, 24 May 2017

SESSION IV – COMPUTER FORENSICS, MOBILE DEVICES AND ELECTRONIC EVIDENCE: TECHNICAL AND LEGAL ISSUES

Chair: Stephen Mason

09:00 **Handling electronic evidence on mobile devices in courts**
- What value do Internet Protocol addresses and other identifiers on mobile devices have in court?
- Deleted data on mobile devices and the attribution of forensic artefacts to an offender
- Evidence value of Voice over Internet Protocol (VoIP) in court

Hein Dries-Ziekenheiner

09:45 **Sextortion and ransomware: the threat is going mobile…**
Cormac Callanan

10:30 Discussion

11:00 Break

Chair: Laviero Buono

11:30 **Handling electronic evidence on mobile devices in courts – legal considerations**
Tais Deus Ramos

12:15 Discussion

12:30 End of conference and lunch

Programme may be subject to amendment.
For programme updates: **www.era.int**

The text of this presentation is © Stephen Mason, 2017

Co-funded by the Justice Programme of the European Union 2014-2020

ELECTRONIC EVIDENCE AND COMPUTER FORENSICS IN CRIMINAL CASES: AN INTRODUCTION

Stephen Mason, Barrister

The life-cycle of e-evidence

L'Accademia di Diritto Europeo – Academy of European Law – Europäische Rechtsakademie – l'Académie de droit européee

Madrid, 23-24 May 2017

Centro de Estudios Jurídicos

Outline

- Electronic evidence generally
  - What it is
  - The categories of electronic evidence
- Forensics

Electronic evidence generally

We have arrived

When did it begin?

Arguably by the 1960s for many people, even if they were not aware

Where are we now?

> ‘Stephen, you don’t understand. We live in the age of the machine now.’ Doreen in 2011 (then aged 84)

The problem is that some judges, lawyers and legal academics do not understand that:

- The basis for understanding evidence has shifted permanently
- Their old knowledge is not adequate for dealing with evidence in digital form

Is this correct? Am I wrong in 2017?

The need for a conceptual change

We know about the information revolution: we know that most documents only exist digitally

But electronic evidence has very different characteristics to paper

The normal rules of evidence that have developed with respect to the authentication of (mainly) paper evidence are being applied to electronic evidence

The rules established for paper no longer apply

With its unique characteristics, complex questions about the integrity and security of electronic evidence are raised which must be examined when considering how to authenticate electronic evidence

The concept of original?

For a discussion, see:

"Electronic evidence and the meaning of 'original'", *Amicus Curiae* The Journal of the Society for Advanced Legal Studies, Issue 79, Autumn 2009, 26 – 28

Available as a free download from: http://sas-space.sas.ac.uk/2565/

All digital data is a copy of a copy of a copy …..

What we need to think about is 'first-in-time' evidence

The importance of understanding logic: software code as the witness

The categories – 1

The records of activities that contain content written by one or more people

e.g.: e-mail messages; word processing files; instant messages

As evidence:

It may be necessary to demonstrate that the *content* of the document is a *reliable record* of the human statement that can be trusted

The categories – 2

Records generated by software code that have not had any direct input from a human

e.g.: data logs; connections made by telephones; ATM transactions

As evidence:

To demonstrate that the computer program that generated the record was *functioning consistently* at the material time

What about VW and the software deliberately written to deceive?!

What about all of the links in the chain?

The categories – 3

Records comprising a mix of human input and calculations generated and stored by software code written by a human

e.g.: financial spreadsheet that contains human statements (input to the spreadsheet program); computer processing (mathematical calculations performed by the spreadsheet program)

As evidence:

The first question:

Did the person inputting the data create the record? or

Did the writer of the software code create the content of the record?

Put another way:

How much of the content was created by the writer of the software code, and how much by the person inputting the data?

Forensics: some issues

Qualifications of practitioner

Continuity of evidence (also called chain of evidence)

Tools

Evidence from other jurisdictions

Some articles (all available on the internet):

Rick Ayers, Sam Brothers and Wayne Jansen, Guidelines on Mobile Device Forensics (NIST Special Publication 800-101, Revision 1, May 2014)

Daniel B. Garrie and J. David Morrissy, 'Digital Forensic Evidence in the Courtroom: Understanding Content and Quality', 12 *Northwestern Journal of Technology and Intellectual Property* (2014), 121 – 128

Gary Kessler, 'Are mobile device examinations practiced like 'forensics'?' 12 *Digital Evidence and Electronic Signature Law Review* (2015), 3 – 9

R. P. Coutts and H. Selby, 'Problems with cell phone evidence tendered to 'prove' the location of a person at a point in time', 13 *Digital Evidence and Electronic Signature Law Review* (2016) 76 – 87

http://stephenmason.co.uk
http://ials.sas.ac.uk/about/about-us/people/stephen-mason

Free journal

Digital Evidence and Electronic Signature Law Review

http://journals.sas.ac.uk/deeslr

Draft Convention on Electronic Evidence

http://journals.sas.ac.uk/deeslr/issue/view/336/showToc

Free books

Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017)

http://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-evidence

Stephen Mason, *Electronic Signatures in Law* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016)

http://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-signatures

International Electronic Evidence (British Institute of International and Comparative Law, 2008)

https://www.biicl.org/international-electronic-evidence

The text of this presentation is © Stephen Mason, 2017

Co-funded by the Justice Programme of the European Union 2014-2020

DEALING WITH ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS: AN OVERVIEW

Stephen Mason, Barrister

The life-cycle of e-evidence

L'Accademia di Diritto Europeo – Academy of European Law – Europäische Rechtsakademie – l'Académie de droit européee

Madrid, 23-24 May 2017

Centro de Estudios Jurídicos

What can be found

Multimedia messages; voicemails; documents; spreadsheets; calendar entries; recorded audio and video; Wi-Fi; Bluetooth connection information; GPS data; Text messages; e-mails; photographs

History of:

- Internet searches and general use of device
- Calls made and received

Identify IP addresses

Possible location

Attribution exercise if a telephone is not registered to a specific user

The range of issues

Seizure

Investigation

Data available

Right to silence

Encryption

Authenticity

Proof of intent

Presentation of evidence in court

The tools used: a judicial response

Bevan v The State of Western Australia [2010] WASCA 101

An investigating police officer carried out two separate downloading operations using two separate tools: Cellebrite and XRY

At the beginning of the trial, counsel for the accused objected to the text messages being received into evidence

The trial judge held that the text messages were admissible

Questions were raised as to the reliability of the software and of the officer's correct use of it

First Court of Appeal

The Court of Appeal concluded that the trial judge erred in law in admitting the text messages into evidence

This was because the officer did not explain the process of how he downloaded it in any detail at trial

It was the first time he had used the software, and he did not have any formal training in its use

Blaxell J said that

> ‘when evidence from a new type of scientific instrument or process is adduced for the first time, there must be proof of its reliability and accuracy’

Re-trial

Bevan v The State of Western Australia [2012] WASCA 153

A new trial

Same argument

Counsel for the appellant accepted that the witness was qualified to operate the equipment used to perform the download

But he was not qualified to give evidence about the accuracy of the download material and the reliability of the material itself

The evidence was admitted by the trial judge

Second Court of Appeal

Two out of three judges agreed that the trial judge was right to admit the text messages into evidence

Detective Tomlinson was qualified as an expert

Therefore he could testify about the machines and the software

He was an expert, therefore his opinion was important, and he considered

- the process to be accurate, and
- because he had performed such actions previously, therefore
- the actions were properly performed

It was not relevant that the user of the program will not know whether it is giving inaccurate results

There was no requirement for the Detective to understand how the software worked, or whether there were any problems with the software

England and Wales: *R v Hallam* [2012] EWCA Crim 1158

Mr Hallam's conviction for 3 offences of murder, conspiracy to commit grievous bodily harm and violent disorder was quashed

One of the grounds of appeal was that Mr Hallam was in possession of two mobile telephones, one of which was a 3G telephone

The police seized both telephones, neither was the subject of forensic analysis

The defence did not have the telephones analysed

It was subsequently established that evidence stored on the 3G telephone that suggested that both Mr Hallam's alibi was probably correct

This meant that the memory of both Mr Hallam and his alibi witness were at fault as to the date they were together

Observations by Hallett LJ, delivering the judgment of the court

67. One reason proffered for the failure to examine the phone was that in 2004 the Metropolitan Police did not have the technology in-house to examine 3G telephones. *However, given our limited knowledge, we would have thought that even a cursory check might have produced some interesting results*.

Naiveté?

See *Electronic Evidence* (4th edition) 2.16

http://stephenmason.co.uk
http://ials.sas.ac.uk/about/about-us/people/stephen-mason

Free journal

Digital Evidence and Electronic Signature Law Review

http://journals.sas.ac.uk/deeslr

Draft Convention on Electronic Evidence

http://journals.sas.ac.uk/deeslr/issue/view/336/showToc

Free books

Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017)

http://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-evidence

Stephen Mason, *Electronic Signatures in Law* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016)

http://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-signatures

International Electronic Evidence (British Institute of International and Comparative Law, 2008)

https://www.biicl.org/international-electronic-evidence

The challenges of dealing with electronic evidence on mobile devices

TÕNU METS

23.05.2017

Co-funded by the Justice Programme of the European Union 2014-2020

Handling mobile devices as sources of evidence

Electronic evidence is considered to be equivalent to traditional evidence.

– The Admissibility of Electronic Evidence in Court in Europe, 2007

All countries in Africa and one-third of countries in other regions report insufficient resources for prosecutors to handle and analyse electronic evidence. […] Very few countries reported the existence of special evidentiary laws governing electronic evidence. […] The greater number of countries that admit electronic evidence reported that it is treated in the same way as physical evidence. […] Admissibility of electronic evidence was also reported to be dependent on the general rules that apply to all evidence.

– Comprehensive Study on Cybercrime, United Nations Office of Drugs and Crime, 2013

Most member states do not have a legal distinction between physical and electronic evidence. Applying traditional evidence rules to electronic evidence may not be sufficient. A distinction between physical and electronic evidence in legal provisions is recommended or where reasonable, the legal provisions should explicitly state that they apply to both physical and electronic evidence. […] Data retention periods vary across jurisdictions and harmonized legislation is necessary.

– EVIDENCE: European Informatics Data Exchange Framework for Courts and Evidence, 2016

Criteria of Admissibility

Relevancy
Usefulness
Believability
Completeness
Authenticity
Reliability
Legitimacy
Proportionality

Common procedures for handling evidence on mobile devices

- ACPO Good Practice Guide for Digital Evidence
- ACPO Good Practice Guide for Computer-Based Electronic Evidence
- SWGDE Best Practices for Computer Forensics
- SWGDE Best Practices for Mobile Device Forensics
- ENISA Electronic evidence – Basic Guide for First Responders
- Guidelines on Digital Forensic Procedures for OLAF Staff
- ENFSI Best Practice Manual for the Forensic Examination of Digital Technology
- …

1. Upon seizing digital evidence, **actions taken should not change that evidence**.

2. When it is necessary for a person to access original digital evidence, that person must be **forensically competent**.

3. All activity relating to the seizure, access, storage, or transfer of digital evidence must be **fully documented, preserved, and available for review**.

4. An individual is **responsible** for all actions taken with respect to digital evidence while the digital evidence is in their possession.

5. Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is **responsible for compliance** with these principles.

– International Organization on Computer Evidence, International Hi-Tech Crime and Forensics Conference in October 1999

1. **No action taken by law enforcement agencies or their agents should change data held** on a computer or storage media which may subsequently be relied upon in court.

2. In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be **competent** to do so and be able to **give evidence explaining the relevance and the implications of their actions**.

3. An **audit trail** or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and **achieve the same result**.

4. The person in charge of the investigation (the case officer) has overall **responsibility for ensuring that the law and these principles are adhered to**.

– ACPO Principles of Digital Evidence

Traffic data and subscriber information

Traffic data means any computer or other **data relating to a communication** by means of a computer program, computer, computer system, or network, generated by a computer program, computer, computer system, or network that formed a part in the chain of communication, indicating the communication's origin, destination, route, format, intent, time, date, size, duration, or type of underlying service.

– International Telecommunication Union, Toolkit for Cybercrime Legislation

See also: Convention on Cybercrime, Article 1(b)

Subscriber information means any information contained in the form of computer data or any other form that is **held by a service provider**, relating to subscribers of its services, other than traffic data or content data, and **by which can be established**: (i) the type of communication service used, the technical provisions taken thereto, and the period of service; (ii) the **subscriber's identity**, postal or geographic address, telephone and other access number, billing and payment information, as it is available on the basis of the service agreement or arrangement; and/or (iii) any information regarding the location of installed communications equipment as disclosed in the service agreement or arrangement.

– International Telecommunication Union, Toolkit for Cybercrime Legislation

See also: Convention on Cybercrime, Article 18(3)(a)-(c)

Charter of Fundamental Rights of the European Union

Article 7:
Everyone has the right to respect for his or her private and family life, home and **communications**.

Article 8(1):
Everyone has the **right to the protection of personal data** concerning him or her.

Article 11(1):
Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to **receive and impart information and ideas without interference by public authority** and regardless of frontiers.

Charter of Fundamental Rights article 52(1):

Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and **respect the essence of those rights and freedoms**. Subject to the **principle of proportionality**, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

Data Protection Directive

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

– OJ L 281, 23.11.1995, p. 31

Directive 95/46/EC article 2(a):

‘Personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Directive 95/46/EC article 2(b):

‘Processing of personal data' shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage , adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Directive 95/46/EC article 13(1):

Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for [...] when such a restriction constitutes a necessary measures to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions.

[…]

Directive on Privacy and Electronic Communications (ePrivacy Directive)

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

– OJ L 201, 31.07.2002, p. 37

Directive 2002/58/EC article 5(1):

Member States shall **ensure the confidentiality of communications and the related traffic data** by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall **prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data** by persons other than users, without the consent of the users concerned, **except when legally authorised to do so in accordance with Article 15(1)**.

Directive 2002/58/EC article 15(1):

Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5 […] of this Directive when such restriction constitutes a **necessary, appropriate and proportionate** measure within a democratic society to **safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences** […] To this end, Member States may, inter alia, adopt legislative measures providing for the **retention of data for a limited period justified on the grounds laid down in this paragraph.** All the measures referred to in this paragraph shall be in accordance with the general principles of Community law.

Data Retention Directive (declared invalid by Court of Justice)

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC – OJ L 105, 13.04.2006, p. 54

- Was applied to **traffic and location data** on both legal entities and natural persons and also to the related **data necessary to identify the subscriber or registered user**
- Data to be retained included data necessary to trace and identify the **source of a communication**, identify the **destination of a communication**, the **date, time and duration of a communication**, the **type of communication**, users' **communication equipment** or what purports to be their equipment, the **location of mobile communication equipment**
- Retention period 6 months to 2 years

Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others

Data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them (para. 27).

The fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the **feeling that their private lives are the subject of constant surveillance** (para. 37).

The retention of data for the purpose of possible access to them by the competent national authorities **directly and specifically affects private life** and, consequently, the rights guaranteed by Article 7 of the Charter. Furthermore, such a retention of data also falls under Article 8 of the Charter because **it constitutes the processing of personal data** within the meaning of that article and, therefore, necessarily **has to satisfy the data protection requirements** arising from that article (para. 29).

Retaining data relating to a person's private life and to his communications and the access of the competent national authorities to the data constitute an **interference with the rights guaranteed by Article 7 of the Charter**. Likewise, it constitutes an **interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter** because it provides for the processing of personal data (para. 34–36).

Interference caused with the fundamental rights laid down in Articles 7 and 8 of the Charter is wide-ranging, and it **must be considered to be particularly serious** (para. 37).

The directive requires the retention of all traffic data concerning fixed telephony, **mobile telephony, Internet access, Internet e-mail and Internet telephony**. It therefore **applies to all means of electronic communication**, the use of which is very widespread and of growing importance in people's everyday lives. Furthermore, the directive covers all subscribers and registered users. It therefore **entails an interference with the fundamental rights of practically the entire European population** (para. 56).

EU legislation in question must lay down **clear and precise rules governing the scope and application of the measure in question** and imposing **minimum safeguards** so that the persons whose data has been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data. The **need for such safeguards is all the greater where personal data is subjected to automatic processing** and where there is a significant risk of unlawful access to those data (para. 54–55).

Main Problems with Data Retention in Directive 2006/24/EC

1. The wide scope of personal data retention and the lack of differentiation, limitations and exceptions (see para. 56–59).
2. The lack of objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use (see para. 60–62).
3. The lack of distinction between the categories of data and lack of objective criteria to determine data retention period (see para. 63–64).
4. The lack of sufficient safeguards to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. Obligation on Member States to establish such rules had not been laid down (see para. 66).

Decision

- By requiring the retention of data and by allowing national authorities to access data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data
- By adopting the Data Retention Directive, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality
- Court of Justice declared the Data Retention Directive to be invalid

Aftermath of Digital Rights Ireland

The decision of whether or not to introduce national data retention laws is a **national decision**. Commission is not coming forward with any new initiatives on Data Retention. In the absence of EU rules, Member States are free to maintain their current data retention systems or set up new ones, providing of course they comply with basic principles under EU law, such as those contained in the ePrivacy Directive.

– European Commission statement on national data retention laws, 16.09.2015, STATEMENT/15/5654

Joined Cases C-203/15 Tele2 Sverige AB v Post-och telestyrelsen and C-698/15 Secretary of State for the Home Department v Tom Watson and Others

Data provides the means of **establishing a profile** of the individuals concerned, **information that is no less sensitive**, having regard to the right to privacy, **than the actual content of communications** (para. 99).

The importance both of **the right to privacy**, guaranteed in Article 7 of the Charter, and of **the right to protection of personal data**, guaranteed in Article 8 of the Charter, must be taken into consideration in interpreting Article 15(1) of Directive 2002/58. The same is true of **the right to freedom of expression** in the light of the particular importance accorded to that freedom in any democratic society (para. 93).

The retention of traffic and location data could have an effect on the use of means of electronic communication and, consequently, on the exercise by the users thereof of their freedom of expression, guaranteed in Article 11 of the Charter (para. 101).

Given the **seriousness of the interference in the fundamental** rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data, **only the objective of fighting serious crime is capable of justifying such a measure**. While the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, **cannot in itself justify** that national legislation **providing for the general and indiscriminate retention of all traffic and location data** should be considered to be necessary for the purposes of that fight (para. 102–103).

National legislation which covers, in a generalised manner, all subscribers and registered users and all means of electronic communication as well as all traffic data, provides for no differentiation, limitation or exception according to the objective pursued. It is comprehensive in that it **affects all persons using electronic communication services**, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences. Further, it **does not provide for any exception**, and consequently it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy (para. 105).

Such legislation does not require there to be any **relationship between the data which must be retained and a threat to public security**. In particular, it is not restricted to retention in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime (para. 106).

National legislation such as that therefore **exceeds the limits of what is strictly necessary** and **cannot be considered to be justified**, within a democratic society (para. 107).

Requirements for National Legislation

1. The retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is **strictly necessary** (see para. 108).
2. Clear and precise rules governing the scope and application of such a data retention measure and **minimum safeguards**, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, **indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted**, thereby ensuring that such a measure is limited to what is strictly necessary (see para. 109).

3. Retention of data must continue to meet **objective criteria, that establish a connection between the data to be retained and the objective pursued**. In particular, such conditions must be shown to be such as actually to **circumscribe, in practice, the extent of that measure** and, thus, the public affected (see para. 110).
4. National legislation must be based on objective evidence which makes it possible to **identify a public whose data is likely to reveal a link**, at least an indirect one, **with serious criminal offences**, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security. Such limits may be set by using a **geographical criterion** where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences (see para. 111).

5. National legislation must be based on objective criteria in order to **define the circumstances and conditions under which the competent national authorities are to be granted access to the data of subscribers or registered users**. In that regard, access can, as a general rule, be granted, in relation to the **objective of fighting crime**, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime. In particular situations, where for example **vital national security, defence or public security interests are threatened by terrorist activities**, **access to the data of other persons might also be granted** where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities (see para. 119).

6. Access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be **subject to a prior review carried out either by a court or by an independent administrative body** (see para. 120).

Decision

Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as **precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication**

and

must be interpreted as **precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union**.

IT LAW

UNIVERSITY OF TARTU

itlaw.ut.ee

Thank you for your time!

tonu.mets@ut.ee

Investigating and Gathering Evidence of Darknet Services

Lodewijk van Zwieten
Cybercrime Expert @ Eurojust

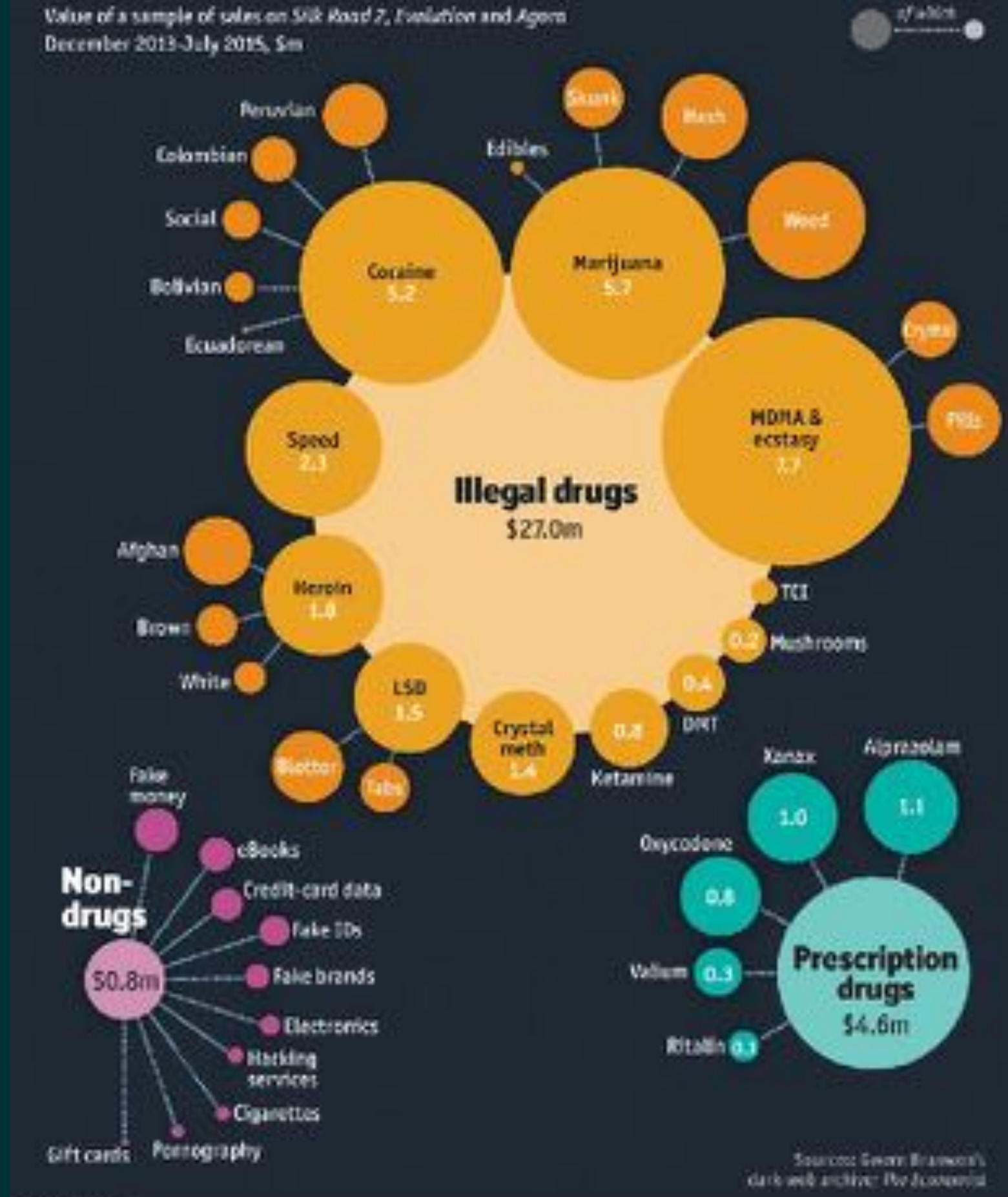
Co-funded by the Justice Programme of the European Union 2014-2020

Island
Bifurcation
Ridge ending
Short Break

For the
Internet
is Large
and
full of
Terrors.

