DEALING WITH ELECTRONIC EVIDENCE

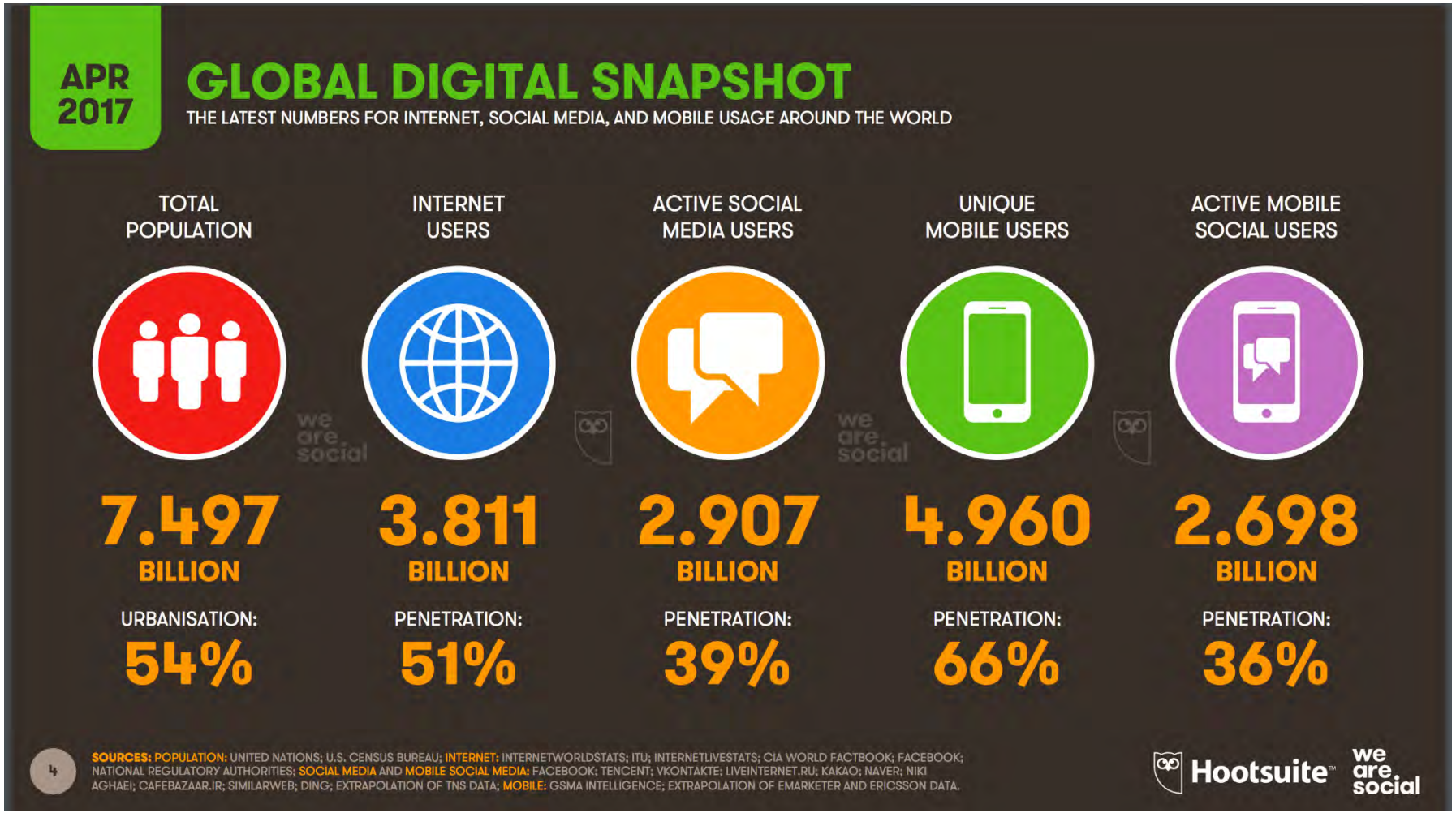
BY: JUDGE RAINELDA H. ESTACIO-MONTESA
PRESIDING JUDGE – RTC BRANCH 46, MANILA

SESSION OBJECTIVES

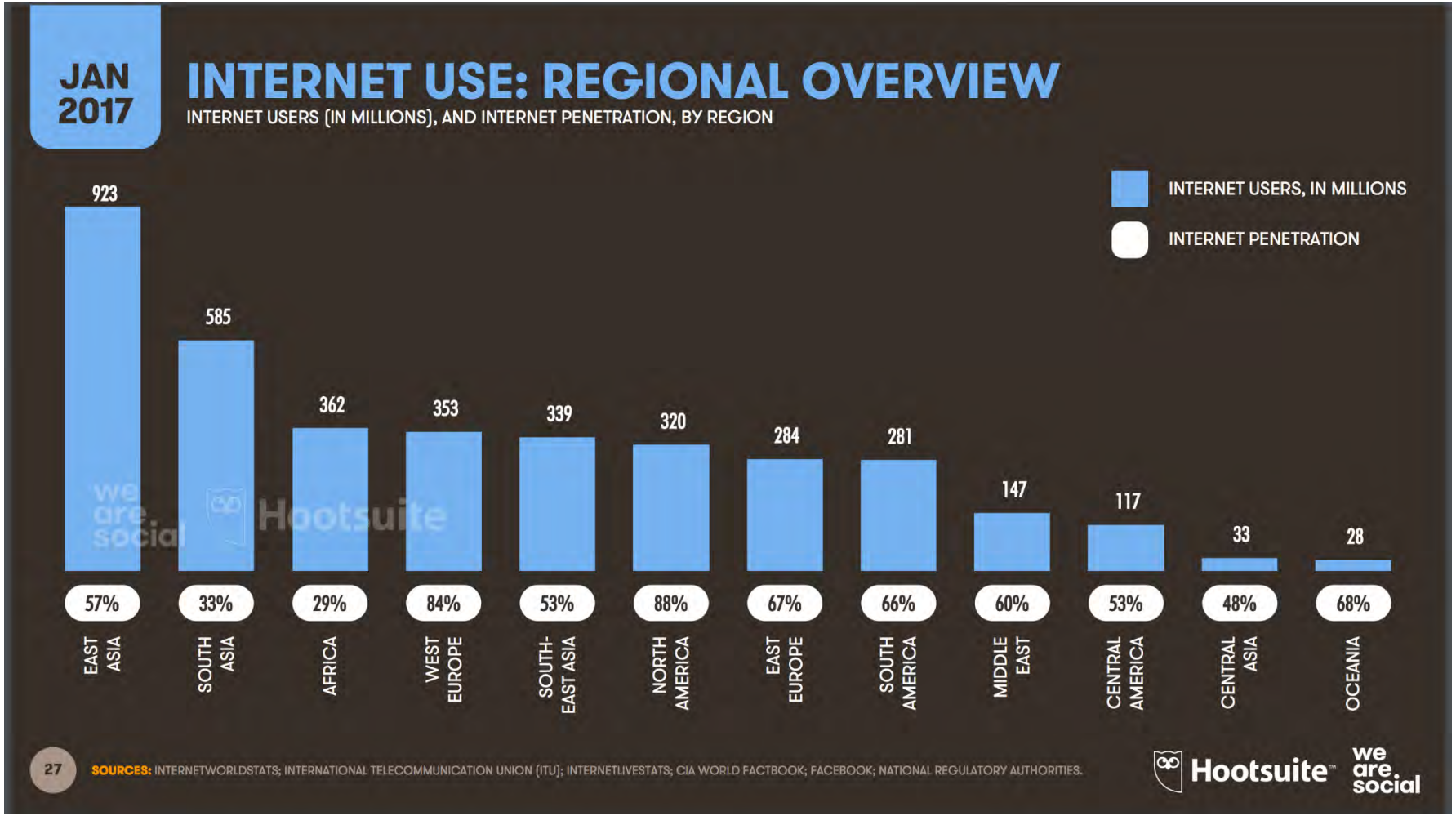
- Discuss principles relating to electronic evidence
- Identify which evidence falls under the Rules on Electronic Evidence
- Present electronic evidence in court

