Digital Forensics

Dott. Bruno Cesena

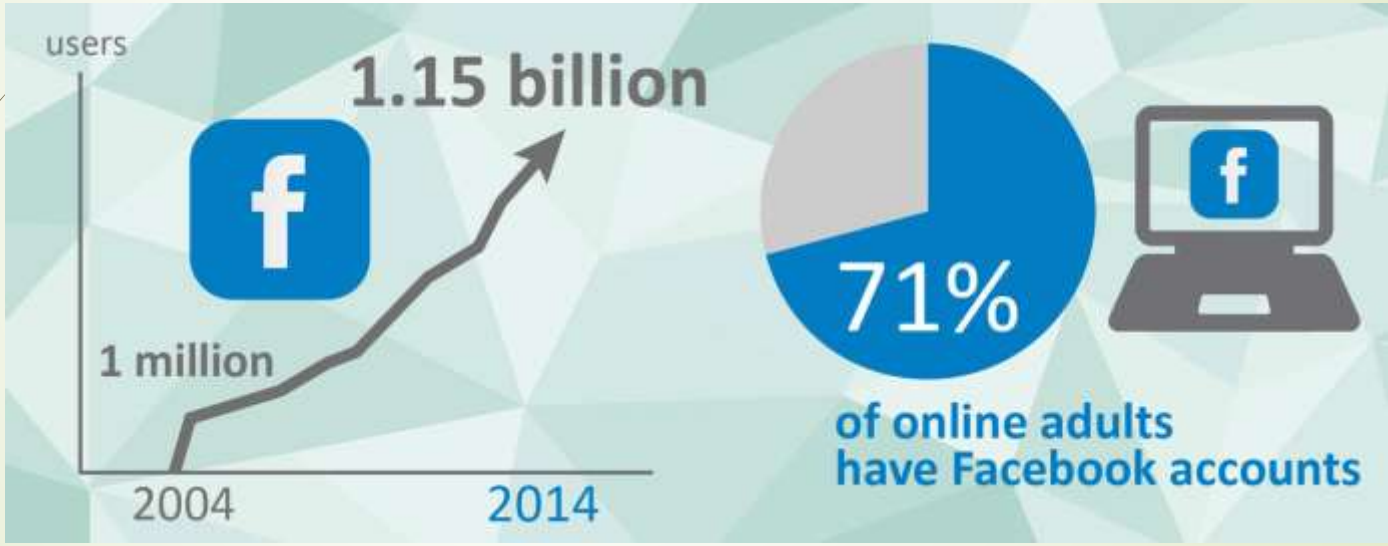
Crime areas

- Crime-as-a-Service
- Malware
- Child sexual exploitation online
- Payment fraud
- Criminal finances online
- Crimes relating to social engineering
- Data breaches and network intrusions
- Vulnerabilities of critical infrastructure

Cybercrime stats (iocta 2014)

Cybercrime stats (iocta 2014)

Cybercrime stats (iocta 2014)



Cybercrime stats

3,059,741,441 Internet Users in the world	**1,195,753,044** Total number of Websites	**173,649,345,268** Emails sent today
3,343,266,658 Google searches today	**3,071,556** Blog posts written today	**601,211,325** Tweets sent today
6,735,157,666 Videos viewed today on YouTube	**121,698,986** Photos uploaded today on Instagram	**122,235,929** Tumblr posts today
1,363,445,862 Facebook active users	**866,780,019** Google+ active users	**330,062,021** Twitter active users
59,352,025 Pinterest active users	**116,842,571** Skype calls today	**39,007** Websites hacked today

SPAM

Motivation	Scam Type	Modus Operandi
Money	Advance fee	Pay money to get money e.g. Nigerian letters, lottery, inheritance…
	Advertisement	Buy fake-/-non-existent goods, often medication
	Dating	Send money to cover medical care, flights or visa
	Investment	Invest into non-existent/fraudulently valued companies and pump and dump schemes
	Employment	Pay upfront administration fees for a falsely promised service and/or become a money mule
	Friend in need	Send money to a friend in need whose email, twitter or social network account has been hacked
	Charity	Contribution to an unregistered charity
Sensitive Information	Phishing	Disclose exploitable information, such as credentials e.g. banking scam, tax scam, raffles
Malware	Malicious website or application	Click the malicious link. A friend's message, adult content, fake virus alerts and breaking news are particularly effective to attract victims' attention

Trends

1. Mobile Threats Become More Sophisticated and Pervasive
   - The worldwide smartphone market reached a new milestone in 2013 with one billion units shipped in a single year for the first time, up 38% from the 725m units shipped in 2012
   - Malicious and high-risk apps are overwhelmingly programmed for Android devices. Although a few do exist for other platforms and more have been promised, Android's popularity and open platform make it likely to remain the focus of malicious app developers for some time yet.
2. Bitcoin's Popularity Makes it a Target for Theft and New Fraud Currencies Emerge Forcing Cybercrime Activity Further Underground

exchange at 31-3-2015 1B= 228.46 Euro

Trends

2. Bitcoin's Popularity Makes it a Target for Theft and New Fraud Currencies Emerge Forcing Cybercrime Activity Further Underground