The dark web

Value of a sample of sales on Silk Road 2, Evolution and Agora
December 2013-July 2015, $m



Sources: Gwern Branwen's dark web archive; The Economist

Counterfeit 50 euro banknote

This listing is for a fake €50,- banknote. The note is printed on cotton paper and contains a hologram. There is no watermark and security line on this note but the printing and color is fine. The feel is also good. The quality is good enough to pass it in clubs, at drug dealers, prostitutes or for example when ordering a pizza. It is not necessary but recommended to spray the bills with...

Sold by PatrickDeWild · 0 sold since Apr 10, 2016 Vendor Level 1 Trust Level 4

	Features		Features
Product class	Physical package	**Origin country**	Netherlands
Quantity left	8 items	**Ships to**	Europe, Netherlands
Ends in	Never	**Payment**	Escrow

Domestic (The Netherlands) - 3 days - USD +1.13 / item

Purchase price: USD 14.25

Qty: 1 Buy Now Queue

Interordnance R94 7,62x39 FULL ESCROW

For sale is an Interordnance R94 Straight-Pull-Repeator, which has been made in Austria by Interordnance. It's a 7,62x39mm caliber and operatd by a simple straight-pull and safety lock. It comes with 2 magazines and 40 Rounds of FMJ Ammo. It is in good condition as you can see for yourself in the pictures. better quality Images http://www0.xup.in/exec/ximg.php?fid=20577835 http://www0.xu...

Sold by daschek1337 - *0* sold since *Oct 5, 2015* **Level 1**

	Features		Features
Product class	Physical package	**Origin country**	Austria
Quantity left	1 items	**Ships to**	Europe
Ends in	Never	**Payment**	Escrow

EU - 10 days - USD +48.46 / item

Purchase price: USD 1,998.52

Qty: 1 Buy Now Queue

5.8038 BTC

BlackMarket Reloaded

http://bmrxwjaua7...onion/

Deposit Address:

Account Balance: 0.00000 BTC

Pending: 0.00000 BTC

Home | Your Account | Your Purchases | Forum | Logout | Help

Categories

- Drugs (2814)
- Services (1177)
- Data (678)
- Weapons (348)
- Collectibles (29)
- Metals/Stones (19)
- Other (244)
- Software (146)
- Movies (32)
- Tobacco (165)
- Counterfeits (82)
- Alcohol (16)
- eBooks (771)

Exchange

- Exchange

User Menu

- Home
- Inbox (0/0)
- Account
- Purchases
- Favorites
- Deposit Addresses
- Forums

There's no account admin or similar here, if anyone other than backspy (user id 1) addresses you by PM **that person has nothing to do with BMR** and is most likely just a scammer trying to impersonate the BMR staff!

Search: [ ] in [All Categories] [Search]

Drugs > Cannabis > Weed

1/2oz. Cosmic OG[FREE 1/4oz. of Indoor Shake Included]

Seller: CaliBoi[0] 2.89261 BTC

Alcohol > Wine

(RARE BAROLO 1964 COLLECTOR'S WINE

Seller: fake-BM

2.47974 BTC

Services > Hacking

(5%/1%/100DB SEARCH: GUARANTEED G4 CCS

Seller: dancoffin[0] 0.19071 BTC

Drugs > Ecstasy

1 kpl 200 mg Party Flocker E950

Seller: Profpa [64]

0.34710 BTC

Drugs > Cannabis > Seeds

(5) LibertSeeds [B.O.G. Seeds]

Seller: Tonash [24]

0.42214 BTC

Drugs > Psychedelics > Others

2C-B 200mg

Seller: nullbarbiton [87]

0.64349 BTC

Drugs > Stimulants > Speed

28.5g Speed / Amphetamine paste (1 Ounce)

Seller: Bungalo [20] 0.33583 BTC

eBooks > Drugs

The Joint Rolling Handbook

Seller: rapperpoint [0]

0.00938 BTC

Drugs > Ecstasy

(**)Green Dutch MDMA Crystals 82%+ Proven

Seller: QuikDrug [43]

0.21978 BTC

Data > Digital Goods

[ebook] Dynamite Hentalkan by George Anderson

Seller: [redacted] 0.07814 BTC

Services > Documents

[Document] Ohio (OH-USA) Driving License PSD File

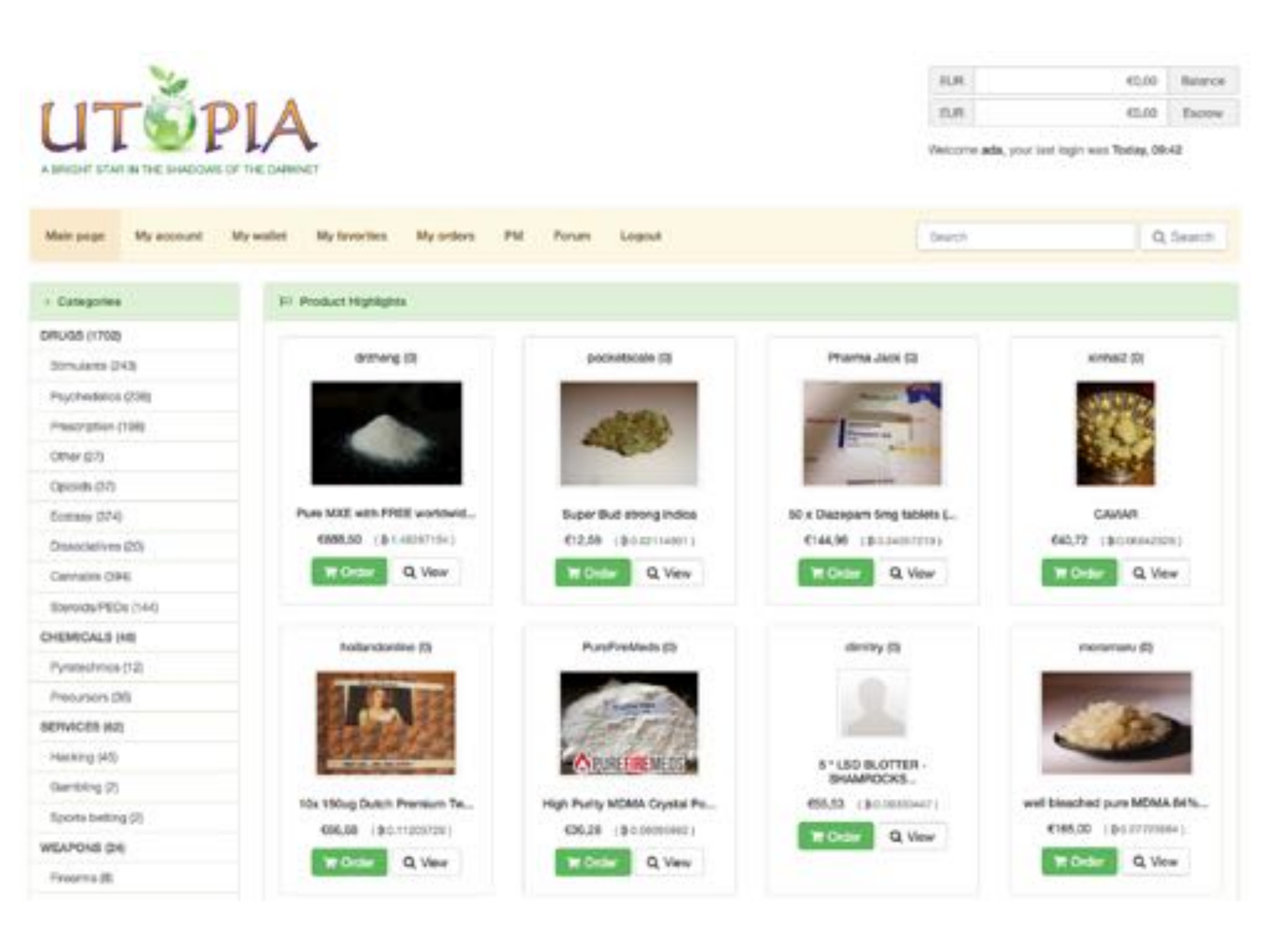
Seller: [redacted] 0.65000 BTC

Services > Money

(5 EU CC No.1

Seller: fav-deals [74]

3.20000 BTC


UTOPIA
A BRIGHT STAR IN THE SHADOWS OF THE DARKNET
EUR €0,00 Balance
EUR €0,00 Escrow
Welcome ada, your last login was Today, 09:42
Main page
My account
My wallet
My favorites
My orders
PM
Forum
Logout
Search
Categories
DRUGS (1702)
Stimulants (243)
Psychedelics (238)
Prescription (198)
Other (27)
Opioids (37)
Ecstasy (374)
Dissociatives (20)
Cannabis (394)
Steroids/PEDs (144)
CHEMICALS (48)
Pyrotechnics (12)
Precursors (36)
SERVICES (62)
Hacking (45)
Gambling (2)
Sports betting (2)
WEAPONS (24)
Firearms (8)
Product Highlights
dritheng (0)
Pure MXE with FREE worldwid...
€888,50
Order
View
pocketscale (0)
Super Bud strong indica
€12,59
Order
View
Pharma Jack (0)
50 x Diazepam 5mg tablets (...
€144,96
Order
View
xinhai2 (0)
CAVIAR
€40,72
Order
View
hollandonline (0)
10x 150ug Dutch Premium Tw...
€66,68
Order
View
PureFireMeds (0)
High Purity MDMA Crystal Po...
€36,28
Order
View
dimitry (0)
5 * LSD BLOTTER - SHAMROCKS...
€55,53
Order
View
moramaru (0)
well bleached pure MDMA 84%...
€165,00
Order
View

Silk Road

anonymous market

messages 0 | orders 0 | account B0.00

Search [ ] Go

Shop by Category

- Drugs 11,406
  - Cannabis 2,590
  - Dissociatives 222
  - Ecstasy 1,122
  - Opioids 600
  - Other 554
  - Precursors 112
  - Prescription 2,623
  - Psychedelics 1,417
  - Stimulants 1,594
- Apparel 451
- Art 4
- Biotic materials 3
- Books 980
- Collectibles 13
- Computer equipment 48
- Custom Orders 91
- Digital goods 706
- Drug paraphernalia 375
- Electronics 129
- Erotica 653
- Fireworks 10
- Food 10
- Forgeries 123
- Hardware 33
- Herbs & Supplements 14
- Home & Garden 17
- Jewelry 106
- Lab Supplies 53
- Lotteries & games 54
- Medical 41
- Money 165
- Musical instruments 3
- Packaging 78
- Services 163

Tramado 100MG - 30 tabs

B0.17

Sustanon 250 10ml

B0.95

5g Good cuality "Ali baba's Hash" from Chaouen

B0.41

Double Platinum Blunt Wraps - Peach

B0.01

250g Methylone Moonrocks! FREE SHIPPING +

B7.29

Amber Glass Concentrate - 1/2 oz

B1.61

PePe 30grams Rolling Tobacco x 3

B0.16

Weed Butter 1oz (28g)

B0.36

2g MEPHEDRONE HCL!!!

B0.33

1g 2C-E 99,7%

B0.71

1Kg Methylone(Little Cristal)FREE SHIP

B22.36

Trben 150mg/ml 10ml (trenbone mix)

B0.58

U.S. Immigration and Customs Enforcement

THIS HIDDEN SITE HAS BEEN SEIZED

as part of a joint law enforcement operation by
the Federal Bureau of Investigation, ICE Homeland Security Investigations,
and European law enforcement agencies acting through Europol and Eurojust

In accordance with the law of European Union member states
and a protective order obtained by the United States Attorney's Office for the Southern District of New York
In coordination with the U.S. Department of Justice's Computer Crime & Intellectual Property Section
Issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

U.S. Immigration and Customs Enforcement

THIS HIDDEN SITE HAS BEEN SEIZED

as part of a joint law enforcement operation by
the Federal Bureau of Investigation, ICE Homeland Security Investigations,
and European law enforcement agencies acting through Europol and Eurojust

In accordance with the law of European Union member states
and a protective order obtained by the United States Attorney's Office for the Southern District of New York
In coordination with the U.S. Department of Justice's Computer Crime & Intellectual Property Section
Issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

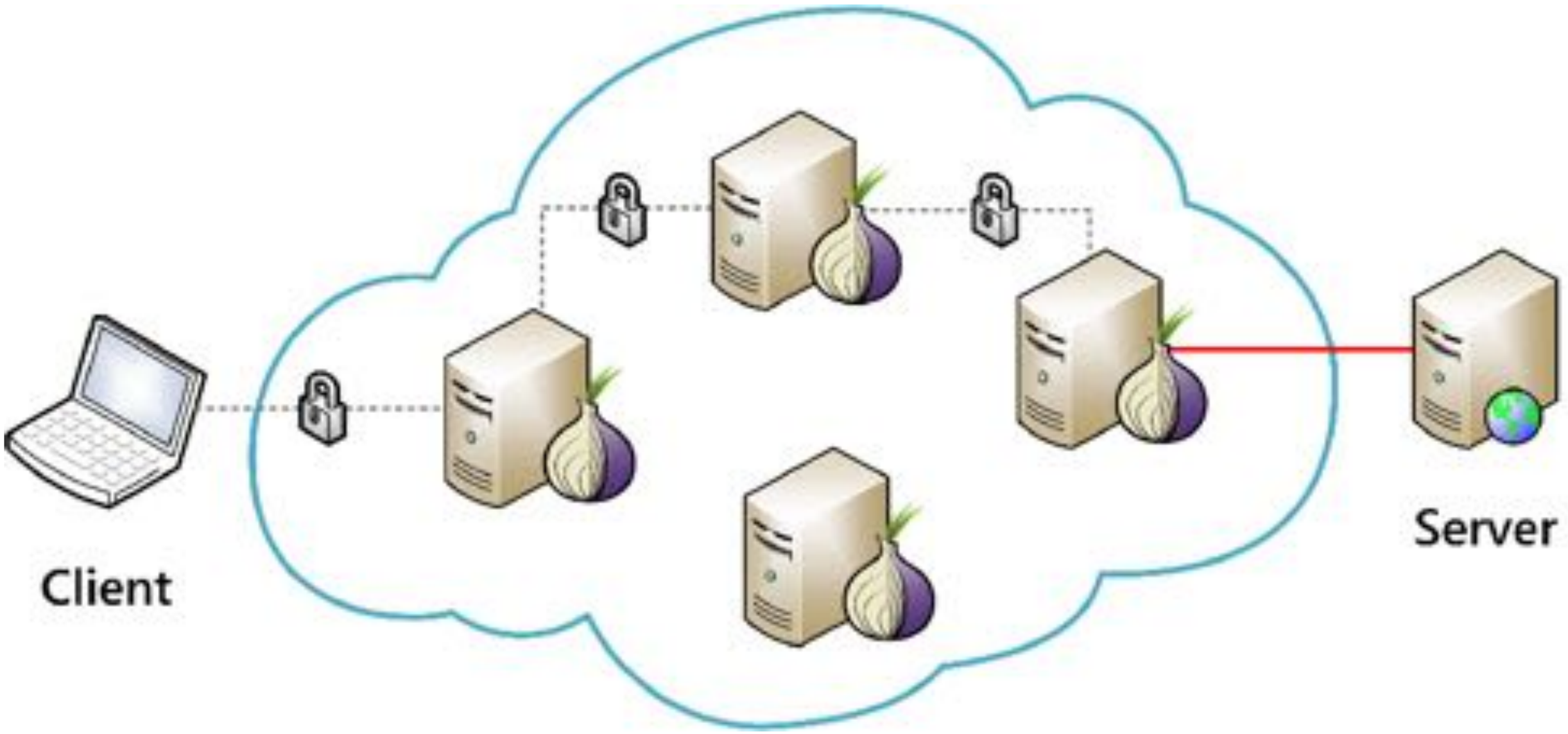
17 arrests of vendors and administrators

more than 410 hidden services taken down

USD 1 million in bitcoins

EUR 180 000 in cash, drugs, gold, and silver seized

Data
loss
Del
Shift


Client
Server

Digital Rights **Ireland**

TELE2

iPhone Apps

Tor Powered Browser &...
Utilities
Get
In-App Purchases

Red Onion - Tor-powered web...
Utilities
€ 2,29

TOR-Powered Onion Web...
Utilities
Get
In-App Purchases

Onion VPN Browser - TOR...
Utilities
Get
In-App Purchases

VPN Browser - Mobile...
Utilities
Get
In-App Purchases

Onion Browser - Secure &...
Utilities
Get

Anonymous Browser for To...
Productivity
Get
In-App Purchases

TOR-Powered Onion Web...
Productivity
Get
In-App Purchases

Red Onion - Tor Browser
Utilities
€ 1,09

Onion Proxy VPN: Be...
Business
Get
In-App Purchases

Onion VPN - Anonymous...
Utilities
Get
In-App Purchases

Anonymous Tor Browser: secur...
Utilities
€ 0,49

Aloha Browser - private browse...
Utilities
Get

TOR Powered Browser & Free...
Utilities
Get
In-App Purchases

Onion - Tor powered...
Utilities
€ 1,09

Network starter - Web browsin...
2 Apps
€ 1,09

Copay

Airbitz

GreenBits

Mycelium

Green Address

Coinomi

Coin.Space

Simple Bitcoin

Bitcoin Wallet

breadwallet

Bither

Bitcoin Knots

mSIGNA

MultiBit HD

Electrum

BitGo

Coinbase

Xapo

Trezor

Ledger Nano

Ledger Nano S

KeepKey

Coinapult

Circle

Copay

Airbitz

GreenBits

Mycelium

Green Address

Coinomi

Coin.Space

Simple Bitcoin

Bitcoin Wallet

breadwallet

Bither

Bitcoin Knots

mSIGNA

MultiBit HD

Electrum

BitGo

Coinbase

Xapo

Trezor

Ledger Nano

Ledger Nano S

KeepKey

Coinapult

Circle

NIET BETREDEN POLITIE

POLIS
POLIS

KEEP
CALM

LITTE

Investigating and Gathering Evidence of Darknet Services

Lodewijk van Zwieten
Cybercrime Expert @ Eurojust

Co-funded by the Justice Programme of the European Union 2014-2020

Electronic evidence on mobile phone devices and the Cloud

Damir Kahvedzic PhD

Copyright © 2017 BSI. All rights reserved

Co-funded by the Justice Programme of the European Union 2014-2020

Introduction

Increased connectivity has resulted in an unprecedented amount of data being sent seamlessly around the world

Privacy and security of this data have become political hot topics

Security and end to end encryption have been discussed

Involves governments, organisations, users and developers

bsi. Copyright © 2017 BSI. All rights reserved

Overview

Where are we technologically?

Where are we in terms of security?

Where are we policy wise?

How has one influenced the other?

How are apps being influenced?

How has it influenced data collection?

bsi. Copyright © 2017 BSI. All rights reserved

Relationships

bsi. Copyright © 2017 BSI. All rights reserved

Manufacturers

bsi. Copyright © 2017 BSI. All rights reserved

Mobile Devices

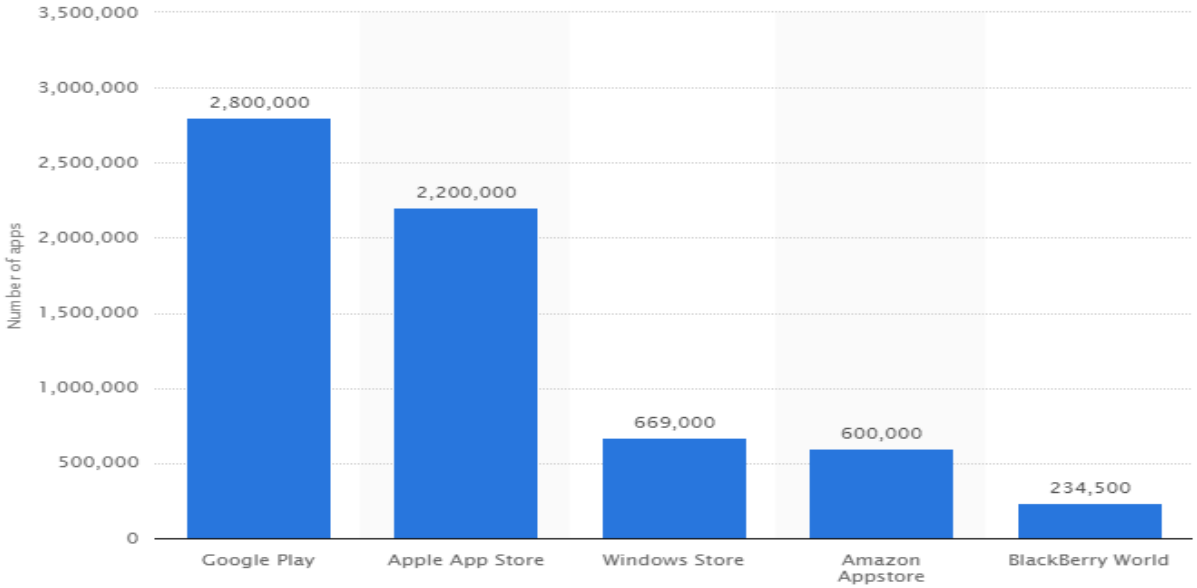
iOS10

Android 7.1
Nougat

bsi. Copyright © 2017 BSI. All rights reserved

iPhone vs the World

1 billion cumulative worldwide iPhone sales up to July 2016



bsi. Copyright © 2017 BSI. All rights reserved

Progression

bsi. Copyright © 2017 BSI. All rights reserved

Where is our Data?