INTERESTING FACTS

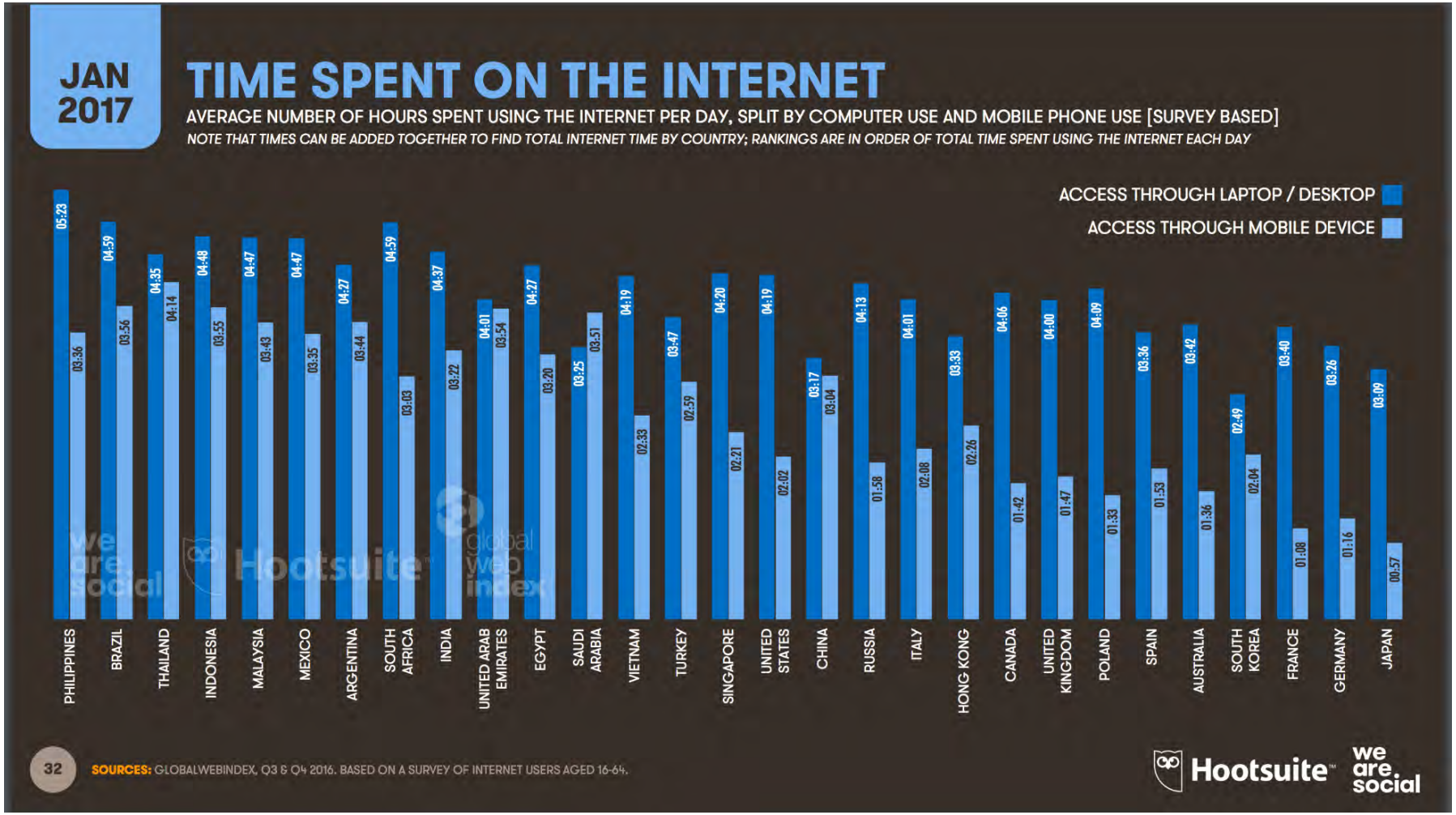
GLOBAL DIGITAL SNAPSHOT



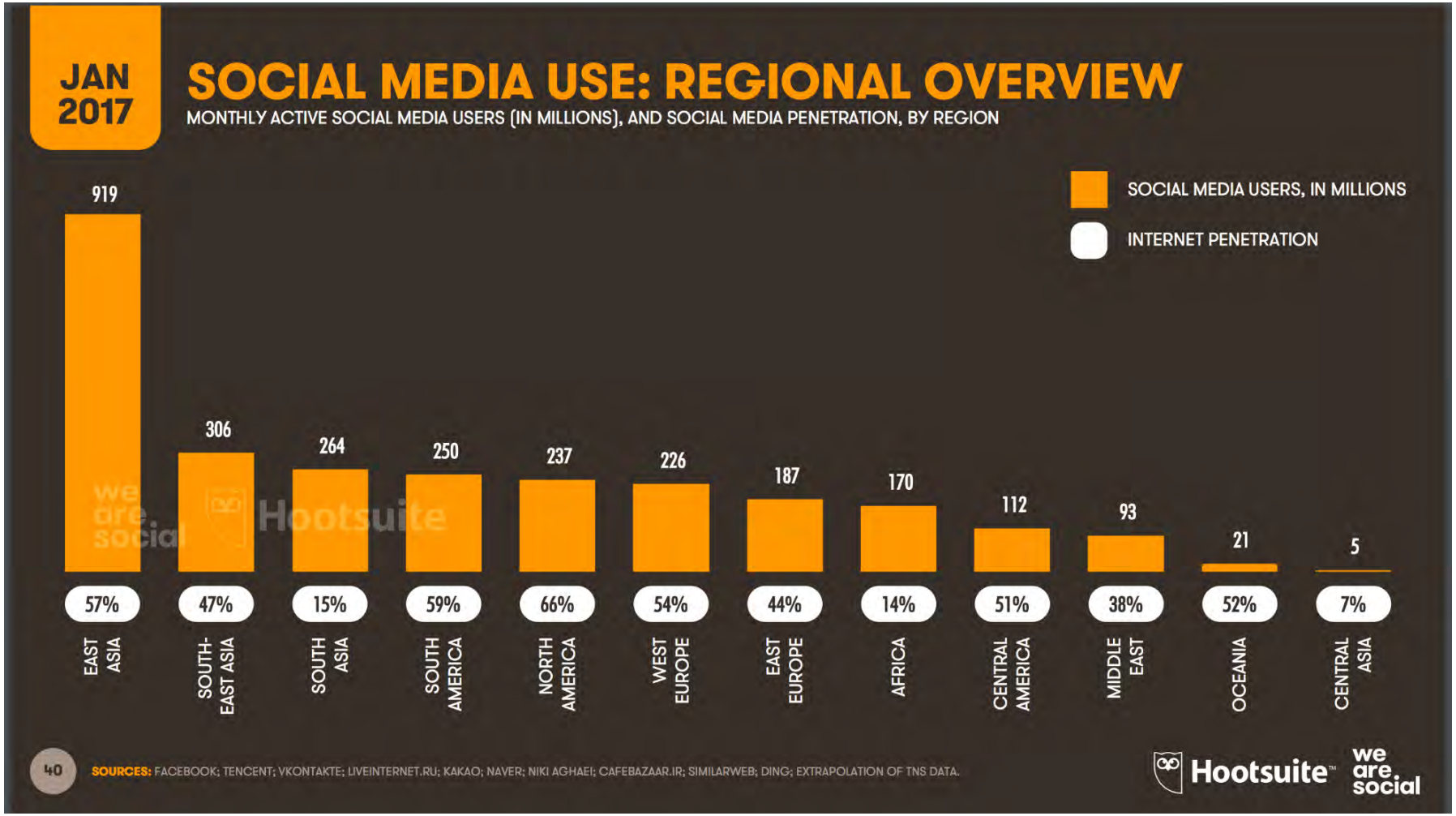
INTERNET USE: REGIONAL OVERVIEW



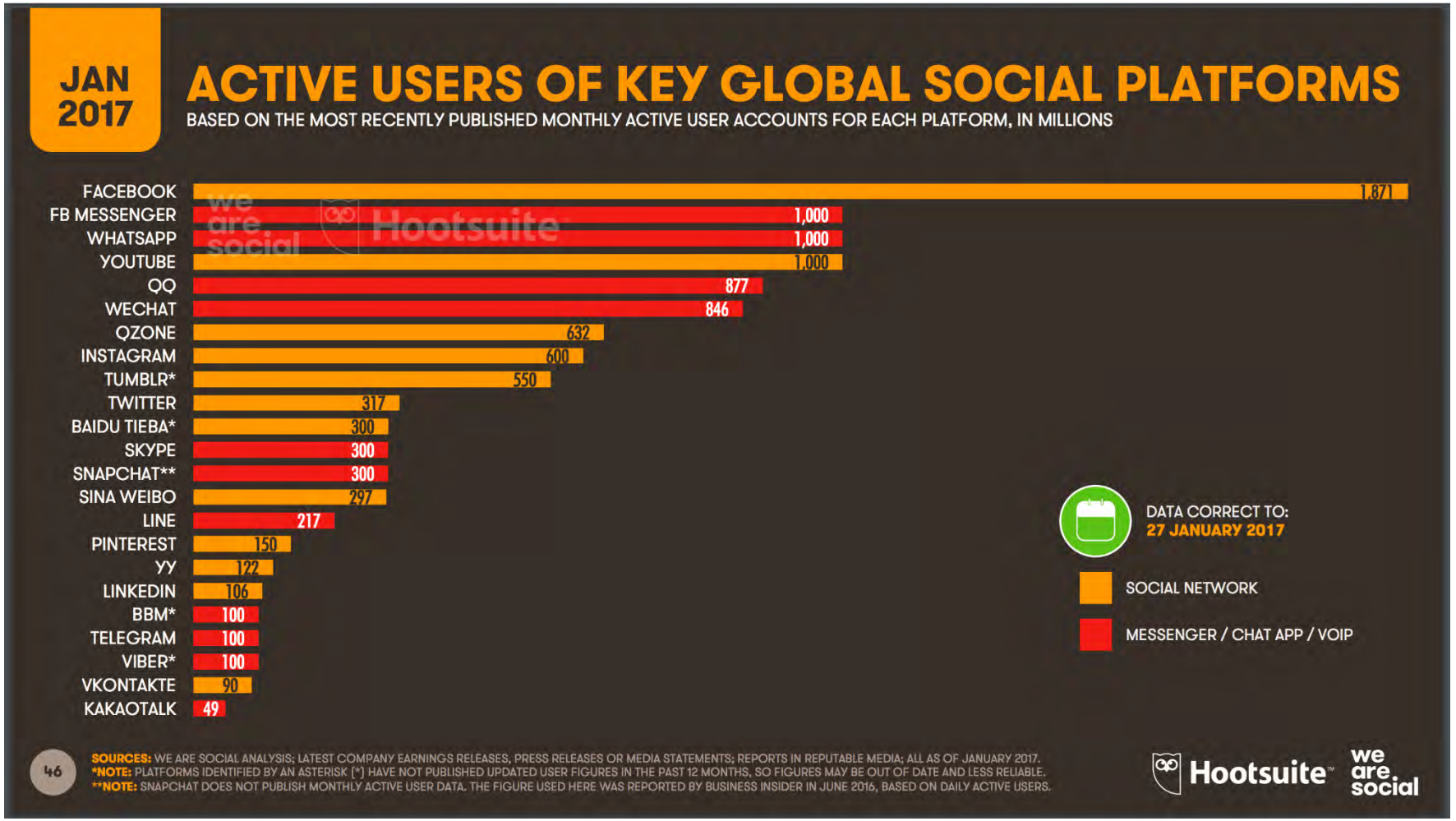
TIME SPENT ON THE INTERNET



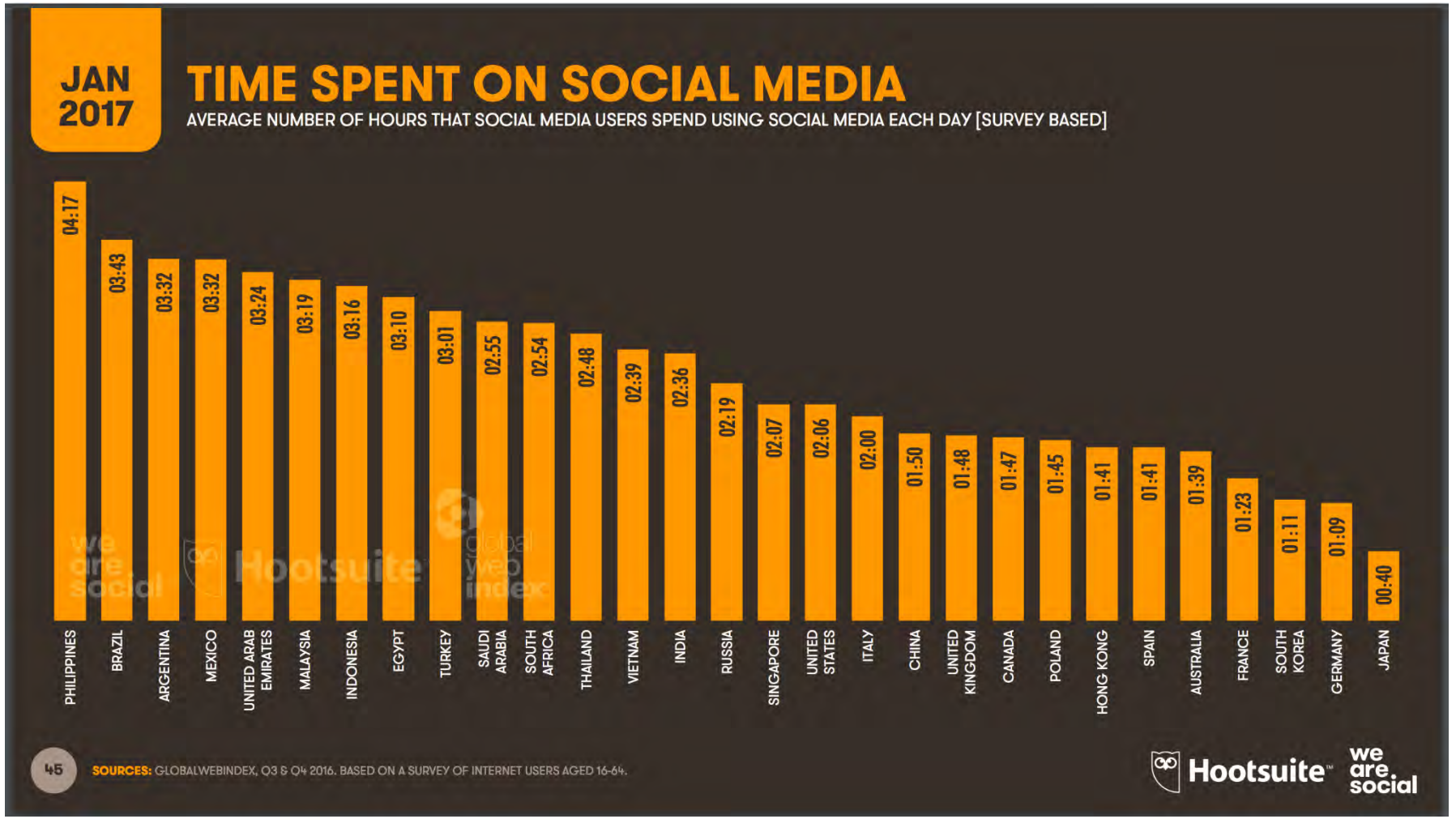
SOCIAL MEDIA USE: REGIONAL OVERVIEW



ACTIVE USERS BY PLATFORM



TIME SPENT ON SOCIAL MEDIA



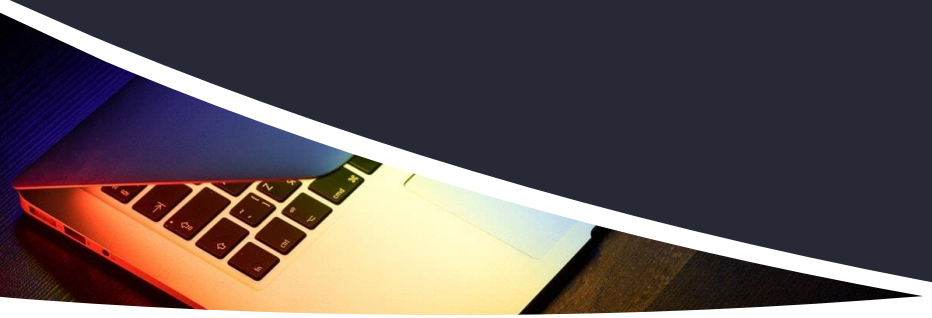
SOME INTERESTING FACTS AND REALITIES

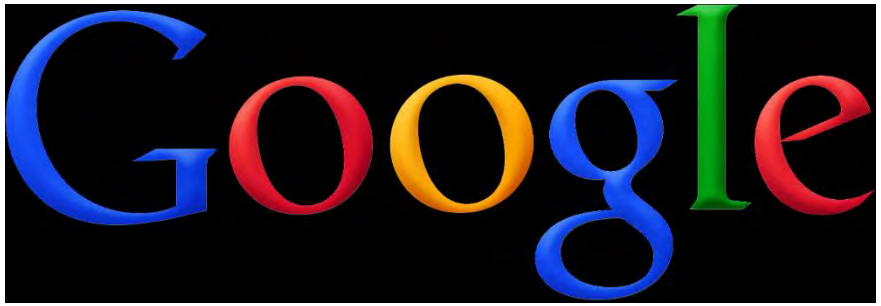
- 2.13 Billion Users
- 68 hours a month
- 33.97% are Filipinos

SOME INTERESTING FACTS AND REALITIES

- 500 Million tweets per day

SOME INTERESTING FACTS AND REALITIES

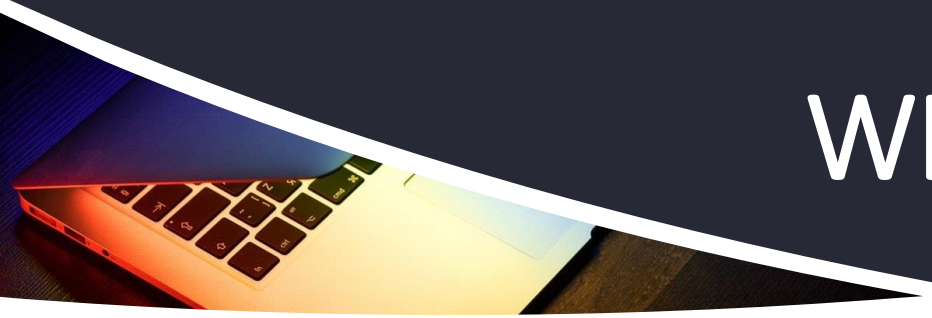




- Google Searches
- 1999 – 15M searches
- 2018 - 106,127,500,000 searches