Cloud

Communication

App Marketplace

Operating System

File System

bsi. Copyright © 2017 BSI. All rights reserved

Apple Device OS

iOS

MacOS

WatchOS

bsi. Copyright © 2017 BSI. All rights reserved

Apple Device Filesystem

HFS+

Other devices

- FAT
- exFAT
- NTFS

bsi. Copyright © 2017 BSI. All rights reserved

Apple Device Filesystem

Apple Filesystem (APFS)

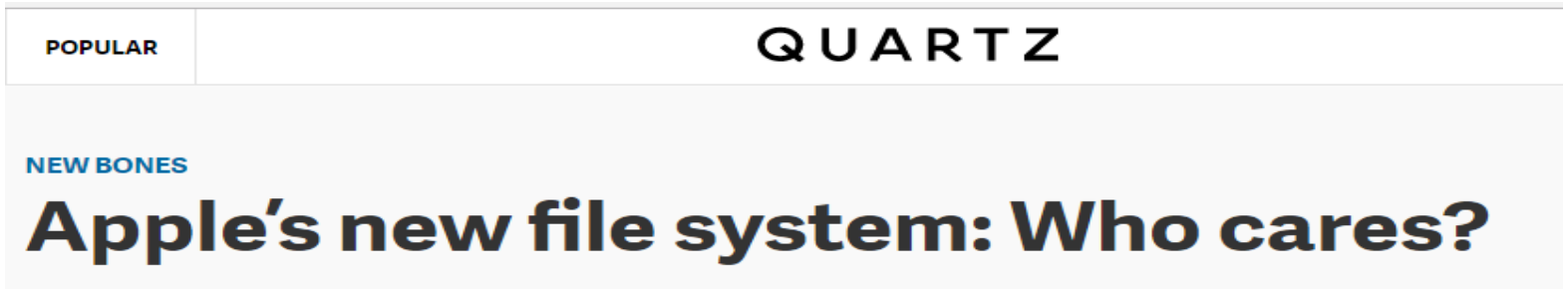
Introduced in iOS 10.3 on iPhones in March 2017

macOS, watchOS, and tvOS will receive it sometimes during 2017

Optimized for flash and solid-state storage

bsi. Copyright © 2017 BSI. All rights reserved

Apple Device Filesystem



bsi. Copyright © 2017 BSI. All rights reserved

Apple Filesystem Encryption

Native support for strong full-disk encryption out of the box

Apple File System supports the following encryption models for each volume in a container:

- No encryption
- Single-key encryption
- Multi-key encryption with per-file keys for file data and a separate key for sensitive metadata

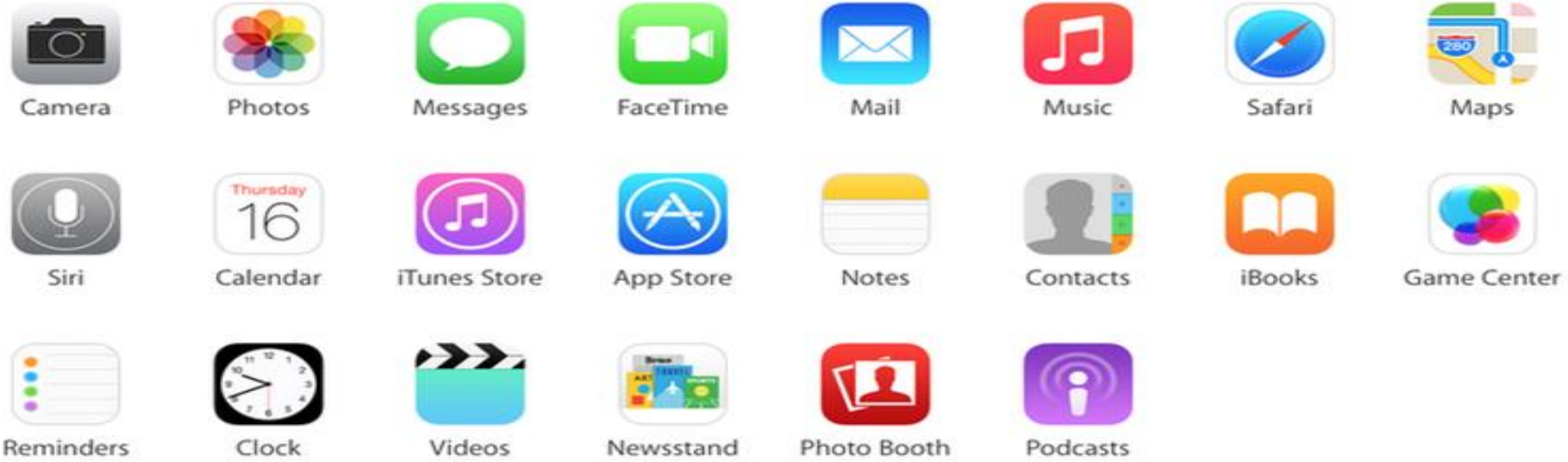
Multi-key encryption ensures the integrity of user data.

Even if someone were to compromise the physical security of the device and gain access to the device key, they still couldn't decrypt the user's files.

Apple File System uses AES-XTS or AES-CBC encryption modes, depending on hardware.

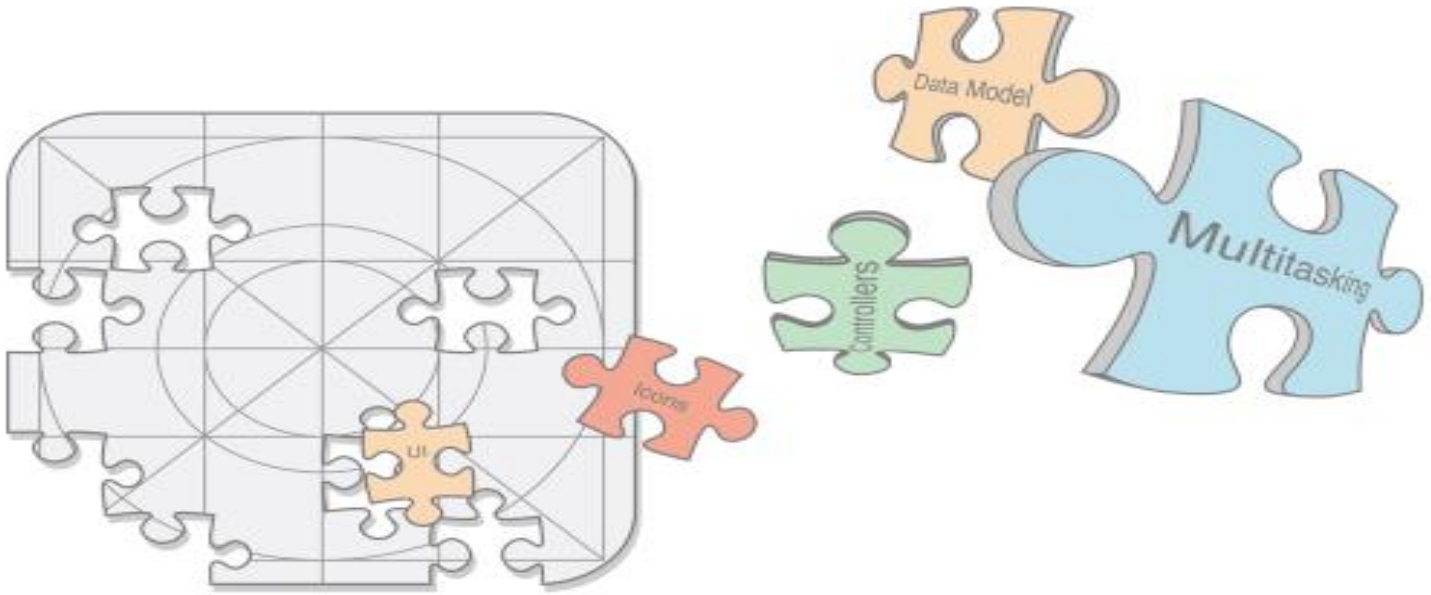
bsi. Copyright © 2017 BSI. All rights reserved

Let’s Dive Deeper



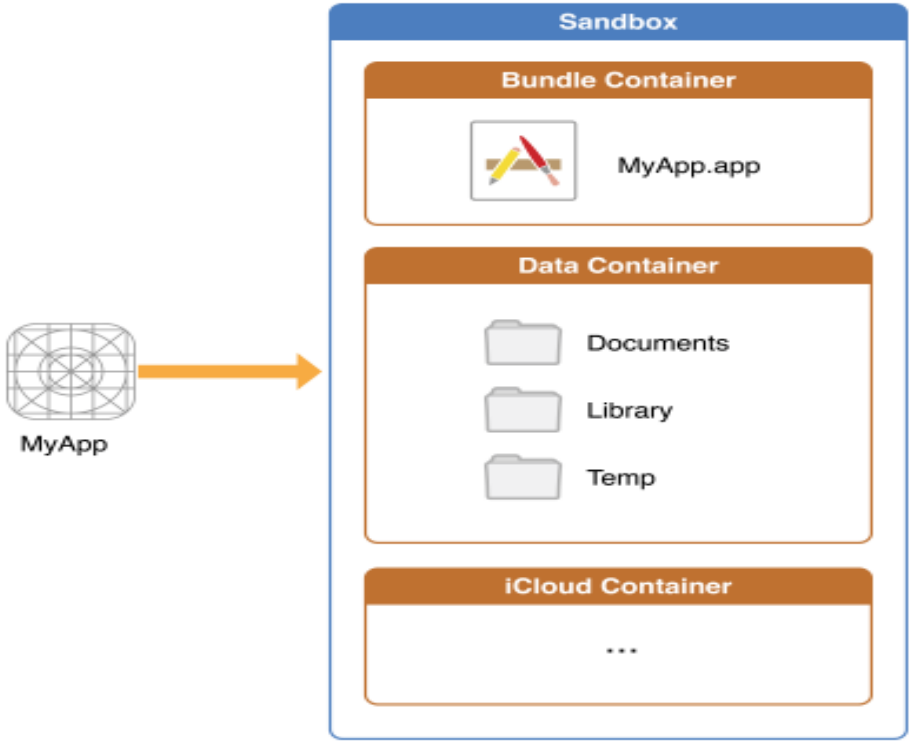
bsi. Copyright © 2017 BSI. All rights reserved

Apple App Marketplace



bsi. Copyright © 2017 BSI. All rights reserved

App Structure



bsi. Copyright © 2017 BSI. All rigl

App Structure

AppName.app

- This is the app's bundle. This directory contains the app and all of its resources.

Documents/

- Use this directory to store user-generated content. The contents of this directory can be made available to the user through file sharing; therefore, his directory should only contain files that you may wish to expose to the users
- The contents of this directory are backed up by iTunes and iCloud.

Documents/Inbox

- Use this directory to access files that your app was asked to open by outside entities. Specifically, the Mail program places email attachments associated with your app in this directory.

Library/

- This is the top-level directory for any files that are not user data files. Use the Library subdirectories for any files you don't want exposed to the user. Your app should not use these directories for user data files.
- The contents of the Library directory are backed up by iTunes and iCloud

tmp/

- Use this directory to write temporary files that do not need to persist between launches of your app. The contents of this directory are not backed up by iTunes or iCloud.

bsi. Copyright © 2017 BSI. All rights reserved

Protecting Data Using Encryption

Data protection uses built-in hardware to store files in an encrypted format on disk and to decrypt them on demand.

While the user's device is locked, protected files are inaccessible, even to the app that created them.

The user must unlock the device (by entering the appropriate passcode) before an app can access one of its protected files.

Data protection is available on most iOS devices and is subject to the following requirements:

- The file system on the user's device must support data protection. Most devices support this behavior.
- The user must have an active passcode lock set for the device.

bsi. Copyright © 2017 BSI. All rights reserved

Protecting Data Using Encryption

No protection—The file is encrypted but is not protected by the passcode and is available when the device is locked.

Complete—The file is encrypted and inaccessible while the device is locked.

Complete unless already open—The file is encrypted. A closed file is inaccessible while the device is locked. After the user unlocks the device, your app can open the file and use it. If the user locks the device while the file is open, though, your app can continue to access it.

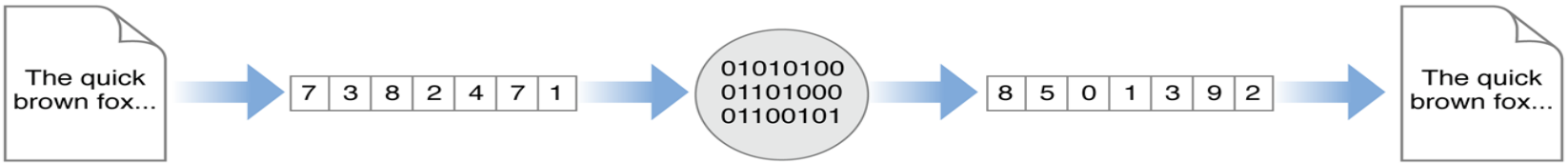
Complete until first login—The file is encrypted and inaccessible until after the device has booted and the user has unlocked it once

bsi. Copyright © 2017 BSI. All rights reserved

App Communication

App Transport Security (ATS) feature starting January 1st, 2017

Requires all app communications to be encrypted



bsi. Copyright © 2017 BSI. All rights reserved

Communication Apps

Threema

WhatsApp

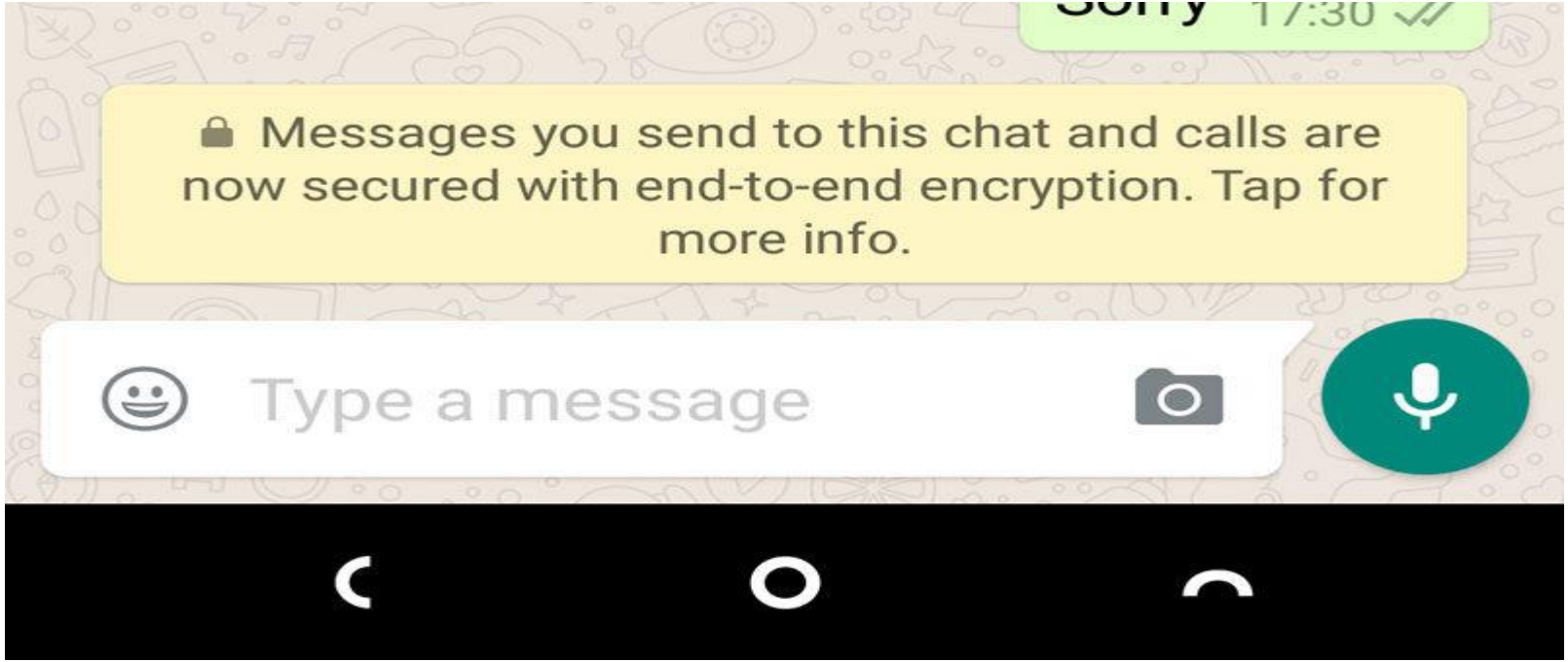
Wickr

Telegram

Signal

bsi. Copyright © 2017 BSI. All rights reserved

WhatsApp



bsi. Copyright © 2017 BSI. All rights reserved

Forensics: How do we get to the data?

To create an exact copy of the data on the device

Create a bit stream copy of all of the files

Types:

- Physical Acquisition
- Logical Acquisition
- SD Card Analysis
- JTAG
- Also just browsing the phone….

bsi. Copyright © 2017 BSI. All rights reserved

Forensic Collections

Collect using forensic applications

Collect from iCloud or other backups

Collect using the apps features

Collect manually

bsi. Copyright © 2017 BSI. All rights reserved

Forensics: Cellebrite

April, 2017

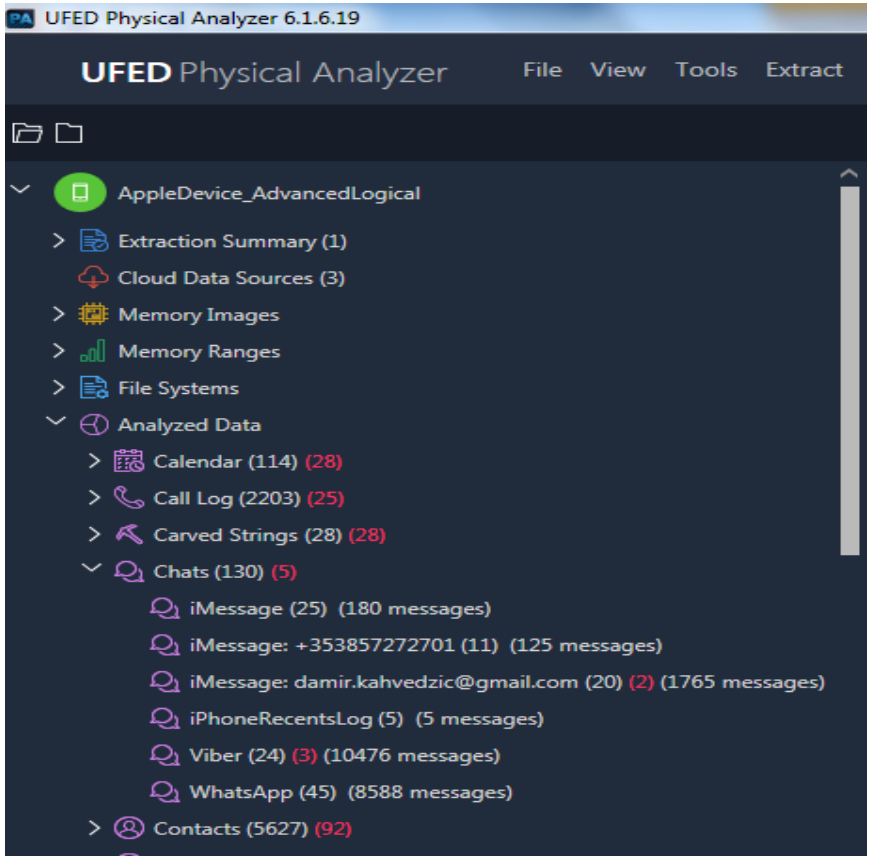
UFED Physical Analyzer, UFED Logical Analyzer and UFED Reader Version 6.1.6

Cellebrite is happy to announce that UFED Physical Analyzer, UFED Logical Analyzer and UFED Reader 6.1.6 are now available.
We have added support for 180 new app versions for iOS and Android devices, including:

- Facebook Messenger version 111.0 (iOS)
- Gmail version 7.2.26.149804060.release (Android)
- Instagram version 10.13.0 (Android), 10.14 (iOS)
- Hangouts version 17.0.148298972 (Android), 14.6.0 (iOS)
- KakaoTalk version 6.1.5 (Android)
- QQ version 7.3.1.3060 (Android), 6.7.1 (iOS)
- Snapchat version 10.4.5.0 (Android), 10.5.0.0 (iOS)
- Threema version 3.11 (Android), 2.9.0 (iOS)
- WeChat version 6.5.6 (iOS)
- WhatsApp version 2.17.107 (Android), version 2.17.11 (iOS)

bsi. Copyright © 2017 BSI. All rights reserved

Forensisc: Cellebrite



bsi. Copyright © 2017 BSI. All rights reserved

Forensics: Oxygen Forensic

Oxygen Forensic® Detective v.9.2.1

We are happy to i

Version 9.2.1 dec
popular secure m
the second metho
commands to ren

Oxygen Forensic® Detective v.9.2.2

We are happy to introc

The new version decry
Private Messenger, Pr
Oxygen Forensic® De

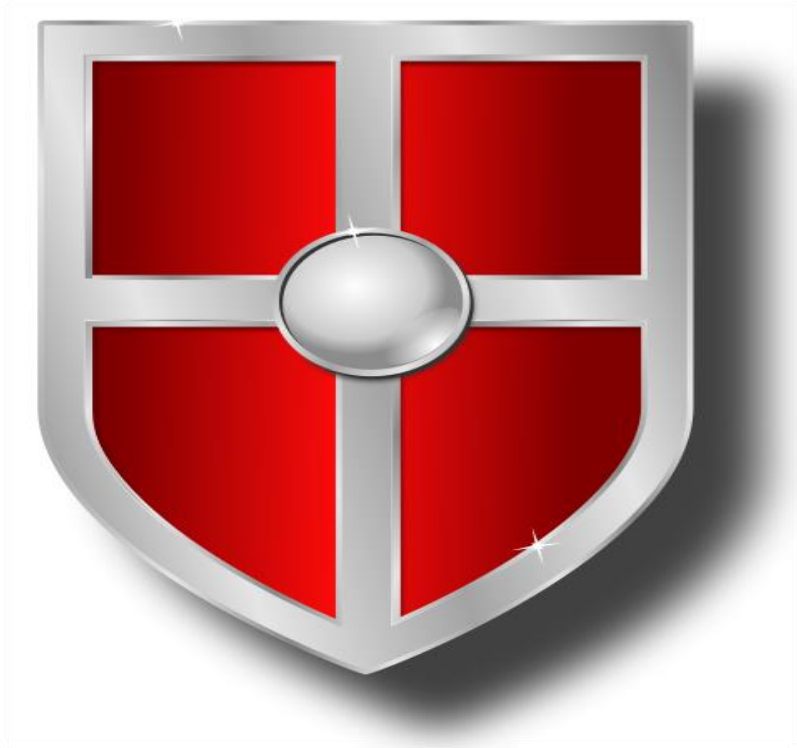
Oxygen Forensic® Detective v.9.3

We are happy to introduce the new Oxygen Forensic® Detective v.9.3.

The new version introduces the ability to extract calls, messages and other data from Huawei cloud via login/password or token. The updated Oxygen Forensic Detective also decrypts contacts and conversations from WhatsApp backup saved in iCloud. Version 9.3 is able to parse encrypted Apple Notes from the latest iOS 9.x and 10.x devices.

bsi. Copyright © 2017 BSI. All rights reserved

SafeHarbour



Copyright © 2017 BSI. All rights reserved

Take Aways

- Device Manufactures provide the means and the features that allow app developers to create apps
- New Apple File System has been introduced
- Security and encryption has become more easier to implement
- Apps are encrypting all of their data:
  - Data on the devices is encrypted
  - Data in communication is encrypted
- Encryption is here to stay and will be more rigorously enforced
- Its likely that getting to the data will be ever more difficult
- Forensic tools have been keeping up but are always lagging behind

bsi. Copyright © 2017 BSI. All rights reserved

Co-funded by the Justice Programme of the European Union 2014-2020

IS WHATSAPP A RELIABLE WITNESS IN COURT?