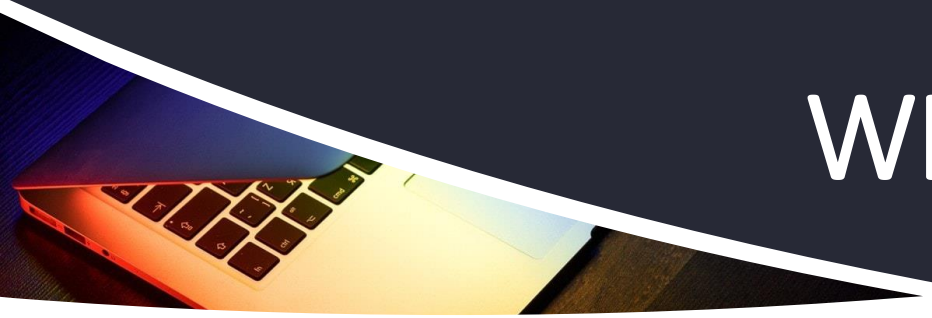
SOME INTERESTING FACTS AND REALITIES

- **FILIPINOS TOP THE LIST OF SOCIAL MEDIA USERS**
  - **9 Hours and 29 Minutes per day**



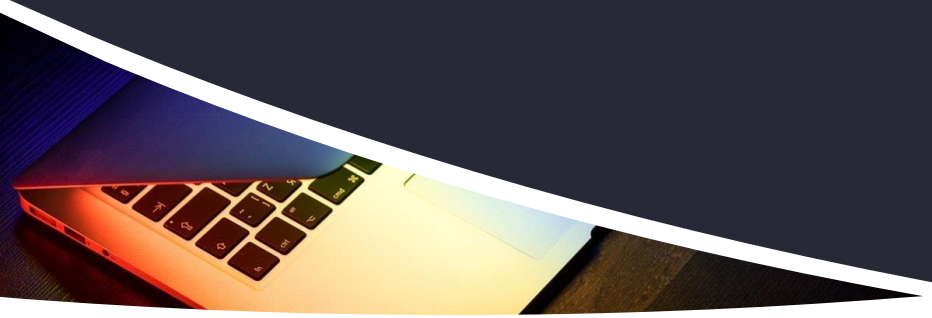
WHAT IS ELECTRONIC EVIDENCE?

- It is any information, generated, stored or transmitted in digital form that may later be needed to prove or disprove a fact disputed in legal proceedings.



WHAT IS ELECTRONIC EVIDENCE?

- Electronic evidence is no different from traditional evidence in that the party introducing it into legal proceedings must be able to demonstrate that it reflects the same set of circumstances and factual information as it did at the time of the offense.



CHARACTERISTICS OF ELECTRONIC EVIDENCE

- It is invisible to the untrained eye
- It is highly volatile
- It may be altered or destroyed through normal use
- It can be copied without degradation

COMPUTERS = DIGITAL DEVICES

- Each 0 or 1 is a BIT (for BINARY DIGIT)

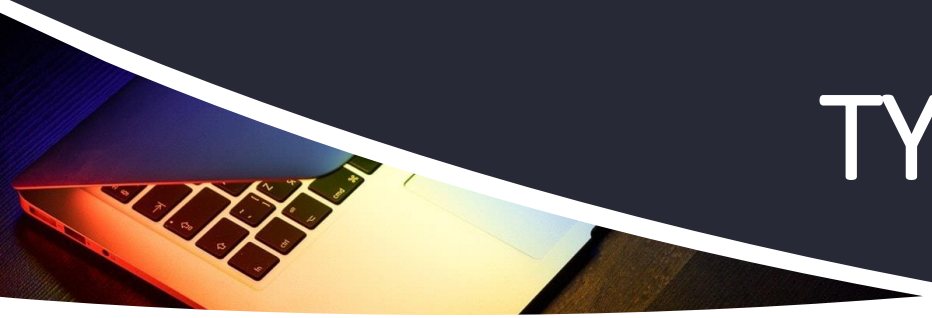
  0 0 0 0 0 0 0 1 = 1

  0 0 0 0 0 0 1 0 = 2 (2+0)

  0 0 0 0 0 0 1 1 = 3 (2+1)

- An 8-bit sequence = 1 byte = a keystroke

  0 1 0 0 0 0 0 1 = A



TYPES OF ELECTRONIC EVIDENCE

- Human Generated
  - Record or data created by some human action that is stored electronically
    - Emails
    - Web sites
    - Chat Contents
    - Comments on Social Media
    - Customer complaints
    - Subscriber information
    - Word processing documents
    - Digital photos

TYPES OF ELECTRONIC EVIDENCE

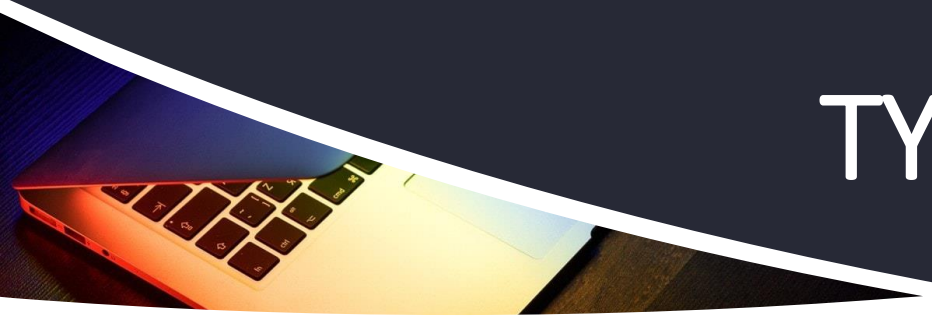
- Computer-generated Evidence
  - Output of a computer program designed to process input following a defined algorithm
  - Human involvement is limited to the creation of the program or action triggering creation of record

    - FTP Transfer Logs
    - Webmail IP logs and records
    - IP logs from ISPs
    - Operating System Logs/Registry Files
    - Toll records
    - Cell Tower and Face Data
    - GPS records

TYPES OF ELECTRONIC EVIDENCE

- Hybrid computer and human generated evidence:
  - Most electronic evidence has computer and human generated components
    - IRC chat logs with time stamps
    - Email contents with computer generated headers
    - Word processing document with metadata

TYPES OF ELECTRONIC EVIDENCE



Header information (sending address, IP and time stamp) may be computer generated

To: Harry the Hacker <Harry42@webmail.com>
From: Connie the Counterfeiter
<conniefielder666@gmail.com>
Subject: new project?

Have an idea that will make us lots of $$. Need you to code. If you are in, come to IRC – I'm talking to BH now.

XOXO,
Connie

Human generated

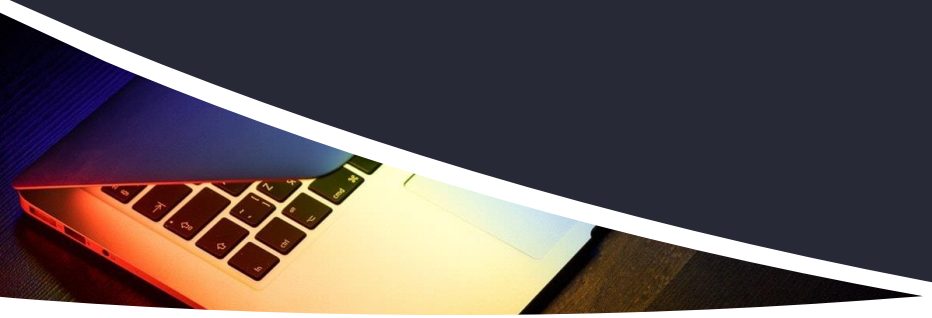
WHERE DIGITAL EVIDENCE CAN BE FOUND

- Desktops
- Laptops
- Servers
- External Media

RULES ON ELECTRONIC EVIDENCE

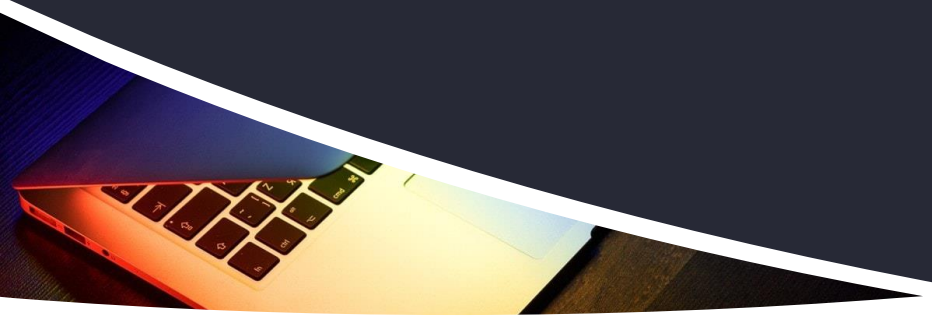
A.M. NO. 01-7-01-SC

- 17 July 2001
  - SC *En Banc* approves **Rules on Electronic Evidence** ("REE")
- 01 August 2001
  - REE went into effect.
- 24 September 2002
  - SC expanded REE's coverage to include criminal cases (A.M. No. 01-07-01)



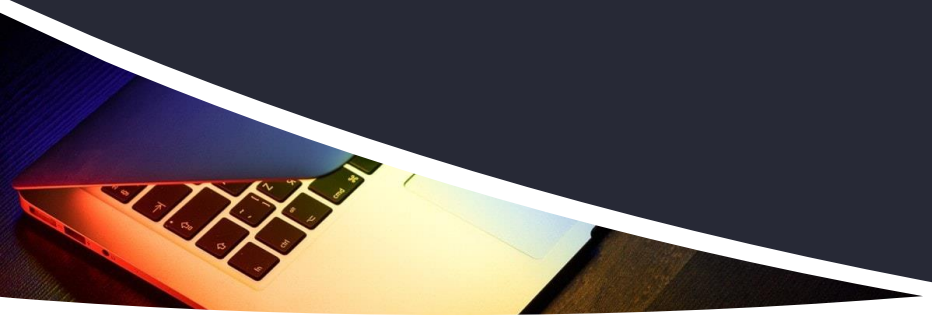
SCOPE / COVERAGE OF REE

- Apply to presentation of electronic documents
- Audio, photographic, video and ephemeral evidence