MODIFYING WHATSAPP MESSAGES IN A FEW CLICKS

ABRAHAM PASAMAR
MAY 2017

WHO AM I

- **WHO AM I**
  - Abraham Pasamar (@apasamar)
  - INCIDE CEO
  - Over 10 years hands-on experience as a Digital Forensic Investigator, Researcher, Cybersecurity Consultant and Expert Witness.
  - Over 300 Expert Witness Reports and over 100 testify in court.
  - Experience in managing Computer Incidents, Internal Fraud, Data Loss and other Incidents in complex environments and high-profile cases. Both from a technical and client management perspective.

incide

WHATSAPP

- Does it ring a bell?
  - Multiplatform chat App
  - Born in 2009 (still alive :)
  - > 1 BILLION USERS !!!
  - Sold to Facebook in 2014 (19.000 MM $)

incide

WHATSAPP IN COURT

- WhatsApp ScreenShots in court:
  - It’s really easy to take a Whatsapp screenshot with a mobile device.
  - Courts are plenty of screenshots presented as “evidence”.
  - It’s easy to “modify” a screenshot:
    - The Photoshop way
    - The “pro” way ...

THE SCREENSHOT MODIFICATION WAY

DEMO

WHATSAPP IN SPANISH COURTS

- **Case number 300/2015**
  - On May 19, 2015 Spanish Criminal High Court established the criteria to accept the probative value of screenshots or “snapshots".
  - The high court stated that it is possible to simulate a communication in which a single user interacts with himself.
  - **It is essential to request an expert to run a forensic analysis of the contents and to provide an expert witness report.**

WHATSAPP MODIFICATION

- Screenshots will not be “alone” again
  - A forensics report is needed
- Is it possible to modify whatsapp messages?
  - During communication?
  - In the mobile phone?

WHATSAPP MODIFICATION

- During communication
  - WhatsApp encryption system is very good
  - Great cryptography model
  - It is not possible to “intercept” whatsapp communications
  - Recently there was a “backdoor” issue

JAILBREAK

WHATSAPP MODIFICATION

- At the mobile phone
  - Messages are not encrypted at the mobile phone
  - To access and modify the messages it is necessary to “root” or “jailbreak” the phone

- What can a **Forensics Expert** do to “**detect**” a **jailbreak**:
  - There are some indicators to detect a Jailbreak:
    - Presence of APPs (i.e. cydia, terminal, etc)
    - Shell access
    - Several files in the filesystem created by the jailbreak process

- What if the **Forensic Expert “detects” a jailbreak**:
  - Messages may have been modified, but maybe not.
  - The expert should look for traces of alteration.
  - Even in the case of not finding any evidences, the messages may have been modified.
  - In this case, **forensic experts are usually not able to be conclusive on the results**.

- What if the **Forensic Expert does NOT “detect” a jailbreak**:
  - What does the expert conclude in this cases:
    - Most experts will certainly be able to assess the integrity of the messages.

- Why is it a mistake?
  - Because **it is possible to modify Whatsapp messages in a no-jailbroken device !**

BACKUP

MODIFYING WHATSAPP MESSAGES

- “Local” BACKUPs (iTunes) can be:
  - Encrypted
  - Not encrypted
- Encrypted backups contain “sensitive” data (email health, etc.)
- Anyway, **backup not encrypted contains a <u>Whatsapp database</u>**

THE DATABASE MODIFICATION “PRO WAY”

DEMO

FORENSICS EXPERT

- We have seen **how to modify WhatsApp Messages in a few clicks**.
- **Is it possible to “detect” these kind of alterations?**
  - **Many experts will not detect** this kind of “modification”:
    - They will consider that is not possible to modify WhatsApp messages without “Jailbreaking” the phone.
    - They will not jailbreak the phone to perform a forensic analysis.
    - They will assume the integrity of the messages.

FORENSICS EXPERT

- **What else can the forensic expert do?**
  - Backup is the the “**cause**” and “**solution**”
  - It is not necessary to perform a Jailbreak in order to look for “modification” traces.
  - The expert has to analyze the backup and there are some interesting indicators... *that will be explained during the presentation.*

REFERENCES

REFERENCES

- https://es.slideshare.net/abrahampasamar/modifying-whatsapp-messages-for-dummies
- https://www.quora.com/Can-a-WhatsApp-message-be-evidence-in-the-court-of-law
- http://blog.lawyer-singapore.com.sg/2016/07/can-whatsapp-message-be-used-as.html
- http://www.elmundo.es/papel/todologia/2016/03/14/56e6cc6b22601d01298b45fb.html (spanish)
- https://translate.google.com/translate?hl=en&sl=es&tl=en&u=http%3A%2F%2Fwww.elmundo.es%2Fpapel%2Ftodologia%2F2016%2F03%2F14%2F56e6cc6b22601d01298b45fb.html (Google translation)

VIGILO consult

Identifiers and Attribution on mobile devices (IP addresses & VOiP)

ERA

Madrid - May 2017

Co-funded by the Justice Programme of the European Union 2014-2020

Introduction

- Mr. Hein Dries-Ziekenheiner
- (LL.M)
- Background
  - Leiden University eLaw dpt.
  - NL ISPA (ISP industry association)
  - Netherlands telecoms agency (OPTA, now ACM): spam and internet safety
  - VIGILO (enforcement online, security, cybercrime)

VIGILO consult

Program

- Introduction
- IP addresses
  - Explanation
  - Issues with identifying users by IP address
- Other mobile identifiers
  - MISDN (Phone number)
  - Other identifiers..
- Attribution of (deleted?) data

VIGILO consult

“Say my name”

Stills from series “Breaking Bad“ © AMC

VIGILO consult

Attribution:“Say My Name”

- “Heisenberg”
- Walter White (“Walt”)
- Bryan Cranston
- Breaking Bad
- And (well..maybe):
  - On 9 feb 2017 at 1500 GMT: 92.78.121.12
  - +1 819 122312341

VIGILO consult

Attribution: Why?

- Cybercrime:
  - Often clear “WHAT”
  - Not so clear “WHO”
  - Regular crime: online identities often at stake
- Examples:
  - Wannacry
  - Sony Hack?
  - Stuxnet (Israel, US?)
  - CP material (expect: TOR, Proxies, VPNs)
  - …

VIGILO consult

VIGILO consult

IP addressing

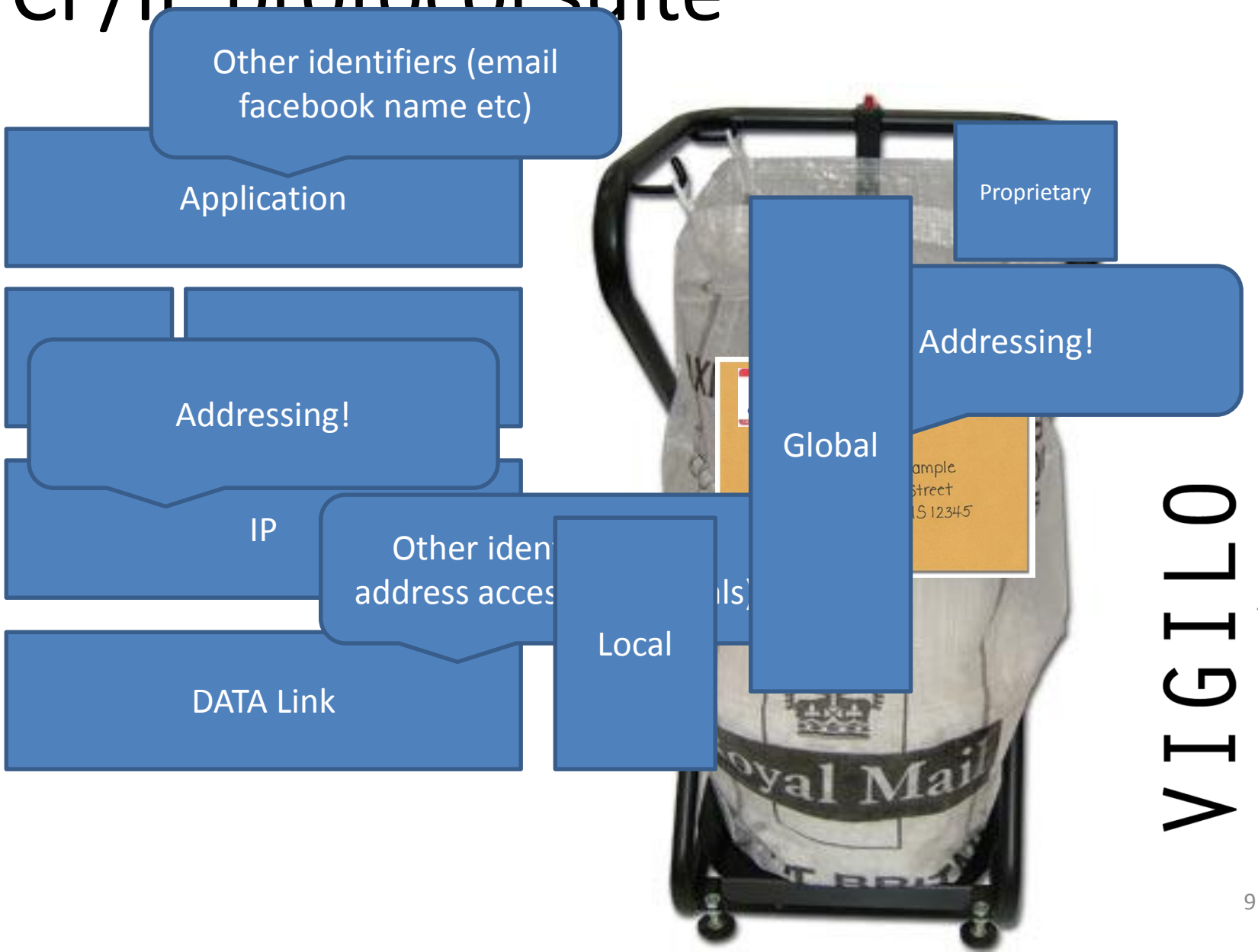
Attribution by IP addresses?

Problem:

- Apache log (not default):
  - 15/05/2017 14:14:59 [16955] [INFO] [hein2] Version='2.2.7' method='POST' from='**88.159.38.171**' cmd='Ping' getUser=**'hein2'** devId='**nine8a55157afa9a**' devType='**Android**'

VIGILO consult

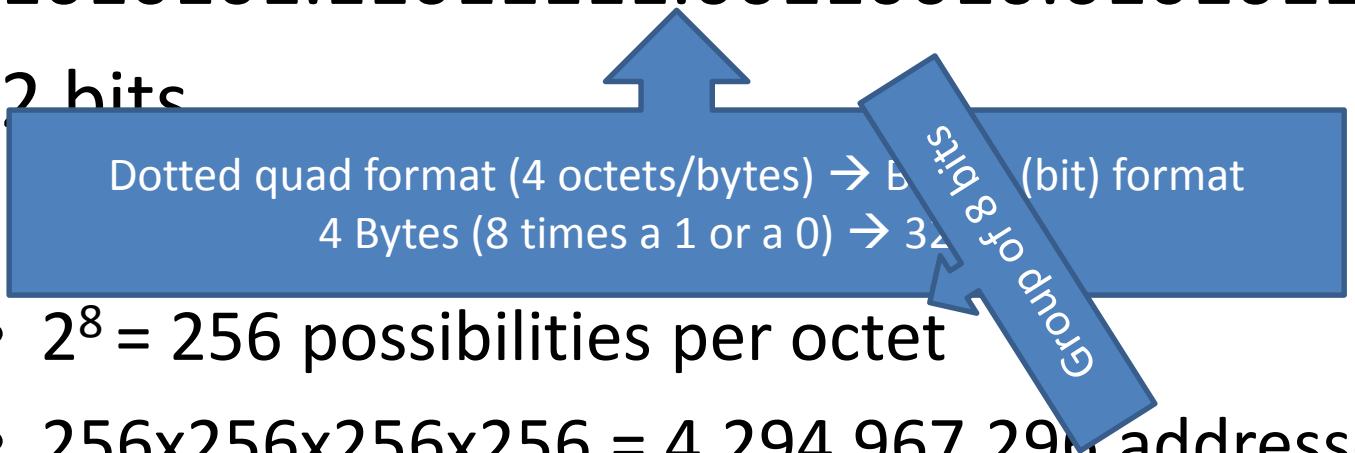
TCP/IP protocol suite



VIGILO consult

Addresses (IPv4)

- What is an IP address?
- Is this an IP address: 85.223.50.87 ?
- And this: 01010101.11011111.00110010.01010111 ?
- 32 bits
- 4
  - 2^8 = 256 possibilities per octet
  - 256x256x256x256 = 4,294,967,296 addresses



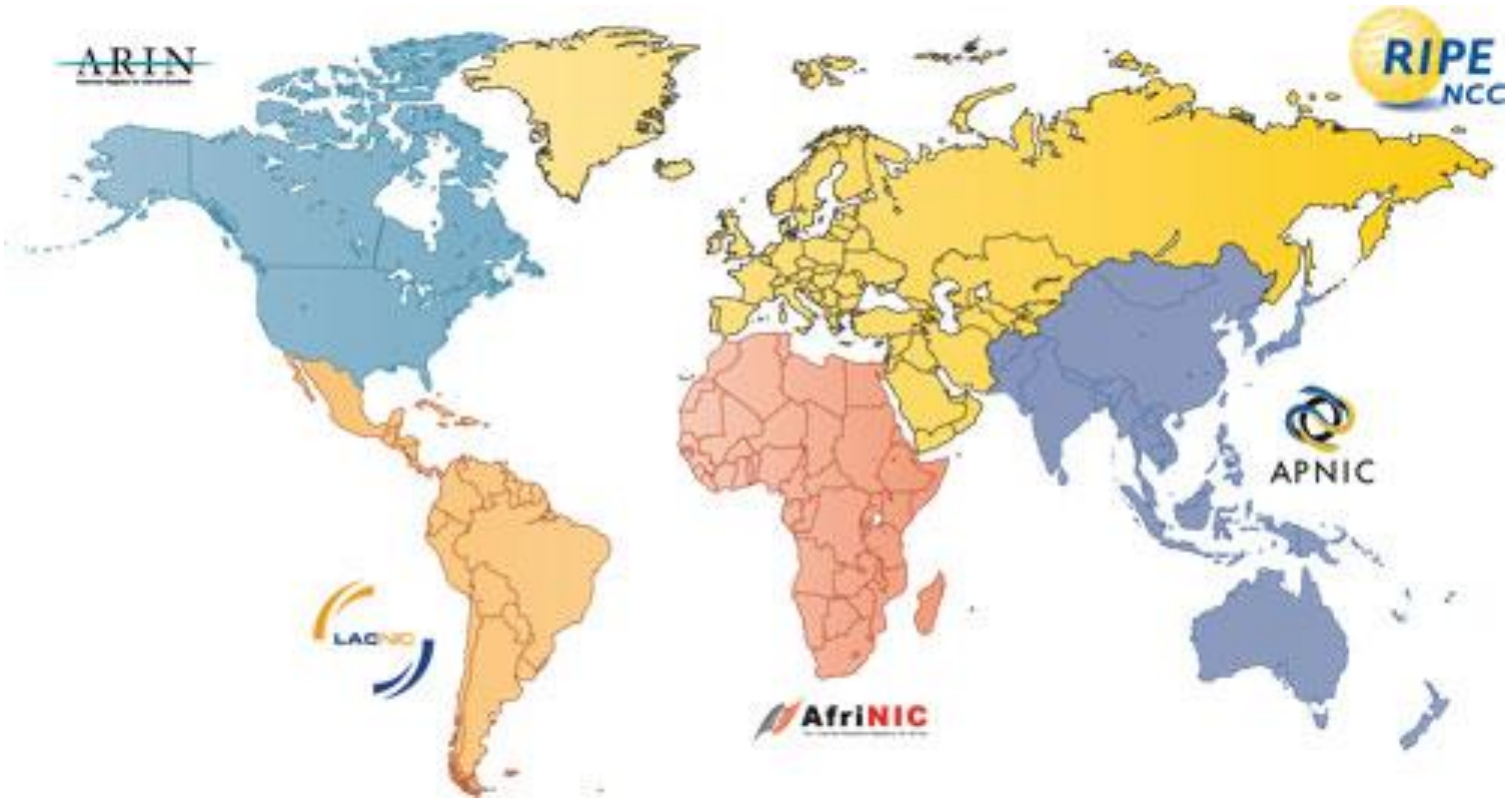
VIGILO consult

Allocation and assignment

- Global: allocation
  - By regions (EU: RIPE NCC, Amsterdam)
  - Large blocks
  - Typically **TO** Internet companies (ISPs)
- Local: assignment (IPv4):
  - One or multiple addresses to an end user
  - Smaller blocks/ Individual addresses
    - Automatically (“DHCP or PPPoE”)
    - Manually

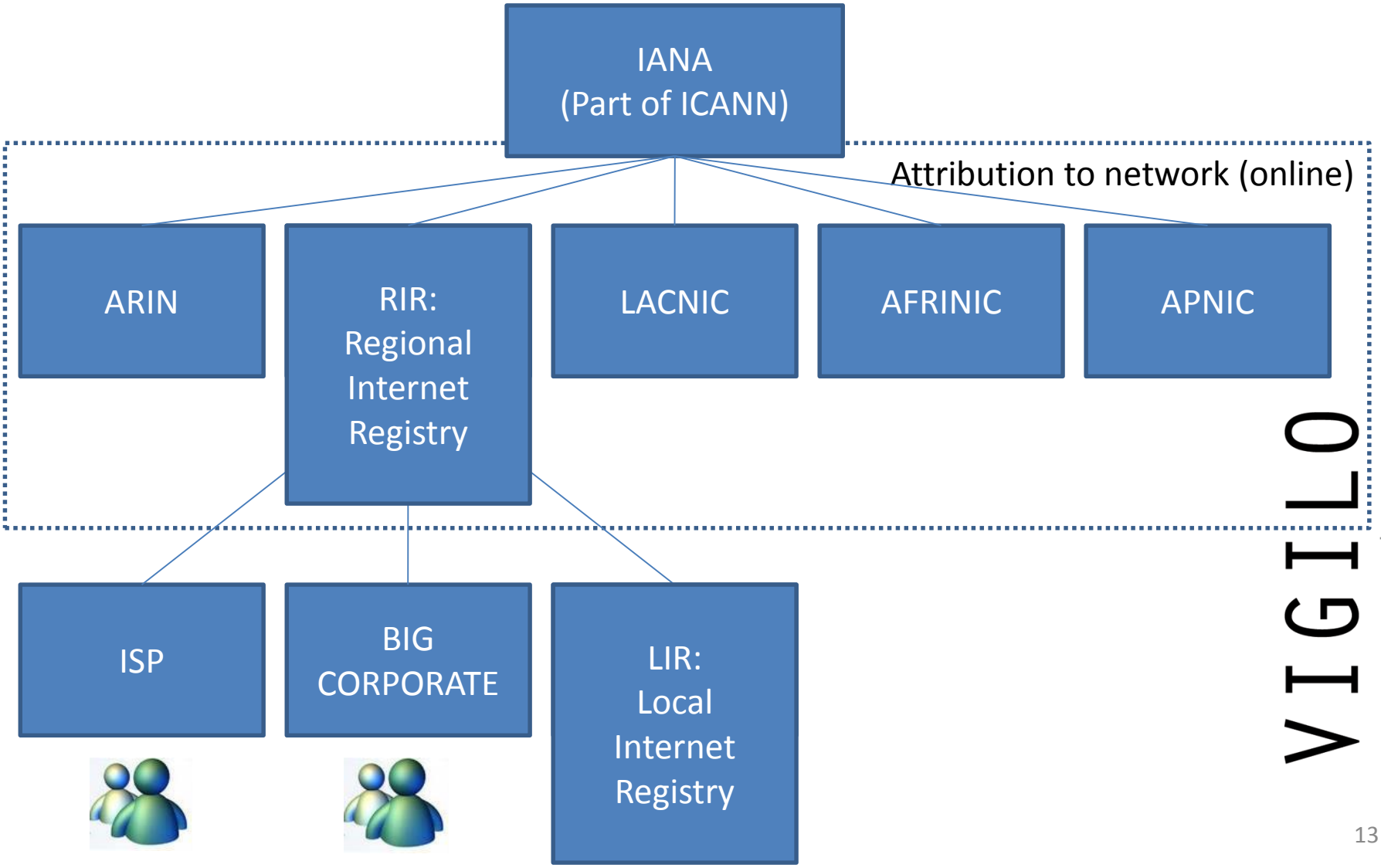
VIGILO consult

Allocation: regions



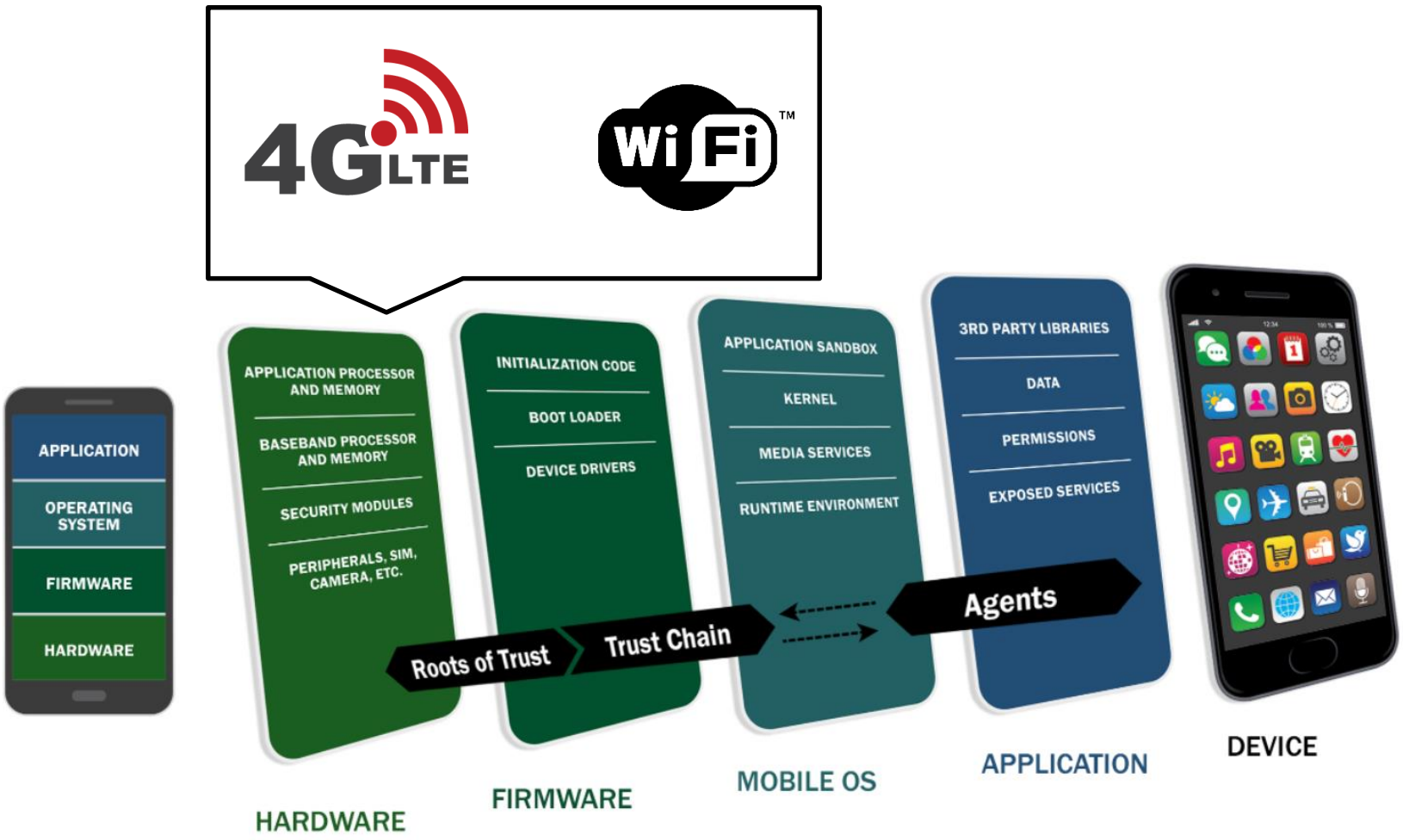
VIGILO consult

Address allocation



VIGILO consult

Assignment


4G LTE
Wi Fi
APPLICATION
OPERATING SYSTEM
FIRMWARE
HARDWARE
APPLICATION PROCESSOR AND MEMORY
BASEBAND PROCESSOR AND MEMORY
SECURITY MODULES
PERIPHERALS, SIM, CAMERA, ETC.
INITIALIZATION CODE
BOOT LOADER
DEVICE DRIVERS
APPLICATION SANDBOX
KERNEL
MEDIA SERVICES
RUNTIME ENVIRONMENT
3RD PARTY LIBRARIES
DATA
PERMISSIONS
EXPOSED SERVICES
Roots of Trust
Trust Chain
Agents
HARDWARE
FIRMWARE
MOBILE OS
APPLICATION
DEVICE

“Technical Issues”

- Dynamic/Static (&Sticky)
- Public/private
- (Carrier Grade) NAT (!?)

VIGILO consult

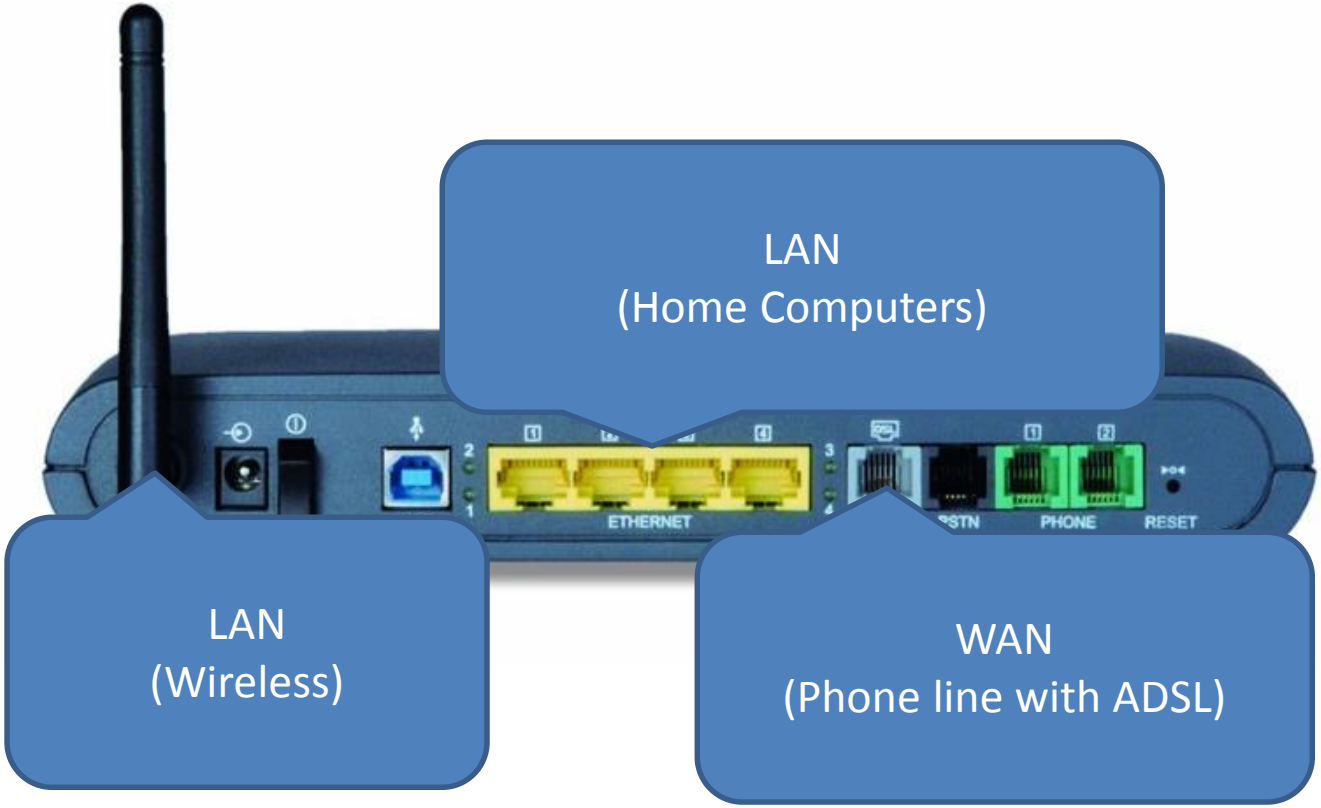
Types: Static vs. Dynamic

- Static
  - Often entered manually
  - Assigned for long period of time
- Dynamic
  - Usually automatically assigned at start of session
  - Upon connection
  - Short periods (may even change during session)
- “Sticky”
  - Dynamic address that sticks to a device (usually only changes after a lengthy disconnection)

VIGILO consult

Private vs Public

- Private
- Public



VIGILO consult

Private vs Public

- Private use (10.x.x.x 192.168.x.x , 172.16-31.x.x)
  - Routed/Used only on LAN
- Public use (basically: the rest)
  - You **need** to have a public address to access the internet (issue: NAT..)
  - Routed on Internet (WAN)

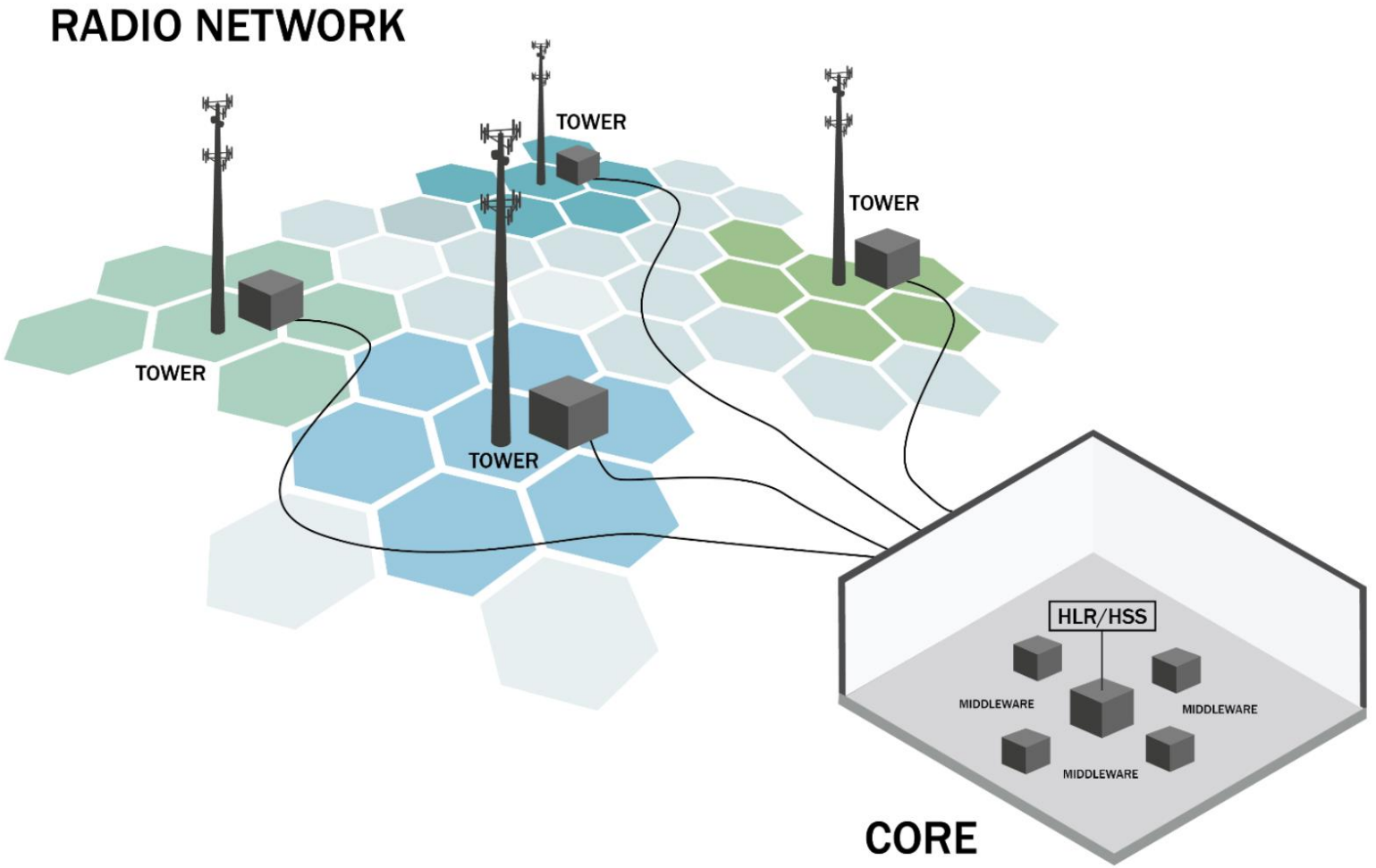
VIGILO consult

Key: time, ports, logging

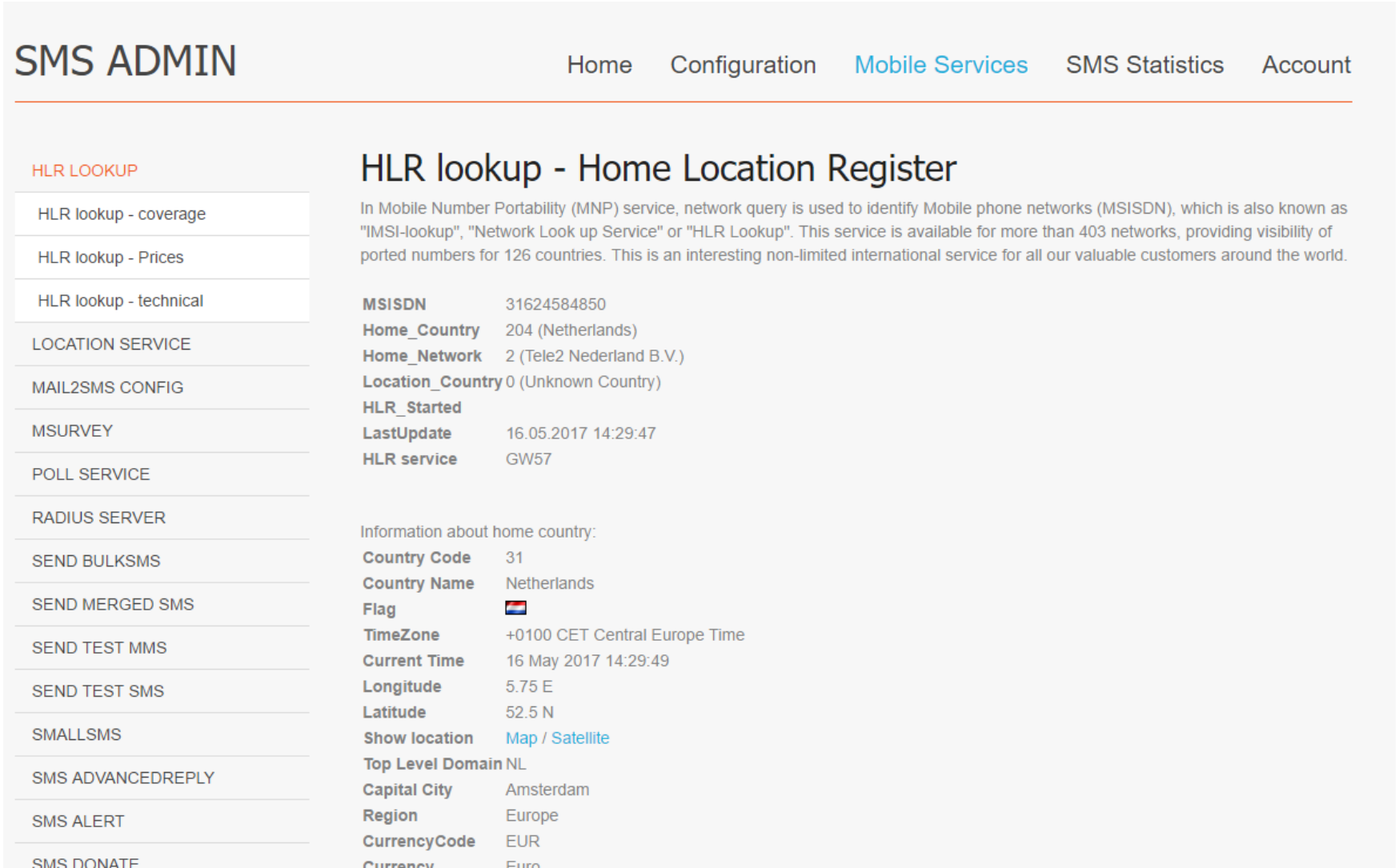
- Attribution Fixed Networks
  - Connection “street” address
  - Useful: Low number of users and long lease time
- Attribution Mobile / Public Wifi
  - Harder: Sometimes user unknown
  - Useful payment details, address
  - Logging not always sufficient
    - In services
    - In the provider administration

VIGILO consult

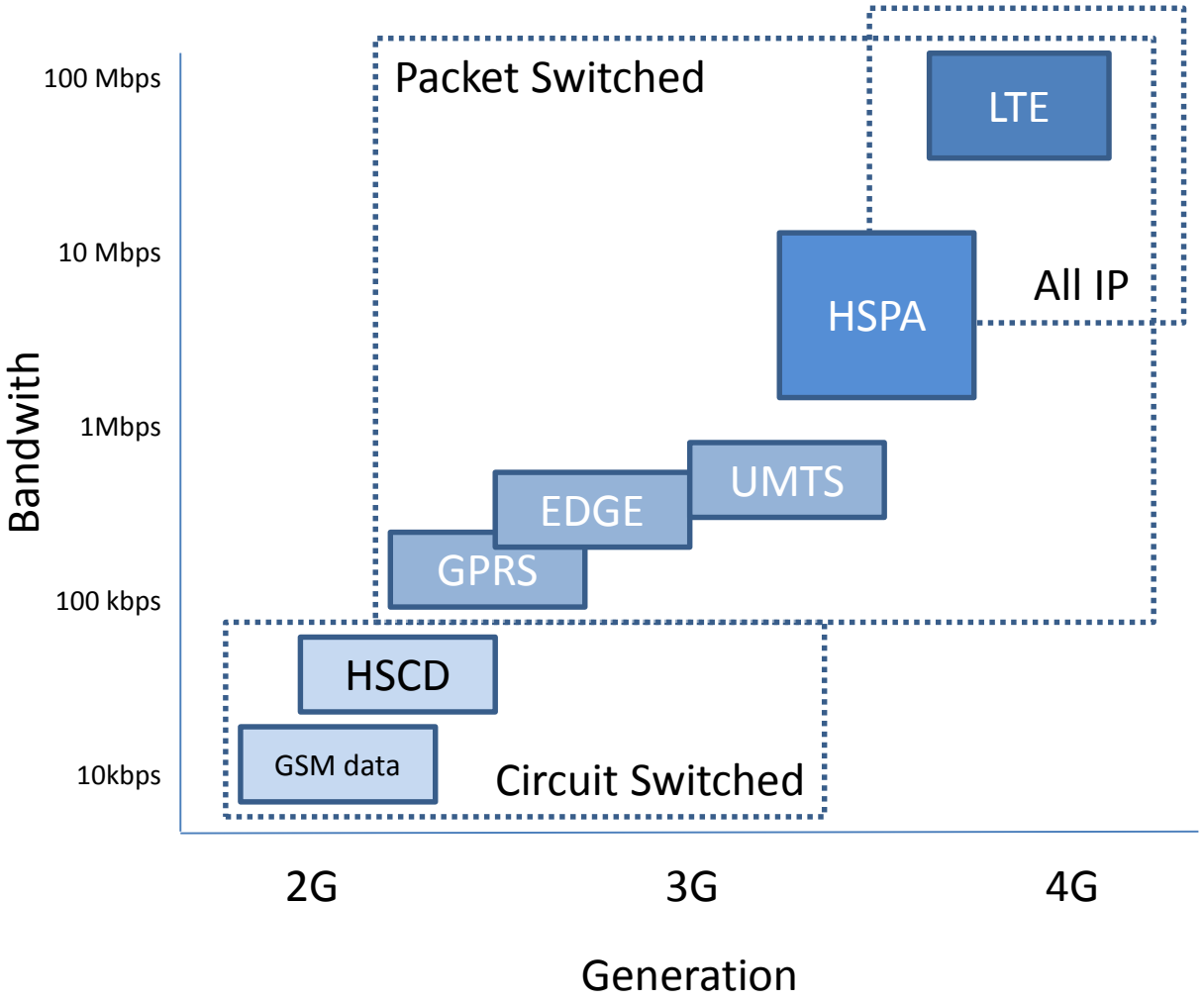
Mobile networks



HLR lookup

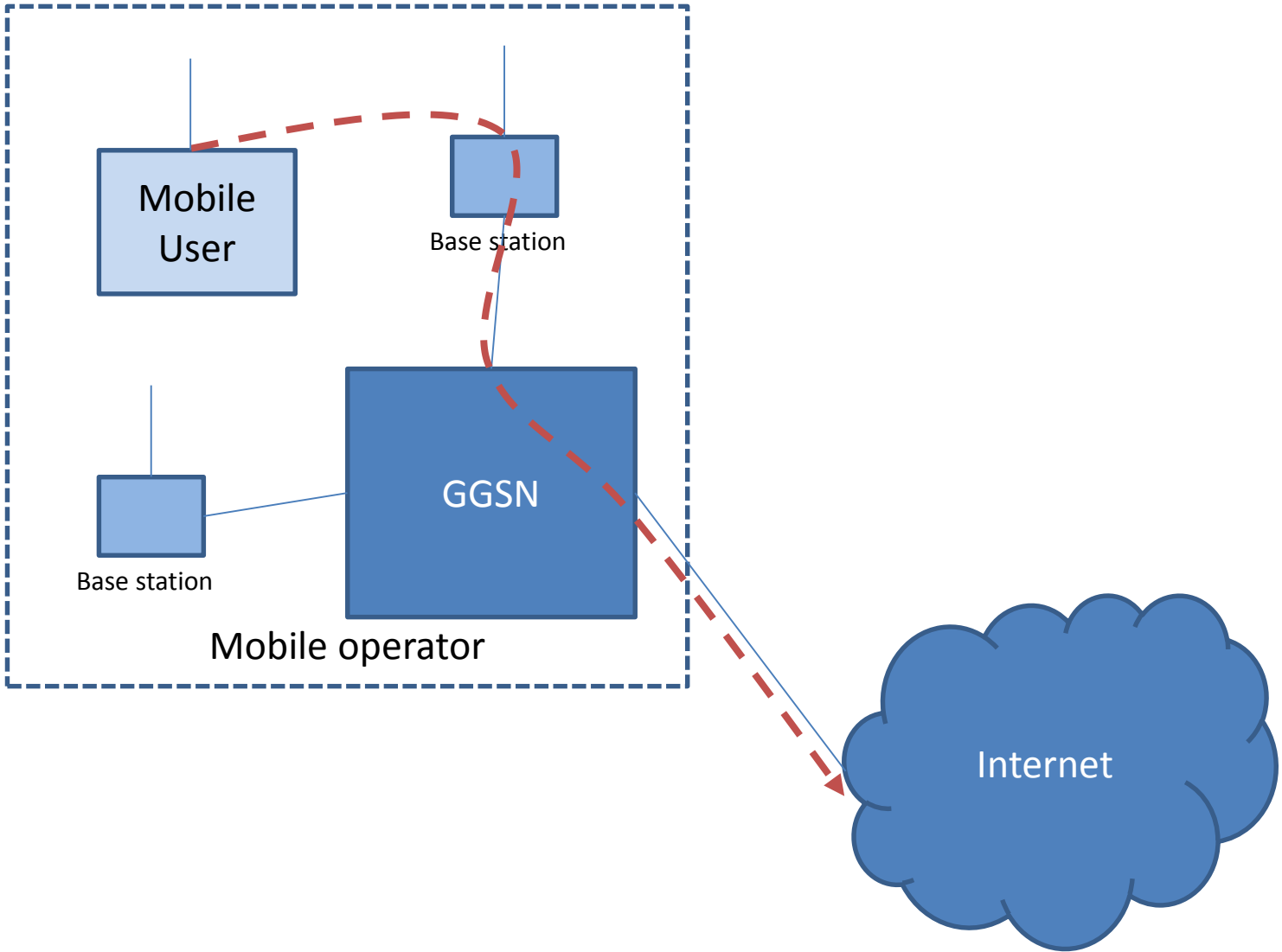

SMS ADMIN
Home
Configuration
Mobile Services
SMS Statistics
Account
HLR LOOKUP
HLR lookup - coverage
HLR lookup - Prices
HLR lookup - technical
LOCATION SERVICE
MAIL2SMS CONFIG
MSURVEY
POLL SERVICE
RADIUS SERVER
SEND BULKSMS
SEND MERGED SMS
SEND TEST MMS
SEND TEST SMS
SMALLSMS
SMS ADVANCEDREPLY
SMS ALERT
SMS DONATE
HLR lookup - Home Location Register
In Mobile Number Portability (MNP) service, network query is used to identify Mobile phone networks (MSISDN), which is also known as "IMSI-lookup", "Network Look up Service" or "HLR Lookup". This service is available for more than 403 networks, providing visibility of ported numbers for 126 countries. This is an interesting non-limited international service for all our valuable customers around the world.
MSISDN 31624584850
Home_Country 204 (Netherlands)
Home_Network 2 (Tele2 Nederland B.V.)
Location_Country 0 (Unknown Country)
HLR_Started
LastUpdate 16.05.2017 14:29:47
HLR service GW57
Information about home country:
Country Code 31
Country Name Netherlands
Flag
TimeZone +0100 CET Central Europe Time
Current Time 16 May 2017 14:29:49
Longitude 5.75 E
Latitude 52.5 N
Show location Map / Satellite
Top Level Domain NL
Capital City Amsterdam
Region Europe
CurrencyCode EUR