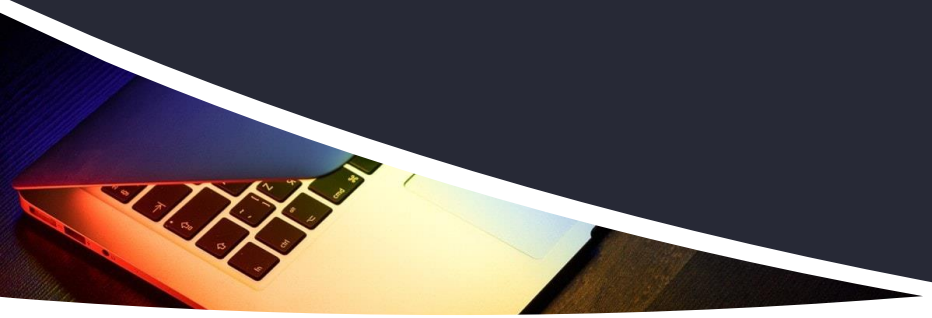
SCOPE / COVERAGE OF REE

- Cases covered:
  - Civil cases / proceedings
  - Quasi-judicial proceedings
  - Administrative proceedings
  - Criminal proceedings (per SC A.M. No. 01-07-01, 24 September 2002)



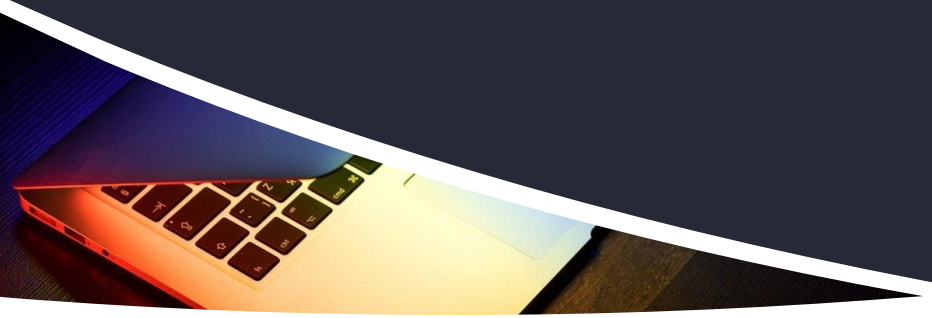
SCOPE / COVERAGE OF REE

- In the case of **Ang v. Pascua** (G.R. No. 182835, 20 April 2010), the SC said that the REE does not apply to criminal actions. In this case, the accused, charged under R.A. 9262 (Violence against Women & Children Act), was questioning the admissibility of a text message as electronic evidence.



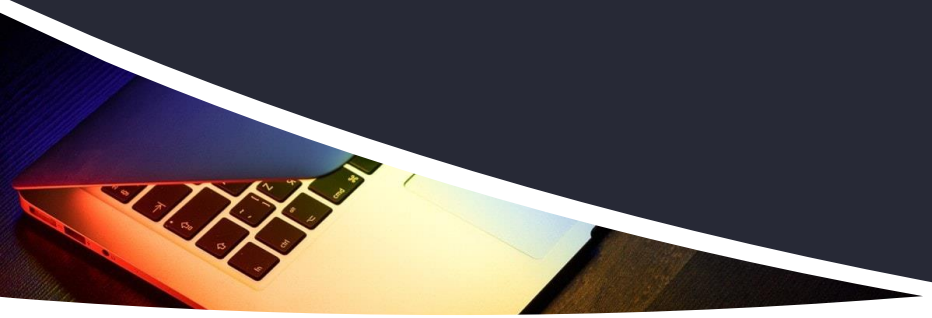
SCOPE / COVERAGE OF REE

- But in the case of **People v. Enojas** (G.R. No. 204894, **10 March 2014**), the SC acknowledged the application of Rules on Electronic Evidence to criminal actions.



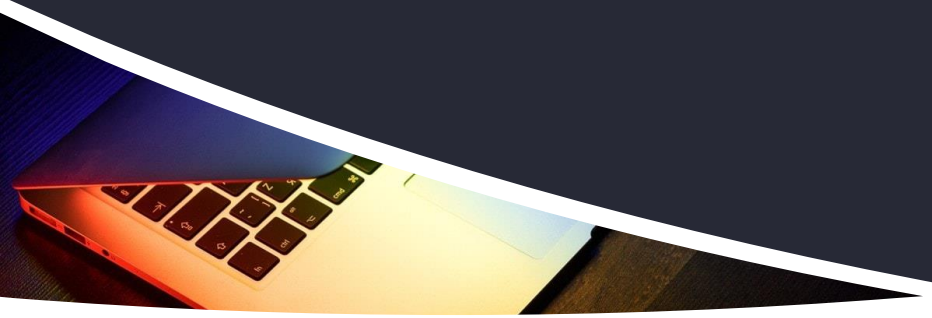
DEFINITION OF TERMS

- **Electronic Document –** refers to information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored processed, retrieved or produced electronically.



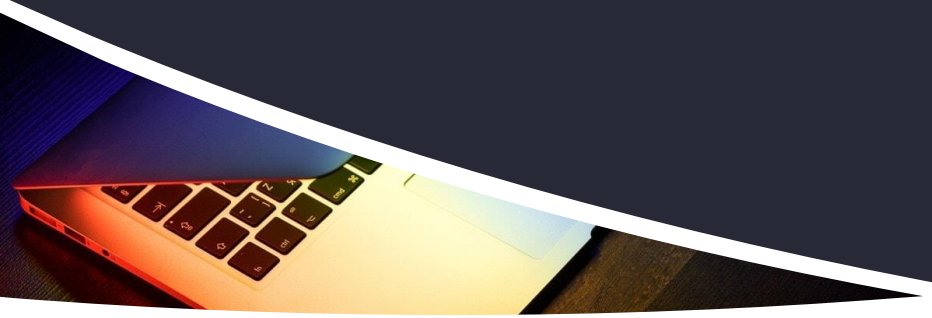
DEFINITION OF TERMS

- **Electronic Document –** includes digitally signed documents and any print-out or output, readable by sight or other means, which accurately reflects the electronic data message or electronic document.



DEFINITION OF TERMS

- **Ephemeral electronic communication** – refers to telephone conversations, text messages, chatroom sessions, streaming audio, streaming video, and other electronic forms of communication the evidence of which is not recorded or retained.



SCOPE / COVERAGE OF REE

- ***Nuez v. Cruz-Apao*** (A.M. No. CA-05-18-P, 12 April 2005)
  - the SC ruled that **SMS or text messages is a form of electronic evidence**, falling under the definition of "**ephemeral electronic communication**" under Sec. 1(k) of the REE.