Technologies



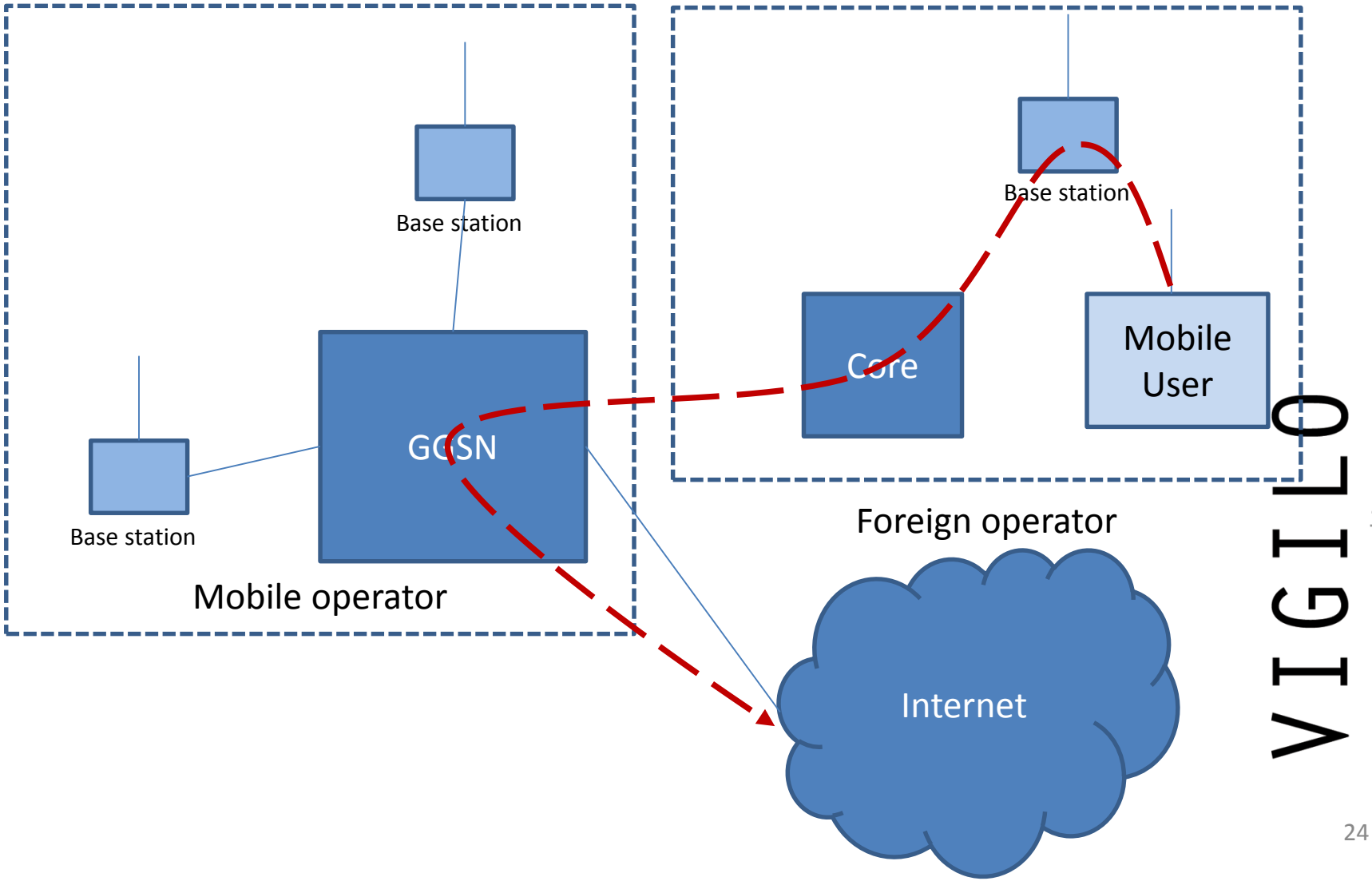
VIGILO consult

Old style



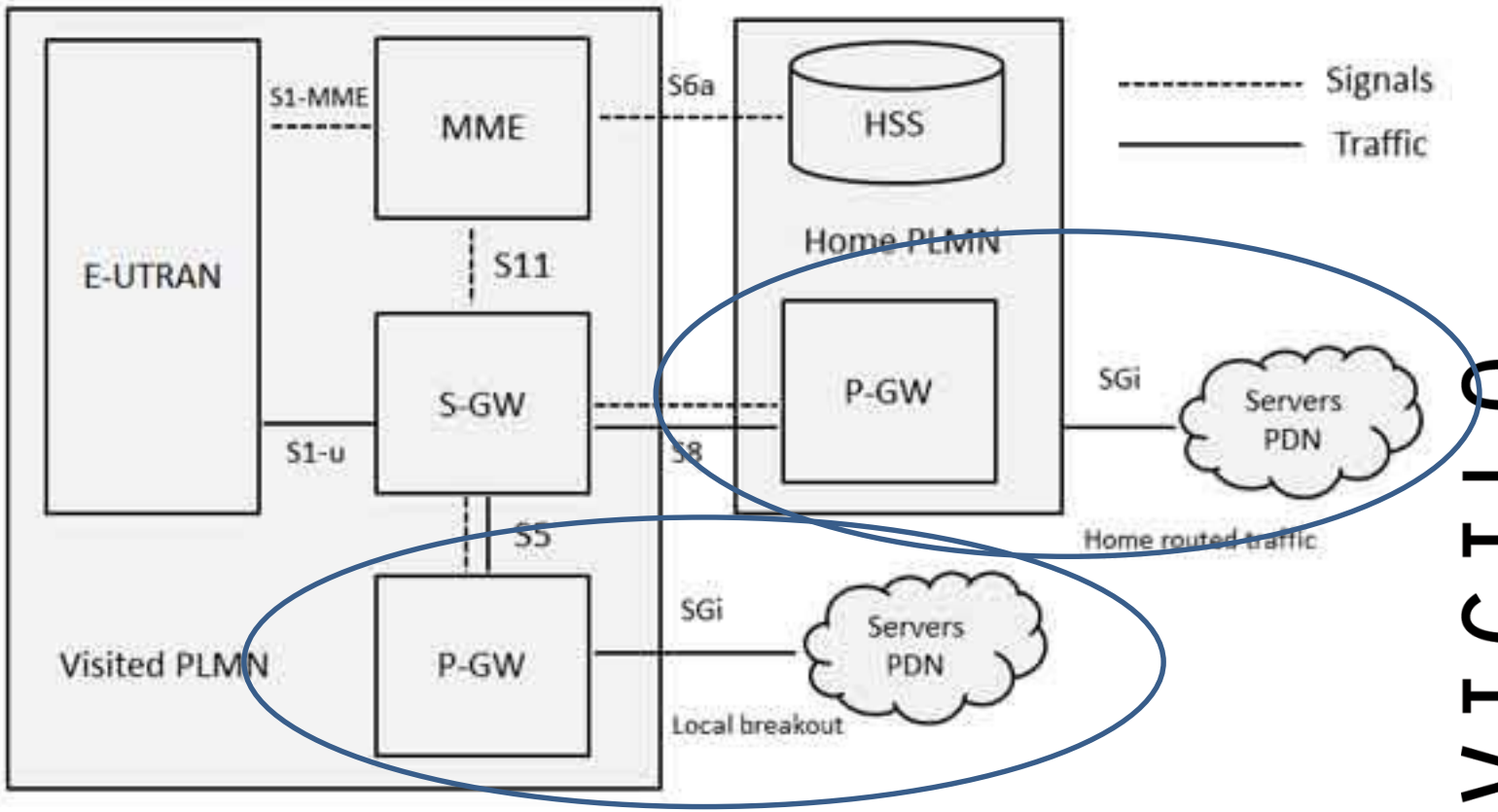
VIGILO consult

Roaming



VIGILO consult

LTE: local breakout



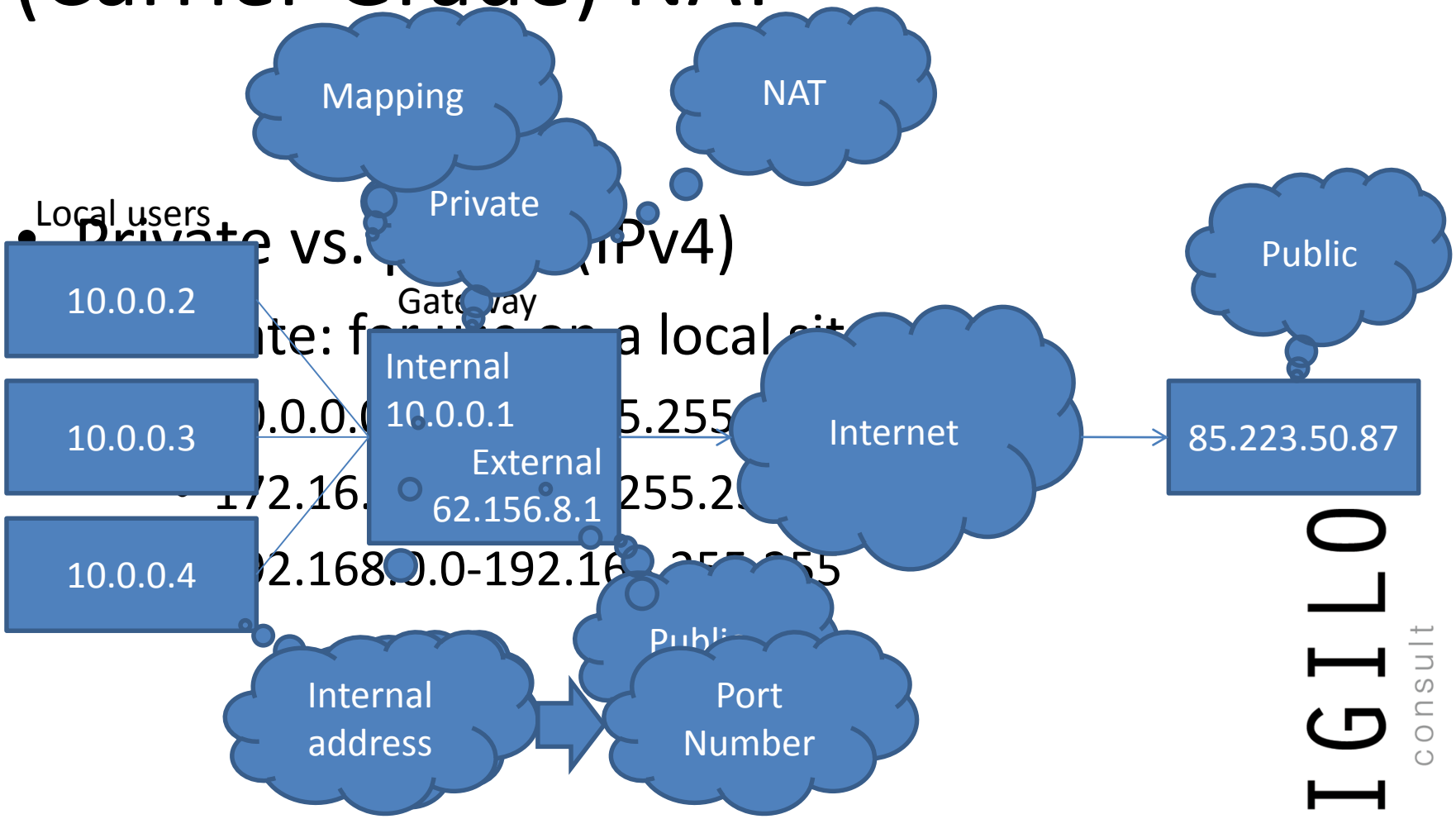
VIGILO consult

Mobile: many devices

- Shortage of IPv4
- IPv6 is slow to pick up (some networks have it now!)
  - IPv6 not widely used yet – not by consumers!
  - Many destinations have it (google, facebook, linkedin, europa.eu)
- Many networks use NAT in the network.

VIGILO consult

(Carrier Grade) NAT



- Private vs. Public (IPv4)
  - Private: for use on a local site
    - 10.0.0.0-10.255.255.255
    - 172.16.0.0-172.31.255.255
    - 192.168.0.0-192.168.255.255

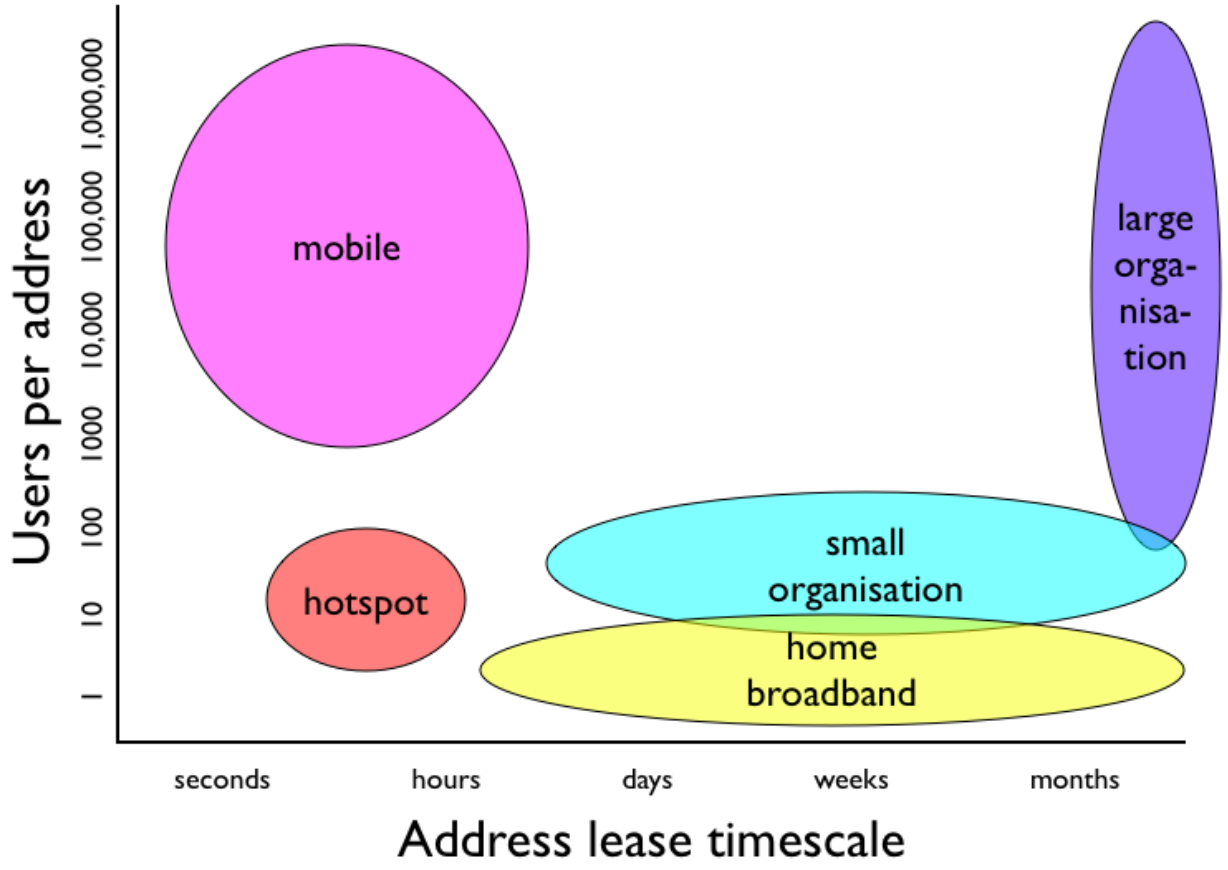
VIGILO consult

NAT: Solution?

- Make outgoing port numbers unique for each user
- Problem: logging of port numbers is not common
- Apache log (default):
  - 180.76.5.158 - - [27/Feb/2012:16:18:44 +0100] "GET /robots.txt HTTP/1.1" 404 294 "-" "Baiduspider+(+http://www.baidu.com/search/spider.htm)“

VIGILO consult

Lease times vs users per address



VIGILO consult

Other issues

- TOR
- VPNs
- Proxies

VIGILO consult

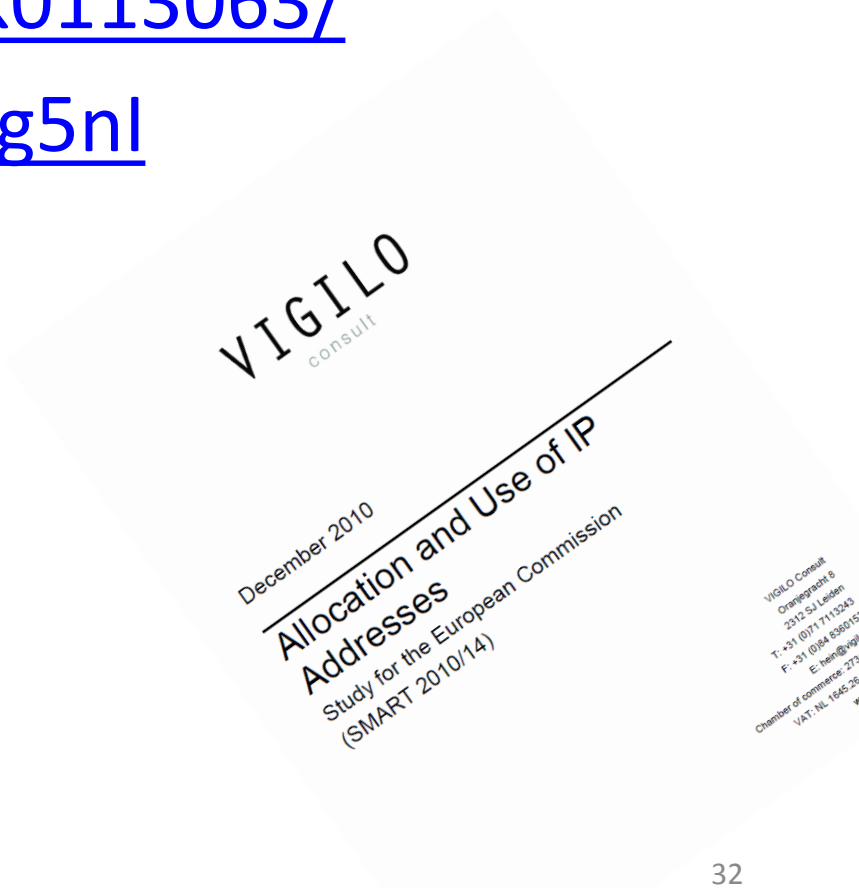
Conclusion: Identifying users by IP

- Depends on precision of logging on both sides
  - TIME (inc Timezone)
  - PORT
- Depends on the provider
  - Note: Data retention (CJEU C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others)
  - (Carrier Grade) NAT (big issue)
- Depends less on “Static” vs “Dynamic” more on NAT
- Spoofing: only UDP

VIGILO consult

More?

- http://bookshop.europa.eu/nl/allocation-and-use-of-ip-addresses-pbKK0113063/
- Or well.. http://bit.ly/17zg5nI



VIGILO consult

Phone numbers

Another namespace ..

Another mess..

Telephone calls

- Used to be

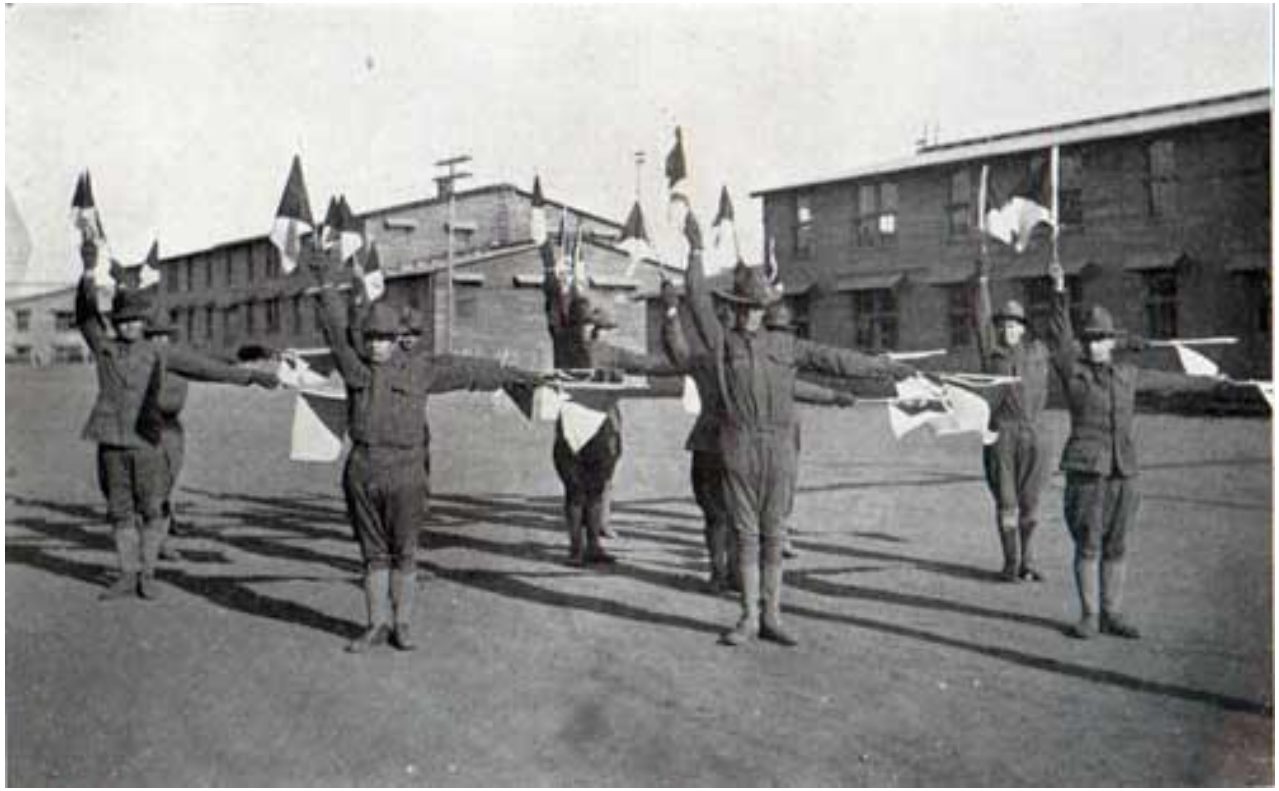
- Interconnection: connecting wires (carry signal).
- Signaling: ringing (transport, dial and ring).

VIGILO consult

Interconnection

VIGILO consult

Signaling

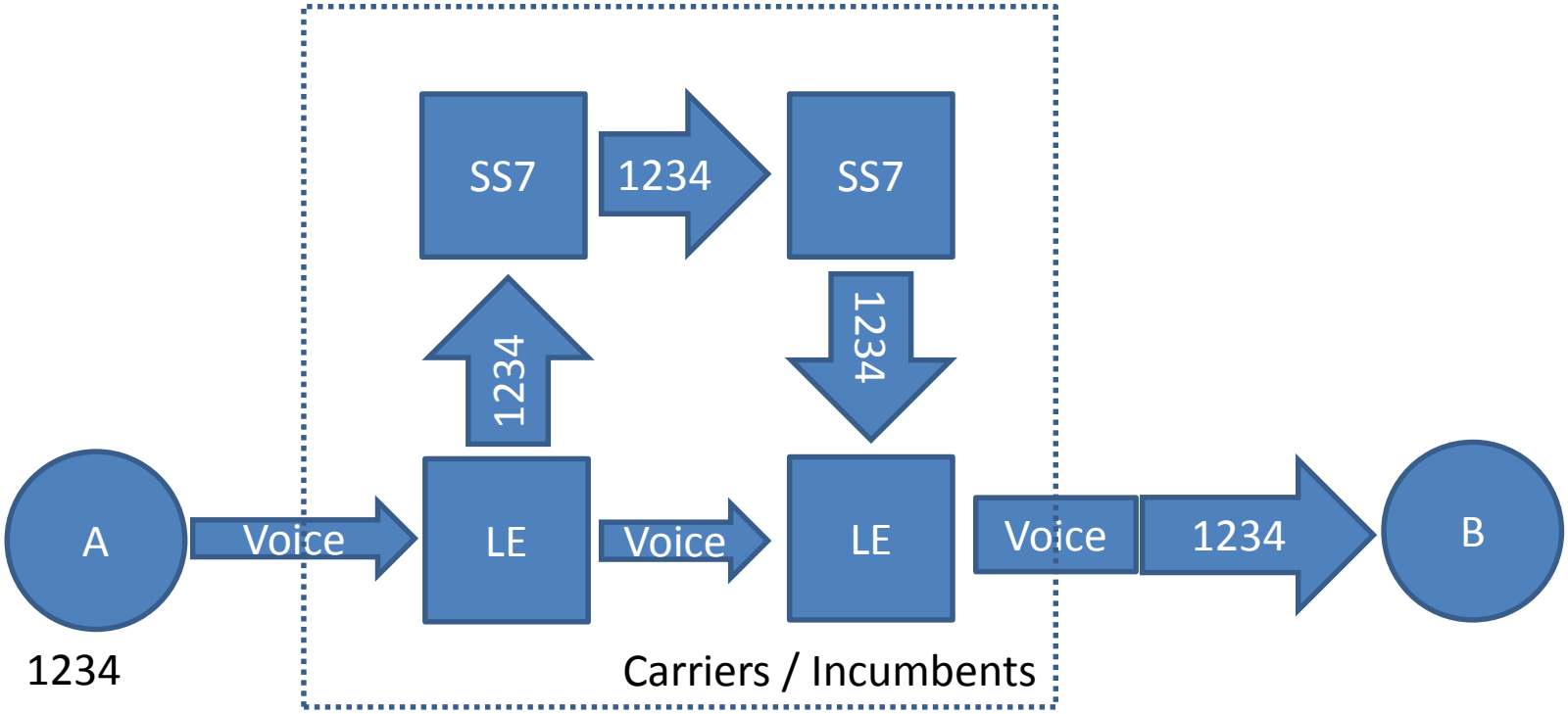


VIGILO consult

1971 Patent

VIGILO consult

SS7 (old networks) & Caller ID

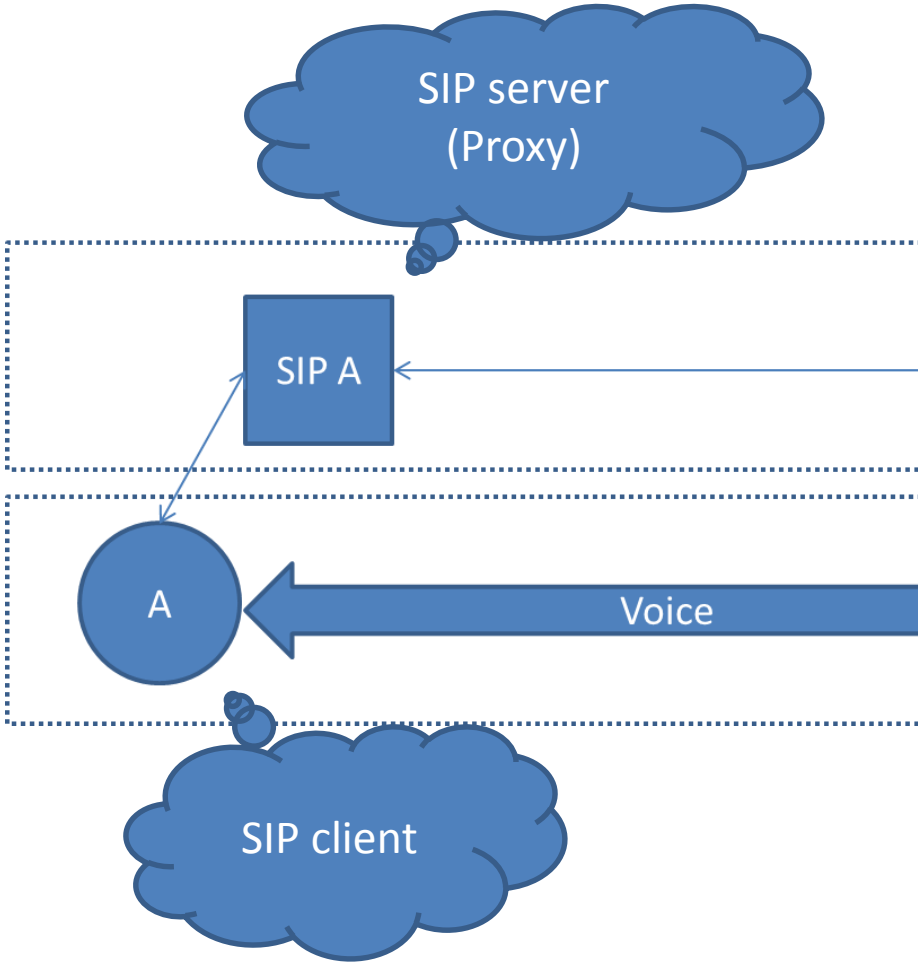


Nowadays

- VOIP
- Main Protocols
- Proprietary: SKYPE etc (not easy to spoof)
- [illegible]
- prone to spoo

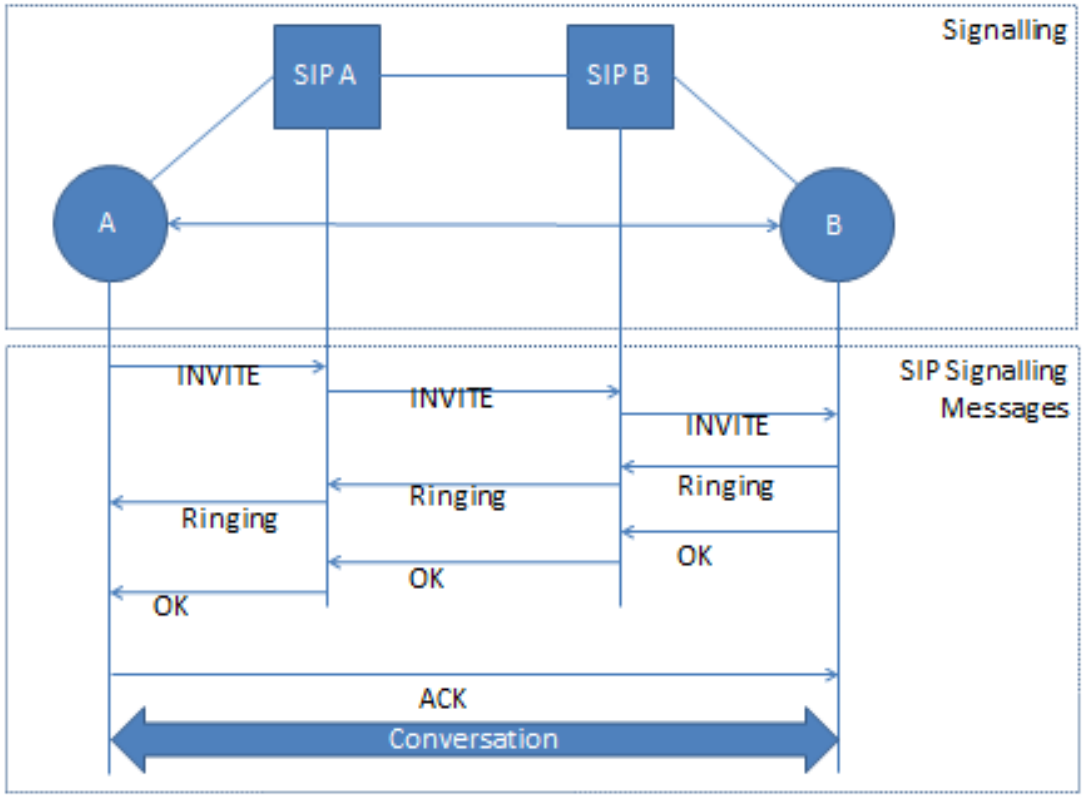
VIGILO consult

SIP call



NTGTA consult

SIP

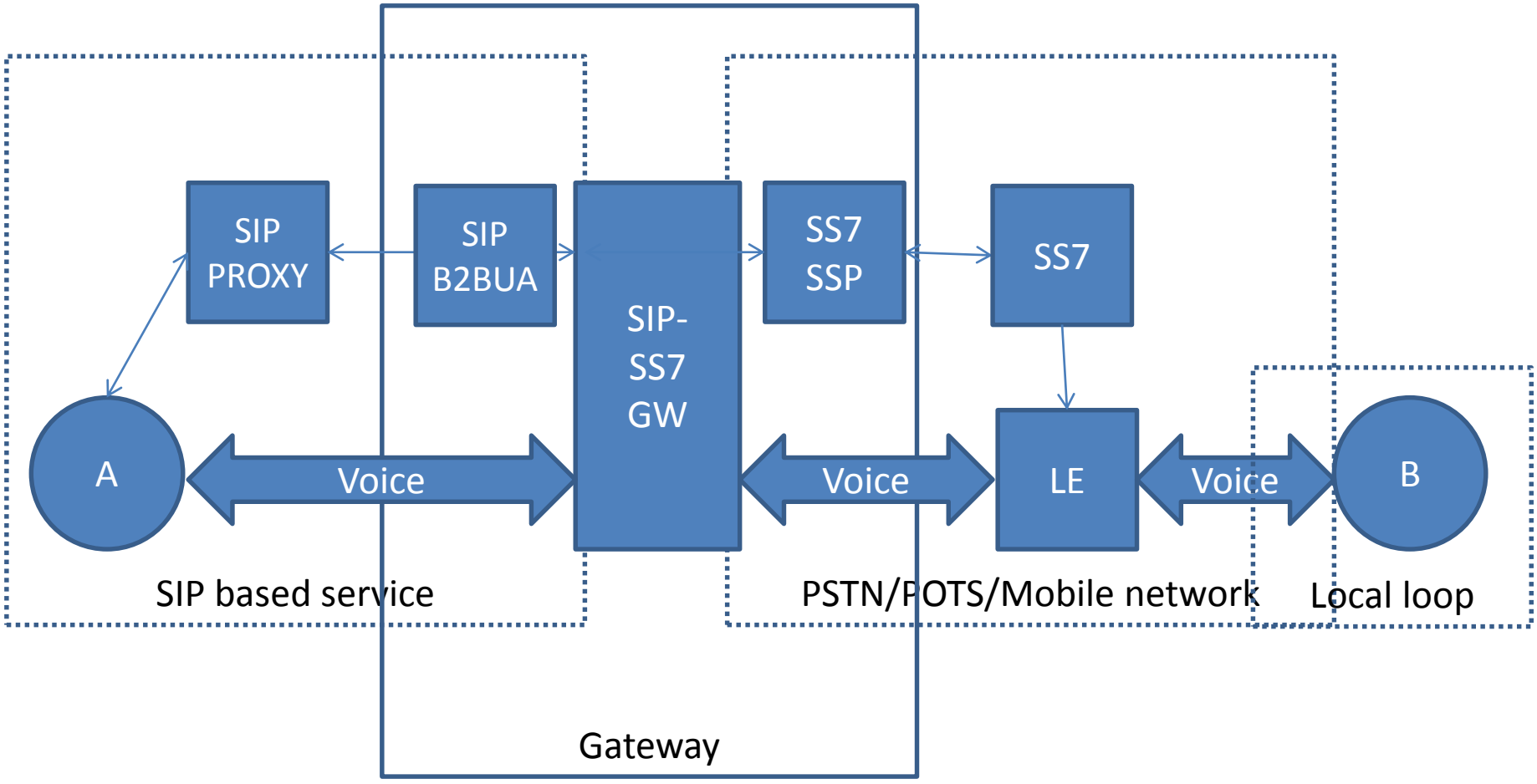


VIGILO consult

Messages (Alice calls Bob)

```
INVITE sip:1234@biloxi.com SIP/2.0
Via: SIP/2.0/UDP
pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:1234@biloxi.com>
From: Alice
<sip:6666@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:6666@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142
```

SIP and SS7: Gateways



Ok Hein.. I am lost..

- What does this all lead to?
- ..Demo time!

VIGILO consult

Issues

- Wire taps
- Recent Calls lists (often found in phones)
- Deliberate “injection” of Caller ID?

Note:

Only relates to “FROM” number.

VIGILO consult

VIGILO consult

Attribution

Attribution

- Data on the phone: more reliable
  - Depends on circumstances
  - What locks the phone/FS key?
    - Nothing?
    - Password
    - Pattern
    - Biometrics

VIGILO consult

Biometrics

Biometric	1:N	Sensor availability
Iris (dual)	Infinite	Low
Fingerprint (10 fingers)	Infinite	Medium
Fingerprint (single finger)	~100.000.000	High
Face (facial recognition)	1000	High
Voice (voice recognition)	1000	High

- Depends on implementation!
- In real life: uniqueness of fingerprint, iris and voice/facial recognition is a trade-off between sensor quality, capture conditions and required speed.

VIGILO consult

Conclusion

- Identifiers online:
  - Many issues
  - IP addresses: attribution is hard, trustworthy
  - Phone numbers: don’t trust originating per se, to: number (A number, destination number) is reliable.
  - Others: depends!
- Solution:
  - Corroberating evidence
- Attribution: biometric sensors make this easier for physical device

VIGILO consult

ACONITE
INTERNET SOLUTIONS

RANSOMWARE

Co-funded by the Justice Programme of the European Union 2014-2020

©2017 - Cormac Callanan, Aconite Internet Solutions

ACONITE
INTERNET SOLUTIONS

RANSOMWARE

©2017 - Cormac Callanan, Aconite Internet Solutions

ACONITE
INTERNET SOLUTIONS

©2017 - Cormac Callanan, Aconite Internet Solutions

ACONITE
INTERNET SOLUTIONS

Definitions – F-Secure

- Malicious application that steal or encrypts the user's data or system, then demands payment to restore the data or system access
- Typically encrypts files on infected computer and displays a message stating that the user must pay a certain sum in a specified method in order to recover the files

©2017 - Cormac Callanan, Aconite Internet Solutions

Definitions – F-Secure

- Specifics of the extortion method may vary:
  - files may appear 'corrupted and the user may be required to buy a 'clean-up program', or
  - files may be 'locked by an authority for an alleged transgression, and the user may need to pay a 'fine'
- Extortion works on the assumption that the data is important enough to the user that they are willing to pay for recovery.

©2017 - Cormac Callanan, Aconite Internet Solutions

Impersonating Police

9 Aug 2012

http://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/

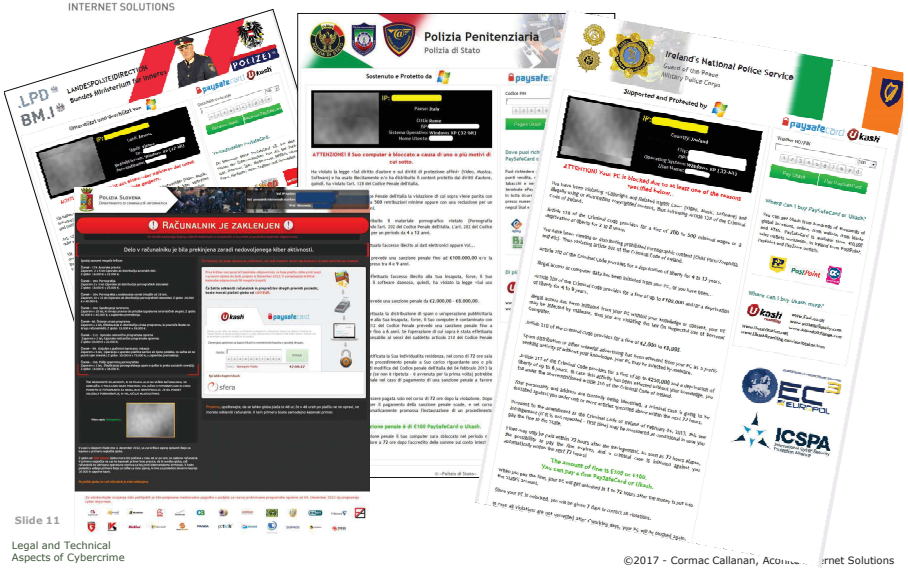
- Online extortion scams impersonate the FBI (or national police forces) and frighten people into paying fines to avoid prosecution for supposedly downloading child pornography and pirated content
- Uses drive-by downloads to hijack host machines
- Malware **displays a threatening message** and blocks the user from doing anything else unless a 'fine' is paid
  - (or the user finds a way to remove the malware)
- Attacks have surged with the help of a "new drive-by virus" called **Reveton**

©2017 - Cormac Callanan, Aconite Internet Solutions

©2017 - Cormac Callanan, Aconite Internet Solutions

Botnets.fr

https://www.botnets.fr/index.php/Reveton



©2017 - Cormac Callanan, Aconite Internet Solutions

Side effects

- RansomWare component is likely the most visible of the threats that reside on the system
- Latest Reveton versions will steal all passwords stored on the victim's PC.
- FBI report indicates Reveton is being bundled with Citadel
  - (extremely powerful and advanced family of malware that can be quite difficult to remove)
- Trojan locks your computer and displays a localized webpage that covers your desktop, and demands the payment of a fine for the supposed possession of illicit material

©2017 - Cormac Callanan, Aconite Internet Solutions

Trojan:W32/Ransomcrypt (1)

http://www.f-secure.com/weblog/archives/00002347.html

- When first run the ransomware will iterate all folders on the system
- Every document, image, and shortcut (.lnk) file found will be encrypted
  - changed extension of .EnCiPhErEd.

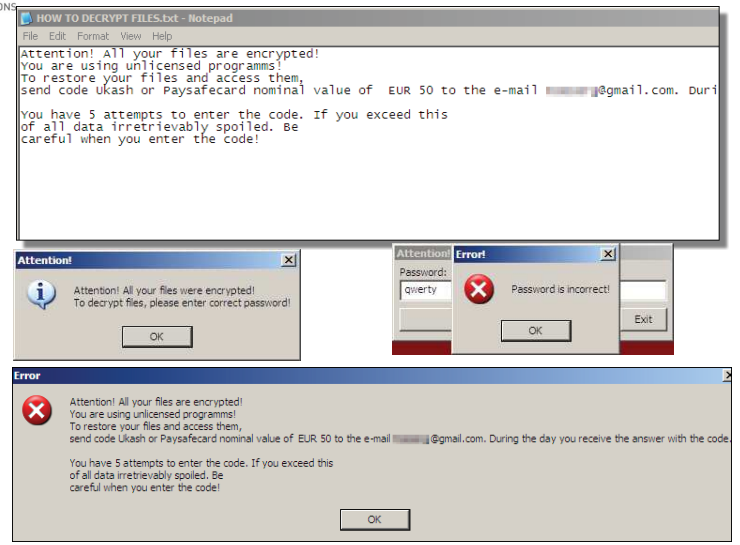
©2017 - Cormac Callanan, Aconite Internet Solutions

Trojan:W32/Ransomcrypt (2)

http://www.f-secure.com/weblog/archives/00002347.html

- In each folder it places a text file called "HOW TO DECRYPT.TXT" which contains instructions on how to proceed and includes a demand for €50
  - Places copy of itself in the system's temp folder with a random name
  - Creates registry entries to associate the .EnCiPhErEd extension with itself, so that the temp folder copy is launched whenever those files are run, in order to demand the decryption password.
  - After five attempts it no longer accept passwords. And it then deletes itself, leaving data encrypted.

©2017 - Cormac Callanan, Aconite Internet Solutions



©2017 - Cormac Callanan, Aconite Internet Solutions

Trojan:Win32/Crilock.A and Trojan:Win32/Crilock.B

Displays a timer stating that the company has 96 hours to pay the ransom or it will delete the encryption key

- Encrypts 40 file types
  - specific files such as documents, spreadsheets, databases and other files that are strategic and valuable
- Encrypts using AES-256 key unique to each file
  - encrypts the file-specific AES key using a 2048-bit RSA public key
- Affected 34,000 machines
  - Sept-13 to Nov-2013
- Ransom can be paid with various online currencies
  - BitCoin, CashU, MoneyPak, Paysafecard, and Ukash

http://blogs.technet.com/b/mmpc/archive/2013/11/19/backup-the-best-defense-against-cri-locked-files.aspx

©2017 - Cormac Callanan, Aconite Internet Solutions

local and mapped network drives

More Information:
http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information

©2017 - Cormac Callanan, Aconite Internet Solutions

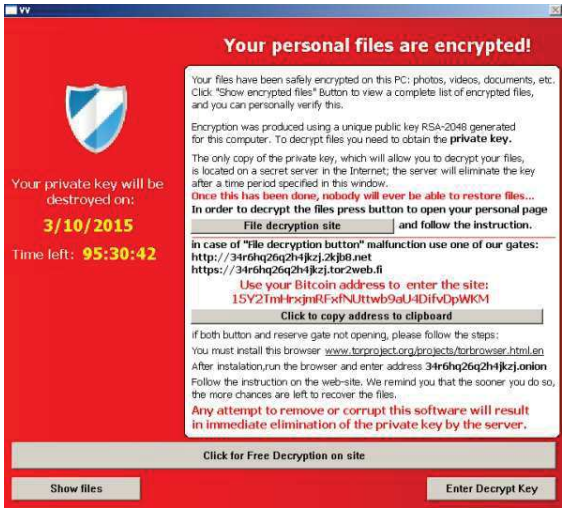
FBI's Internet Crime Complaint Center (IC3)

http://www.ic3.gov/media/2015/150623.aspx

- IC3 reporting identified CryptoWall as one of the significant ransomware threat targeting U.S. individuals and businesses
- Financial impact to victims goes beyond the ransom fee itself
  - which is typically between $200 and $10,000
- Victims incur additional costs
  - associated with network mitigation, network countermeasures, loss of productivity, legal fees, IT services, and/or the purchase of credit monitoring services for employees or customers
- Between April 2014 and June 2015, the IC3 received 992 CryptoWall-related complaints
  - victims reporting losses totaling over $18 million.

©2017 - Cormac Callanan, Aconite Internet Solutions

Ransomware



http://uk.businessinsider.com/fbi-recommends-paying-ransom-for-infected-computer-2015-10?r=US&IR=T

©2017 - Cormac Callanan, Aconite Internet Solutions

FBI Advice

https://securityledger.com/2015/10/fbis-advice-on-cryptolocker-just-pay-the-ransom/

Joseph R. Bonavolonta
ASAC Counterintelligence/ Cyber/Tech/Security FBI Boston
Joseph R. Bonavolonta reported as Assistant Special Agent in Charge (ASAC) with the Boston Division of the Federal Bureau of Investigation (FBI) on October 1, 2013.