FACTORS TO CONSIDER IN THE ADMISSIBILITY OF ELECTRONIC EVIDENCE IN LEGAL PROCEEDINGS

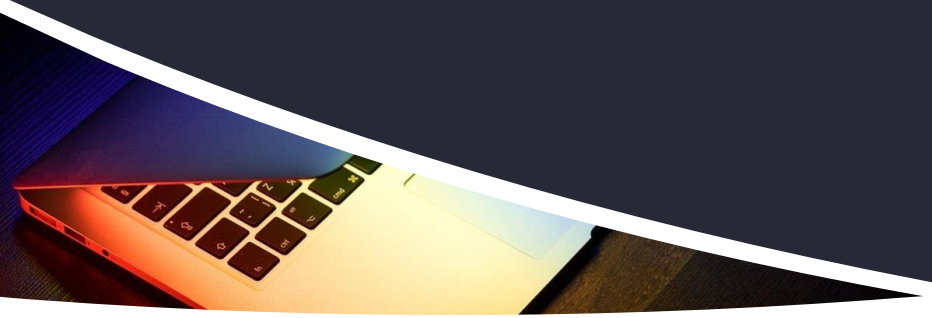
- **AUTHENTICITY**: The evidence must establish facts in a way that cannot be disputed and is representative of its original state.

- **COMPLETENESS**: The analysis of or any opinion based on the evidence must tell the whole story and not be tailored to match a more favourable or desired perspective.

- **RELIABILITY**: There must be nothing about the way in which the evidence was collected and subsequently handled that may cast doubt on its authenticity or veracity.

- **BELIEVABILITY**: The evidence must be persuasive as to the facts it represents and the finders of fact in the court process must be able to rely on it as the truth.

- **PROPORTIONALITY**: The methods used to gather the evidence must be fair and proportionate to the interests of justice: the prejudice (i.e. the level of intrusion or coercion) caused to the rights of any party should not outweigh the “probative value” of the evidence (i.e. its value as proof).



- **AUTHENTICITY :** is the recovered evidence same as the originally seized data?

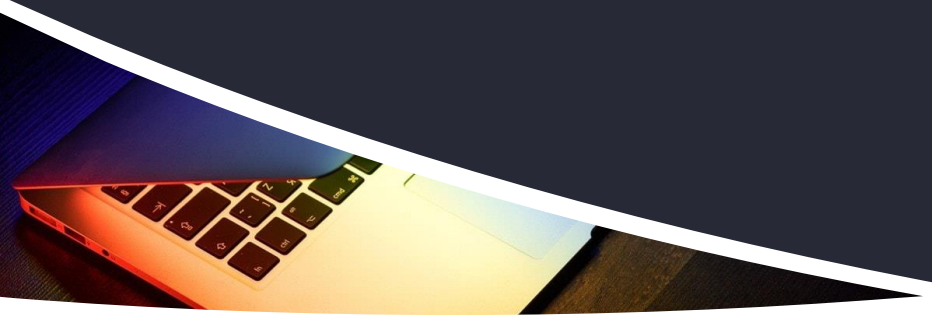
  - The evidence must establish facts in a way that cannot be disputed and is representative of its original state. To demonstrate that digital evidence is authentic, it is generally necessary **to satisfy the court that it was acquired from a specific computer and/or location, that a complete and accurate copy of digital evidence was acquired, and that it has remained unchanged since it was collected.**

- **Chain of custody and integrity documentation**
  - important for demonstrating the authenticity of electronic evidence. Proper chain of custody demonstrates that digital evidence was acquired from a specific system and/or location, and that it was continuously controlled since it was collected.

Susceptibility to alteration

- The intangible nature of any electronically stored information makes it susceptible to manipulation and more prone to alteration than traditional forms of evidence.

- Must always ensure that digital evidence is AUTHENTIC in order to be admissible



- **RELIABILITY:** Can the digital evidence be relied upon in court? Is the computer/computer program that generated the evidence reliable or was functioning normally? Is the digital evidence tampered?

  - There must be nothing about the way in which the evidence was collected and subsequently handled that may cast doubt on its authenticity or veracity. The reliability of particular computer system or process is difficult to assess and, in practice, courts are not well equipped to assess the reliability of computer systems or processes.

- **COMPLETENESS:** is the evidence the entire record or conversation?

  - The analysis of or any opinion based on the evidence must tell the whole story and not be tailored to match a more favorable or desired perspective.

ADMISSIBILITY

SECTION 2, RULE 3

- Requisites for Admissibility of Electronic Document:

1. Complies with the rules on admissibility;
2. Authenticated in the manner prescribed by the REE; and
3. Requirement of integrity / built-in modes of authentication

ADMISSIBILITY

CASE IN POINT

- **NAPOCOR v. Codilla** (G.R. No. 170491, 04 April 2007, the SC ruled whether photocopies of documentary evidence were admissible in evidence (in this case, the document contained manual signatures). The SC held that **a manual signature contained in a print-out or photocopy of documents cannot be considered as information electronically received, recorded, transmitted, stored, processed, retrieved, or reproduced**, as defined under the REE.

ADMISSIBILITY

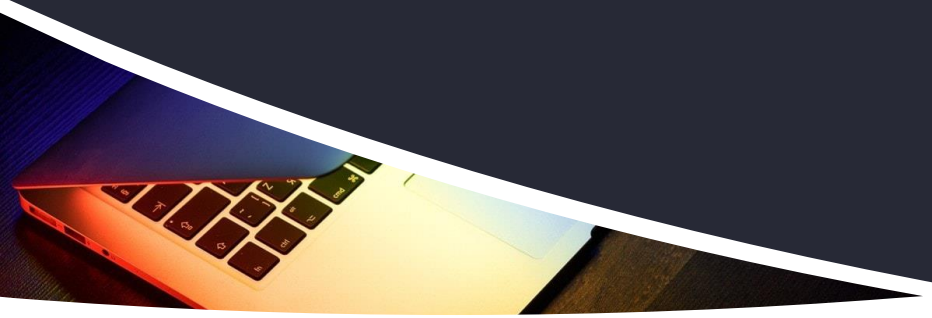
CASE IN POINT

- **MCC Industrial Sales Corporation v. Ssangyong Corporation** (G.R. No. 170633, 17 October 2007), the SC held that a facsimile transmission, by its very nature, is not admissible as electronic evidence since it cannot be considered an electronic document or electronic data message.

PROVING THE INTEGRITY OF AN ELECTRONIC EVIDENCE

WHAT IS A HASH VALUE?

- Digital fingerprint of the digital evidence
  - Hash value is relevant in proving the integrity of the evidence
  - Mathematical algorithm that calculates any amount of data that you put in ad runs into a math program like MD5 or SHA1 and produces a fixed output



PROVING THE INTEGRITY OF AN ELECTRONIC EVIDENCE

WHAT IS A HASH VALUE?

- An MD5 Hash is a 32 character string that looks like:
  - Acquisition Hash:

    3FDSJO90U43JIVJU904FRBEWH

    •Verification Hash:

    3FDSJO90U43JIVJU904FRBEWH

    •The chances of two different inputs producing the same MD5 Hash is greater than:

    1 in 340 Unidecillion: or 1 in 340,000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000,

EXERCISE

- Please look at the two documents:
  - Mail 11
  - Mail 11 (hash)

- Can you see any differences between the documents?

Mail11.doc

From: Otos Polaroidos <otos@ubp.co.nrl>

Sent: Thursday, September 28, 2017 5:55 PM

To: Artemida Olimpiakos cfo@fba.co.atls

Subject: Re: FBA – UBP printing deal

Att: Invoice

Dear Artemida,

Following previous e-mail, I'm sending you invoice. Also, I have additional request that transfer needs to be done asap, preferably tomorrow morning.

Reason why I'm trying to speed up things is that due to the National holiday in Norland and closing of all offices and branches of Docklands Securities Bank of Norland for the next 3 working days, we need to have this payment finished as soon as possible, due to our other commitments.

Please use following bank account details of UBP account in DSBN Ostland, which will over bridge this gap:

Docklands Securities Bank of Norland/Ostland branch

Account number 23568974

SWIFT UBPNRO26

IBAN NRLO2356897498653225589652 3

Although holiday starts very soon, I'll be reachable by mail if urgently needed.

Thank you for understanding.

Best regards,

Otos

UBP

MD5 HASH OF FILE MAIL11.DOC

b5d7a782e6e37df72beaffab61cf6db

Mail11 (hash).doc

From: Otos Polaroidos <otos@ubp.co.nrl>

Sent: Thursday, September 28, 2017 5:55 PM

To: Artemida Olimpiakos cfo@fba.co.atls

Subject: Re: FBA – UBP printing deal

Att: Invoice

Dear Artemida,

Following previous e-mail, I'm sending you invoice. Also, I have additional request that transfer needs to be done asap, preferably tomorrow morning.

Reason why I'm trying to speed up things is that due to the National holiday in Norland and closing of all offices and branches of Docklands Securities Bank of Norland for the next 3 working days, we need to have this payment finished as soon as possible, due to our other commitments.

Please use following bank account details of UBP account in DSBN Ostland, which will over bridge this gap:

Docklands Securities Bank of Norland/Ostland branch

Account number 23568974

SWIFT UBPNRO26

IBAN NRLO2356897498653225589652 3

Although holiday starts very soon, I'll be reachable by mail if urgently needed.

Thank you for understanding.

Best regards,

Otos

UBP

MD5 HASH OF 11TH MAIL (HASH).DOC

4358069e0c514e533356c1ada6701259


nigeljones — -bash — 102×24
Last login: Mon Oct 16 14:08:37 on ttys000
Nigels-iMac:~ nigeljones$ md5 /Users/nigeljones/Desktop/11th\ mail.docx
MD5 (/Users/nigeljones/Desktop/11th mail.docx) = b5d7a782e6e37df72beaffab61cf6dbb
Nigels-iMac:~ nigeljones$ md5 /Users/nigeljones/Desktop/11th\ mail\ \(hash\).docx
MD5 (/Users/nigeljones/Desktop/11th mail (hash).docx) = 4358069e0c514e533356c1ada6701259
Nigels-iMac:~ nigeljones$
b5d7a782e6e37df72beaffab61cf6dbb
4358069e0c514e533356c1ada6701259

WHAT DOES THIS MEAN?

- If handled correctly, electronic evidence is one of the best evidence types
  - There should be evidence at both ends of an email chain.
  - It can be checked against the original or the evidence image.
  - Judges can ask for any file to be checked.
  - Judges can ask how the evidence was collected and handled.
  - Emails have additional header information that can be checked.
  - IP addresses in emails can sometimes be checked.
  - Third party validation of evidence is preferable.

BEST EVIDENCE RULE

SECTION 1, RULE 4

- An electronic document shall be regarded as the equivalent of an original document under the Best Evidence Rule if:

1) Any printout or other output;
2) Readable by sight or by other means; and
3) Shown to reflect the data accurately (Sec. 1, Rule 4).

AUTHENTICATION OF ELECTRONIC DOCUMENTS

SECTION 2, RULE 5

- Manner of authentication (any of the following means):
  - By evidence that it had been **digitally signed** by the person purported to have signed the same;
  - By evidence that other appropriate **security procedures or devices** as may be authorized by the Supreme Court or by law **for authentication** of electronic documents were applied to the document; or
  - By **other evidence** showing its integrity and reliability to the satisfaction of the judge.

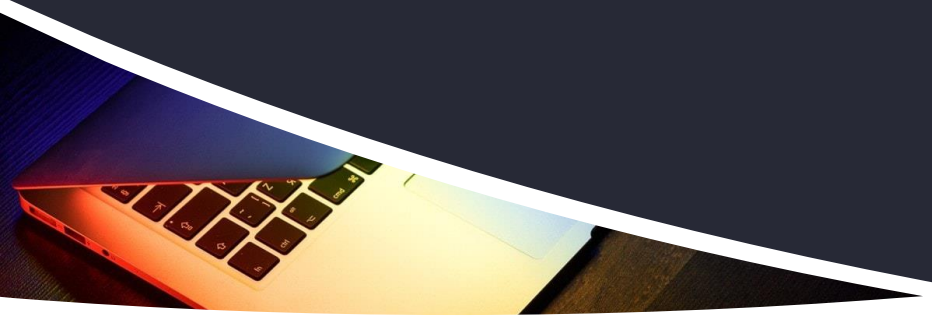
AUTHENTICATION OF ELECTRONIC DOCUMENTS

- In the case of **Aznar v. Citibank** (G.R. No. 164273, 28 March 2007), the Supreme Court ruled that to show the integrity and reliability of a private electronic document under Sec. 2(c), Rule 5 of the REE, one must demonstrate how the information reflected in a **computer print-out** was generated and how said information could be relied upon as true.

CHALLENGES IN DEALING WITH ELECTRONIC EVIDENCE

TECHNICAL / LEGAL CHALLENGES

PRACTICAL CHALLENGES



TECHNICAL CHALLENGES

I. Search and seizure issues

- There is a persisting question on whether the information stored electronically is covered by the **plain view doctrine** or do law enforcement agencies need a search warrant to examine such data, when the electronic devices containing such information is already covered by a search warrant.

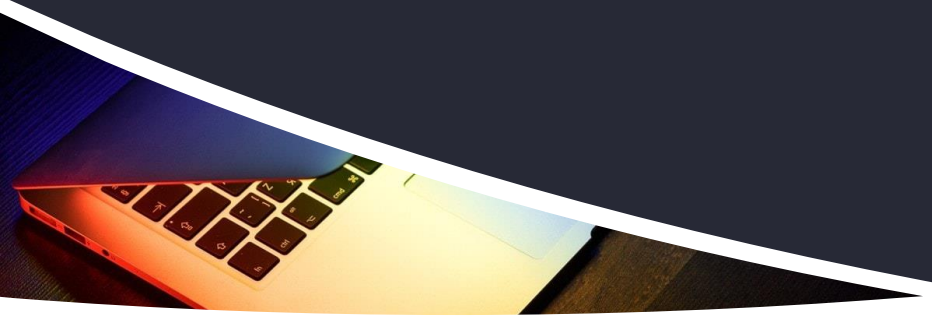
II. Susceptibility to alteration

- The intangible nature of any electronically stored information makes it susceptible to manipulation and more prone to alteration than traditional forms of evidence.
- Must always ensure that digital evidence is AUTHENTIC in order to be admissible
- Issues on admissibility

III. Issues on Jurisdiction and Conflict of Laws Situation and International Cooperation

- How to courts obtain evidence which are outside their jurisdiction and are governed by existing local laws?

- What law shall be applied if data the needs to obtained and later presented as evidence are stored elsewhere



- Swift and reliable international cooperation is essential in securing documents where ESP’s are based in a foreign country

- Documents secured thru MLA’s undergo authentication mechanisms and are coursed thru Central Authorities established among states

(Microsoft vs United States case)

THANK YOU!

neldamontesa@yahoo.com