Mr. Bonavolonta is responsible for oversight of the Cyber/Counterintelligence/Technical Program/Security Branch.
http://cybersummitusa.com/2015/08/joseph-r-bonavolonta/

- At Cyber Security Summit 2015 in Boston, Joseph Bonavolonta, an assistant special agent with FBI stated that the FBI advises companies that fall victim to hacks involving Cryptolocker, Cryptowall or other forms of ransomware to pay the ransom
- Noting that while the agency has their back, "***the ransomware is that good***," the Security Ledger quoted Bonavolonta as saying.
- "***To be honest, we often advise people just to pay the ransom" because efforts by the Bureau to defeat the encryption used have proved futile.***"

http://www.scmagazine.com/cheaper-easier-for-hacked-businesses-to-pay-ransom/article/449489/

©2017 - Cormac Callanan, Aconite Internet Solutions

Europol and Checkpoint

https://www.europol.europa.eu/publications-documents/ransomware-what-you-need-to-know

- Ransomware software have been found to have bugs in the encryption tool.
- Decryption tools are sometimes available
- Professional implementation and and high infection rate
  - Locky, CryptXXX, Torrentlocker, Jigaw, Cerber, Crysis
- No More Ransom (NMR) launched in July 2016 project has more than 30 new partners from both the public and private sectors.

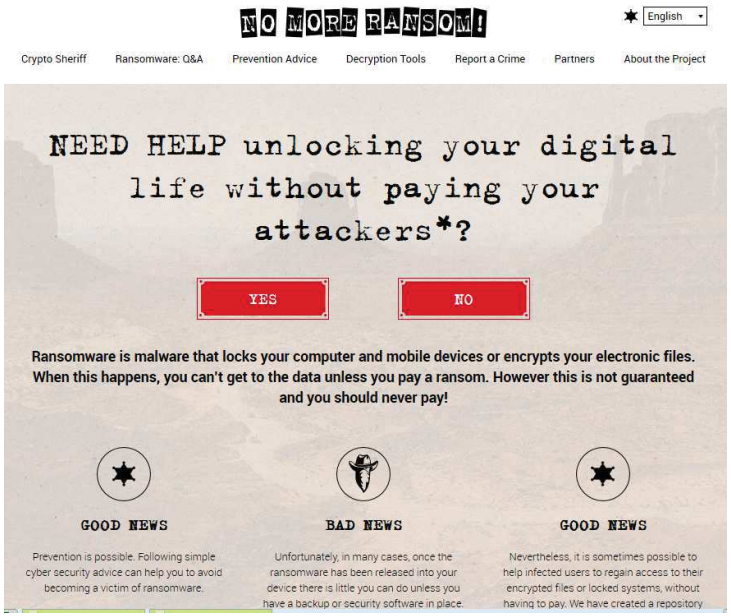
©2017 - Cormac Callanan, Aconite Internet Solutions

No More Ransom

https://www.europol.europa.eu/newsroom/news/no-more-ransom-new-partners-new-decryption-tools-new-languages-to-better-fight-ransomware

- No More Ransom (NMR) was launched in July 2016 project by the Dutch National Police, Europol, Intel Security and Kaspersky Lab
- More than 30 new partners from both the public and private sectors.
- Online portal is now available not only in English, but also in Dutch, French, Italian, Portuguese and Russian.
- 40 decryption tools have been added to nomoreransom.org.
- Nearly 6000 people were able to successfully decrypt their devices without having to pay criminals to do so

©2017 - Cormac Callanan, Aconite Internet Solutions



©2017 - Cormac Callanan, Aconite Internet Solutions

©2017 - Cormac Callanan, Aconite Internet Solutions

Advice

https://www.europol.europa.eu/newsroom/news/no-more-ransom-new-partners-new-decryption-tools-new-languages-to-better-fight-ransomware

- Always have a back-up system in place so a ransomware infection can't destroy your personal data forever
- use robust antivirus software to protect your system from ransomware but don't take for granted that your computer's anti-virus software is a guarantee against intrusions.
- Cover your webcam when not in use.
- keep all the software on your computer up to date
- Don't open attachments without independently verifying that they were sent from someone you know. Literally trust no-one, as any account can be compromised

©2017 - Cormac Callanan, Aconite Internet Solutions

- If your computer has been compromised and you are receiving extortion threats, don't be afraid to talk to your parents or to call law enforcement.

©2017 - Cormac Callanan, Aconite Internet Solutions

Questions?

Cormac Callanan
CEO, Aconite Internet Solutions

email: cc@aconite.com gsm: +353-87-257 7791

©2017 - Cormac Callanan, Aconite Internet Solutions

ACONITE
INTERNET SOLUTIONS

Cormac Callanan
Aconite Internet Solutions

SEXTORTION & RANSOMWARE

Co-funded by the Justice Programme of the European Union 2014-2020

©2017 - Cormac Callanan, Aconite Internet Solutions

ACONITE
INTERNET SOLUTIONS

Aspects of Sextortion

- Use of intimate sexual material to blackmail or extort financial benefit
- Includes
  - Attacks against systems using password cracking or spear phishing
  - Exfiltration of personal intimate documents
  - Blackmail
  - Payment

©2017 - Cormac Callanan, Aconite Internet Solutions

ACONITE
INTERNET SOLUTIONS

FBI

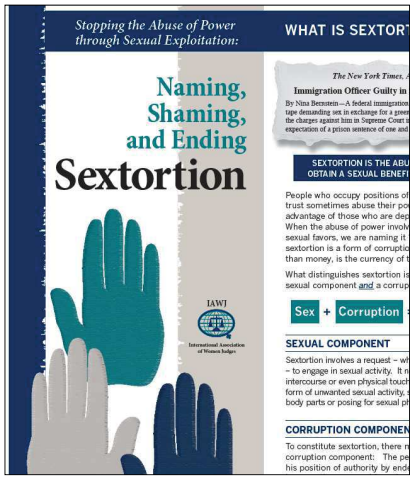
https://archives.fbi.gov/archives/losangeles/press-releases/2013/glendale-man-who-admitted-hacking-into-hundreds-of-computers-in-sextortion-case-sentenced-to-five-years-in-federal-prison

- "Sextortion" is a type of extortion or blackmail of a victim who is usually asked for a nude image.
- The perpetrator typically threatens to publicly release a nude image unless a victim performs a sexual act or complies with other demands.

©2017 - Cormac Callanan, Aconite Internet Solutions

ACONITE
INTERNET SOLUTIONS

What is Sextortion?



http://www.iawj.org/IAWJ_Sextortion_brochure.pdf

- A form of sexual exploitation that employs non-physical forms of coercion by threatening to release sexual images or information to extort sexual favours from the victim.
(Collins Dictionary)

©2017 - Cormac Callanan, Aconite Internet Solutions

ACONITE
INTERNET SOLUTIONS

2010 - Keith Hudson (39)/ Tyler Schrier (23)
docket number 2:11-cr-01175-SJO, USA v. Schrier, filed in the Central District of California

CASE STUDY: POKER PLAYERS

©2017 - Cormac Callanan, Aconite Internet Solutions

ACONITE
INTERNET SOLUTIONS

The crime

http://arstechnica.com/tech-policy/2013/04/how-the-fbi-cracked-a-sextortion-plot-against-pro-poker-players/

- Hotmail account of professional poker player Joe Sebok hacked - a tournament pro with almost $1.9 million in winnings
- Copies of sexually explicit images featuring Sebok (stored there as attachments) were copied
- Sebok was contacted and repeatedly asked for different sums of cash so the images would not be published. Sebok did not comply
- Extortionist released two images to key people in the poker community
- Extortionist claimed he was helping out an online acquaintance
  - a college student and poker fanatic named Tyler Schrier, who had provided the login

©2017 - Cormac Callanan, Aconite Internet Solutions

ACONITE
INTERNET SOLUTIONS

18 October 2010

Joe Sebok
http://www.thepokerpractice.com/poker/joe-sebok-nude-photos-extortion-plot

- Joe Sebok found himself locked out of his Hotmail account twice within two hours.
- He reset the password each time and regained access.
- He thought nothing of it until the first e-mail arrived from `stankylaggg@gmail.com` at `7:23pm` with the subject of "Amanda's Sex Stories"
- It asked Sebok if he wanted to "buy" back the pictures he had taken with a former girlfriend.
- Another e-mail arrived at 7:30, a third at 7:33, with more rolling in at 7:35, 7:39, 7:42, 7:45, 7:46, 7:48, 7:52, and 7:58. Eleven more would arrive during the evening.

©2017 - Cormac Callanan, Aconite Internet Solutions

ACONITE
INTERNET SOLUTIONS

Extortion

- Stankylaggg eventually asked Sebok to switch to instant messenger, where the extortionist had created the account "just4kicksbrah" to chat with his target.
- "*You are going to pay me 60k initially then you are going to pay me 5k every year... the 5k every year will show that I have motivation to never reveal the pictures. … If not ill just post the pics.*"
- Sebok sent no money, despite his promises.
- The extortionist continued blitzing Sebok with e-mails and instant messages and expanded his circle of contacts to include Sebok's former girlfriend Amanda and her new boyfriend, who was also a pro poker player.

©2017 - Cormac Callanan, Aconite Internet Solutions

Industry Disclosure

Trinity College Hartford Connecticut http://www.trincoll.edu/AboutTrinity/Pages/default.aspx

- 26th October 2010
  Microsoft gave information on every IP address which recently accessed Sebok's Hotmail account.
- Google provided similar information on the `stankylaggg@gmail.com` account.

- Most IP addresses clearly belonged to Sebok, but several stood out—including one that resolved to Trinity College, a small private school in Connecticut.
- Though the account creator had signed up with a bogus name, the "originating IP address" used to register the account resolved to Trinity College.

©2017 - Cormac Callanan, Aconite Internet Solutions

Investigation

FBI Photo - Schrier's room during the search (with Schrier at left).
https://arstechnica.com/tech-policy/2013/04/how-the-fbi-cracked-a-sextortion-plot-against-pro-poker-players/2/

- FBI sent subpoena to Trinity, which assigned a static IP address to each particular student device using the campus network.

- 3rd November 2010
  Trinity College Disclosed to FBI that IP addresses in question were assigned to computer 041e64fd3a80—and that computer belonged to one Tyler Schrier (23 yo)

©2017 - Cormac Callanan, Aconite Internet Solutions

Extortion

- Friday 5 November 2010
  Extortionist sent two photos from Sebok's collection to 100 people in the poker world, including many who worked with Sebok
- The images ended up on a well-known poker blog, where a reader submitted them
  - *"Some dude hacked [Sebok's] hotmail and found very graphic emails and one very revealing pic! i bet your wondering how i got it right? well it wasn't too hard cuz the dude emailed it to like 100 bigtime poker pros, pretty much anyone who's email he had! i cant believe this hasn't been posted anywhere yet so I thought hey, this would be a great first post here!"*

©2017 - Cormac Callanan, Aconite Internet Solutions

Convictions

- An incessant sms texter, Schrier had taken no precautions in using his phone and had a large collection of messages relating to the extortion.
- 26th January 2011
  LA FBI office obtained a warrant to search the phone, and the contents were significant.
  - Schrier 42 months in prison
  - Hudson got 24 months
- A third person was also charged with the extortion crimes - 22-year-old Ryder Finney pleaded guilty to conspiracy and is set to receive his sentence later this year in Philadelphia.

©2017 - Cormac Callanan, Aconite Internet Solutions

Making things worse

- Schrier was released on a $50,000 appearance bond put up by his father.
- 4 October 2012
  Schrier broke into another victim's Hotmail account and obtained his online poker account login information.
- 22 October
  Schrier hit another Hotmail account and from there another online poker account.
- Two victims lost > $4,000 balances in accounts.
- Hudson eventually admitted his part in the scheme, saying that he had accessed Sebok's e-mail account and sent the pictures to Schrier.

©2017 - Cormac Callanan, Aconite Internet Solutions

Victim Impact Statements

- Joe Sebok addressed the court and said the victims of the plot had "their lives altered and shattered in irreparable ways."
- "In short, I was no longer able to maintain my then-current level of participation in the poker industry, representing the brands that I had been previously, as well as greatly destroying my ability to do so with new companies moving forward.
- Without belaboring the point too much, it was a nightmare, and one that I was forced to live through with millions of people watching." He was a professional poker player for five years, but his career took a hit when one of his poker contracts was terminated.

FBI - https://archives.fbi.gov/archives/losangeles/press-releases/2013/two-northern-california-men-in-sextortion-plot-targeting-professional-poker-players-receive-federal-prison-sentences

©2017 - Cormac Callanan, Aconite Internet Solutions

http://arstechnica.com/tech-policy/2013/01/internet-criminals-so-reliably-dumb-at-hiding-their-tracks/
https://archives.fbi.gov/archives/losangeles/press-releases/2013/glendale-man-who-admitted-hacking-into-hundreds-of-computers-in-sextortion-case-sentenced-to-five-years-in-federal-prison

KAREN "GARY" KAZARYAN (27)

©2017 - Cormac Callanan, Aconite Internet Solutions

Prosecutors wrote

Karen "Gary" Kazaryan, 27

http://www.nydailynews.com/news/national/california-sexual-cyber-terrorist-behind-bars-article-1.1542996

- "Kazaryan is a sexual cyber terrorist.
- He hacked into hundreds of victims' e-mail, Facebook, and Skype accounts using their usernames and passwords or password reset questions.
- He then methodically searched their accounts for naked pictures, passwords, and the contact information of their friends.
- He had two goals every time that he accessed these accounts: get more naked pictures in any way he could and get more victims."

©2017 - Cormac Callanan, Aconite Internet Solutions

Modus Operandi

- If found, the photos were then used to approach the account holders and blackmail them into making further displays, usually over Skype, to the watching hacker.
- If they didn't comply, the original photos might be posted to their Facebook page.
- Posed online as women and sent instant messages to their friends and persuaded the friends to remove their clothing so he could see and take photos of them
- Hacked email and social media accounts of 350 women
- According to FBI agents who searched his computer he obtained some 3,000 explicit images

©2017 - Cormac Callanan, Aconite Internet Solutions

Victims

- Obtained a topless photo of a woman in a hot tub from one victim's Facebook account, and two sisters
- Demanded that [victim 1] and [her sister, victim 2] take their tops off and show their breasts on the Skype camera or he would post the photos on their Facebook walls for all of their friends to see.
- The unknown person told [the sisters] they had 10 seconds to do this
- In retaliation for not complying within 10 seconds, the unknown person, without authorization, logged into [a friend of both girls'] Facebook account and added the [topless] photo of [victim 2] to [the friend's] Facebook wall.

©2017 - Cormac Callanan, Aconite Internet Solutions

Extortion

- The unknown person then instant messaged [the victim] on Skype and sent the link to Facebook with the compromising photo attached.
  - The link was [sic] the photos he had just put on their Facebook walls since they did not comply to his demands.
- They were crying and both then showed their breasts to the unknown person on Skype.
  - The unknown person said they did not show them for a long enough period of time and demanded that they do it again.
  - The girls again complied to his demand and he took the link to the photos off of their Facebook pages.

©2017 - Cormac Callanan, Aconite Internet Solutions

Extortion

- Kazaryan's computer held 3,000 photos of nude or semi-nude women, some seized from their own e-mail and Facebook accounts, some snapped from Skype chats like the one described above.
- More than 350 women may have been targeted.
- "His victims were devastated and felt like they had been raped," according to the sentencing memorandum. "They continue to be thoroughly traumatized by his criminal conduct."
- He would lock women out of their own online accounts

©2017 - Cormac Callanan, Aconite Internet Solutions

Industry Disclosure 27 December 2010

- Facebook's internal security team had wrapped up an investigation in which it simply pulled the IP addresses for everyone who had accessed the various victim accounts over the last two months, then correlated them.
- IP address 71.83.210.142 was common to each
- Facebook's team then searched for every account that had been logged into from 71.83.210.142
- Produced a new list of 176 different accounts
  - a large number of these accounts had recently been disabled due to hacking or had filed tickets with Facebook complaining about being hacked.
- the single most commonly accessed account from 71.83.210.142—and by a huge margin—was for one Karen Kazaryan

©2017 - Cormac Callanan, Aconite Internet Solutions

- the FBI ran Kazaryan's name through various database and quickly found that he lived in a Glendale, California apartment and had "*an arrest and pending trial for a rape charge in 2008*"
- Charter Communications confirmed that the 71.83.210.142 address was registered to the Glendale apartment owned by Kazaryan
- Sept 2013, Sentenced to five years in federal prison.

©2017 - Cormac Callanan, Aconite Internet Solutions

Case Study - Suicide Victim

AMANDA TODD

©2017 - Cormac Callanan, Aconite Internet Solutions

Suicide of Amanda Todd

http://en.wikipedia.org/wiki/Suicide_of_Amanda_Todd

- On 7 September 2012, Todd posted a 9-minute YouTube video entitled *My Story: Struggling, bullying, suicide and self-harm*, which showed her using a series of flash cards to tell of her experiences being bullied
- Todd writes that when she was in grade 7 (2009-2010) she used video chat to meet new people over the Internet and she received compliments on her looks.
- A stranger convinced Todd to bare her breasts on camera. The individual later blackmailed her with threats to expose the topless photo to her friends unless she gave a "show"

©2017 - Cormac Callanan, Aconite Internet Solutions

- During Christmas holidays in 2012 police informed her at 4:00 a.m. that the photo was circulating on the Internet.
- Todd wrote that she experienced anxiety, depression and panic disorder due to the experience.
- Her family moved to a new home, where Todd later stated that she began using drugs and alcohol.
- A year later, the individual reappeared, creating a Facebook profile which used the topless photograph as the profile image, and contacting classmates at her new school.
- On 10 October 2012 Todd was found hanged at her home

©2017 - Cormac Callanan, Aconite Internet Solutions

Advice

- Don't take for granted that your computer's anti-virus software is a guarantee against intrusions.
- Turn off your computer when you aren't using it.
- Cover your webcam when not in use.
- Don't open attachments without independently verifying that they were sent from someone you know.
- Be suspicious.
- If your computer has been compromised and you are receiving extortion threats, don't be afraid to talk to your parents or to call law enforcement.

©2017 - Cormac Callanan, Aconite Internet Solutions

FBI Advice

https://archives.fbi.gov/archives/losangeles/press-releases/2013/glendale-man-who-admitted-hacking-into-hundreds-of-computers-in-sextortion-case-sentenced-to-five-years-in-federal-prison

- To avoid become a victim, everyone should be prudent when posting images online or to any wireless communication (computer, phone, tablet), especially if the images have private or compromising content.
- Victims who receive extortionate threats or whose personal accounts have been compromised are urged to contact a parent, trusted adult, or law enforcement, since the situation will only worsen.
- As always, computer users are warned to ensure their passwords are difficult for others to guess, avoid opening unverified attachments, and use reliable anti-virus software with updated definitions. Lastly, computer users should cover their webcams when they are not in use.

©2017 - Cormac Callanan, Aconite Internet Solutions

©2017 - Cormac Callanan, Aconite Internet Solutions

Questions?

Cormac Callanan
CEO, Aconite Internet Solutions

email: cc@aconite.com gsm: +353-87-257 7791

Handling electronic evidence on mobile devices in courts – legal considerations

Tais Deus Ramos, prosecutor

The Life Cycle of E-Evidence
The Rise of Evidence on Mobile Devices
Madrid, 24-25 May 2017

ERA - Academy of European Law
Centro de Estudios Jurídicos, Madrid

Co-funded by the Justice Programme of the European Union 2014-2020

Outline

- Introduction
- Legal framework:
- Authenticity and Integrity
- Requirements according to procedural law
- Some examples
- Conclusions

Introduction

Some statistics at national level: criminal proceedings initiated in 2015 (according to statistics of the General Prosecutor's Office):

	TOTAL	%
Crimes against freedom (threats and coertion - 1009, bullying or harassment - 96)	1.105	4,9
Crimes against moral integrity	226	1,00
Pornography and corruption of minors -767, harassment of minors 98, other crimes against sexual freedom - 77	942	4,17
Crimes against privacy (including hacking of electronic systems and e-data - 220, discovery and disclosure of secrets - 597)	817	3,61
Defamation and slander	254	1,13
Crimes against property (including frauds – 18.201, disclosure of business secrets - 276, crimes against broadcasting services -27, electronic damages - 295, crimes against intellectual property - 70)	18.869	83,58
Counterfeiting	193	0,85
Discrimination	40	0,18
Other offences	129	0,57
TOTAL	22.575	100,00

Legal framework

- Do we have a legal definition of e-evidence?
  - The case of Spanish Criminal Procedural law: there is no definition of "E-evidence", or evidence in electronic support. However, "electronic documents" can be assimilated to "documents" (according to the definition in the Criminal Code and the Civil Procedural Law), and provisions relating to electronic files and electronic documents as evidence are included in the Civil Procedural Law.

- What are the main rules used by Spanish Courts to assess e-evidence ?
  - Free assessment of evidence
  - "Evidence contained in telematic supports or obtained through them, will be **as valid and effective as an original document**, if its **authenticity**, **integrity**, and the observance of the **requisites established by procedural laws are guaranteed**" (STS 1066/2009, 4 November)

- In particular, printed messages:
  - "Evidence of a bidirectional communication through any of the various instant messaging systems must be tackled very cautiously. The **possibility of manipulation** of the digital data (…) is part of the reality of things. The anonymity that these systems allow and the free creation of accounts with a false identity, make it perfectly possible to feign a conversation in which an only user speaks to himself. For this reason, **the challenge of the authenticity of any of these conversations**, when these are introduced in the process through printed files, **shifts the burden of proof** to the party that defends the suitability of the evidence. It will be necessary in this case to call an expert witness to identify the **real origin of the communication**, the identity of the **speakers** and, finally, the **integrity of the contents**" (STS 300/2015, 19 May)

  - **However**, challenging the authenticity of the conversation may not make it useless, when there is other evidence that supports the authenticity and integrity of the document – importance of the **assessment of the evidence as a whole.**

Authenticity and Integrity

- Collection of evidence
  - Evidence collected by the police in the course of a judicial investigation vs. evidence provided by the victim / witnesses / the defendant
  - Judicial intervention required when fundamental rights are involved

- The assessment of authenticity and integrity
  - Intervention of expert witness
  - Metadata as evidence
  - Intervention of the court secretary

- Other issues:
  - Cooperation with internet service providers – the use of MLA instruments
  - The preservation of associated data after Judgment CJEU 21 December 2016 (Joined Cases C-203/15 and C-698/15)

Requirements according to procedural law

- Respect for fundamental rights
  - Privacy rights and the need of judicial authorization
  - Example: regulation by the Spanish Procedural Law
  - The problem with personal / business messages

- Respect for procedural rules
  - How do we introduce e-evidence in the judicial process? (Most cases: printed copy with certification by the Court Secretary; when possible, the electronic support is also needed)

Some examples

- Intervention of email communications in real time and its difficulties
- The value of Whatsapp state as evidence
- Facebook's "like" as a means to breach a restraining order
- Emails and geolocation
- Business mails and privacy
- Stalking and mobile devices
- Child abuse and social media

Conclusions

- Necessity of a definition of e-evidence
- Standard of proof – necessity of more precise rules
- At the same time, we must not forget that e-evidence must be assessed as a whole with the rest of evidence
- Special training for judges / prosecutors is still needed

Thank you for your attention

Tais Deus Ramos
tais.deus@fiscal.es