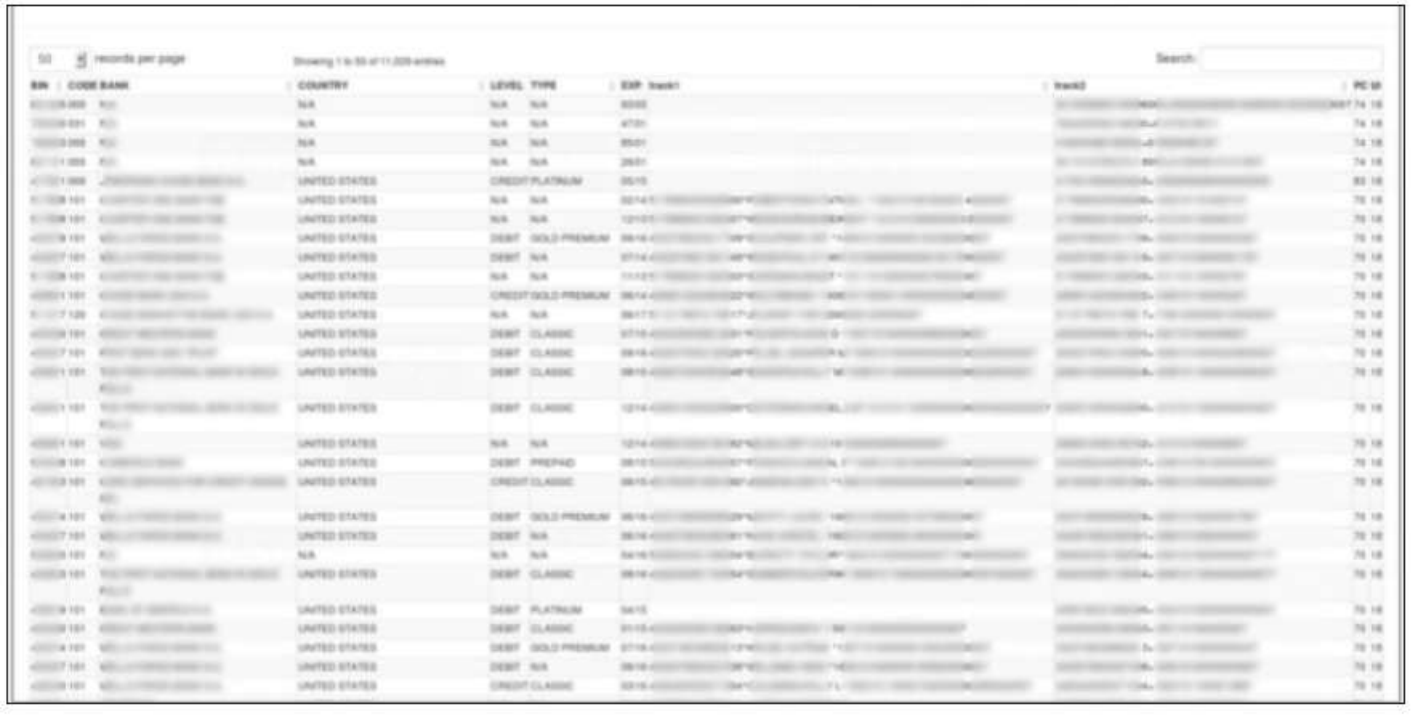
- Gaming outlets, and retailers including Overstock and Zynga, accept it as a valid payment method.
- In August 2013, the German government recognized it as a legal private currency and even imposed a tax on it.
- Chinese and Russian governments banned Bitcoin transactions over fears of money laundering, funding terrorism or tax evasion

exchange at 31-3-2015 1B= 228.46 Euro

Trends

3. Malware Gets More Sophisticated, APT Attacks Remain Unabated and POS Malware Attacks Become Common

- POS malware to referral abuse, cybercriminals are continually in search of new approaches to monetize their bots. At the same time they seek to spawn new attacks, they are also creating more



Trends

4. User Authentication Will be Redefined by Mobile
   - Consumers create multiple digital identities requiring them to remember multiple passwords.
   - Major password breaches made headlines throughout 2013, compromising tens of millions of passwords, user IDs, email addresses and other personal information.
   - according to the 2013 Verizon Data Breach Investigations Report, over 75% of attacks leveraged weak or stolen credentials.

Crimes in Italian Penal Code

- Documenti informatici (art. 491 bis c.p.)
- Falso (materiale e ideologico) in documenti informatici (da 476 al 493 bis c.p.)
- Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis e ter c.p.)
- Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.)
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.)
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.)
- Intercettazione non autorizzata (art. 617 quater, quinquies, sexies c.p.)
- Violazioni della riservatezza dei dati personali (D. Lgs. 196/03)

Some attacks (Eavesdropping)

Registrazione conclusa con successo !

Configura subito la tua connessione a Libero.
» Scarica il software per configurare automaticamente la connessione con il numero unico!
Ti consigliamo di stampare questa pagina e di conservare queste informazioni.

Riepilogo Dati Anagrafici

Nome: **aaaa**	Cognome: **bbbb**
Sesso: **M**	Data di nascita: **09/08/1934**
Provincia: **AG**	Privato/Azienda: **Privato** Telefono:

Per configurare la posta elettronica

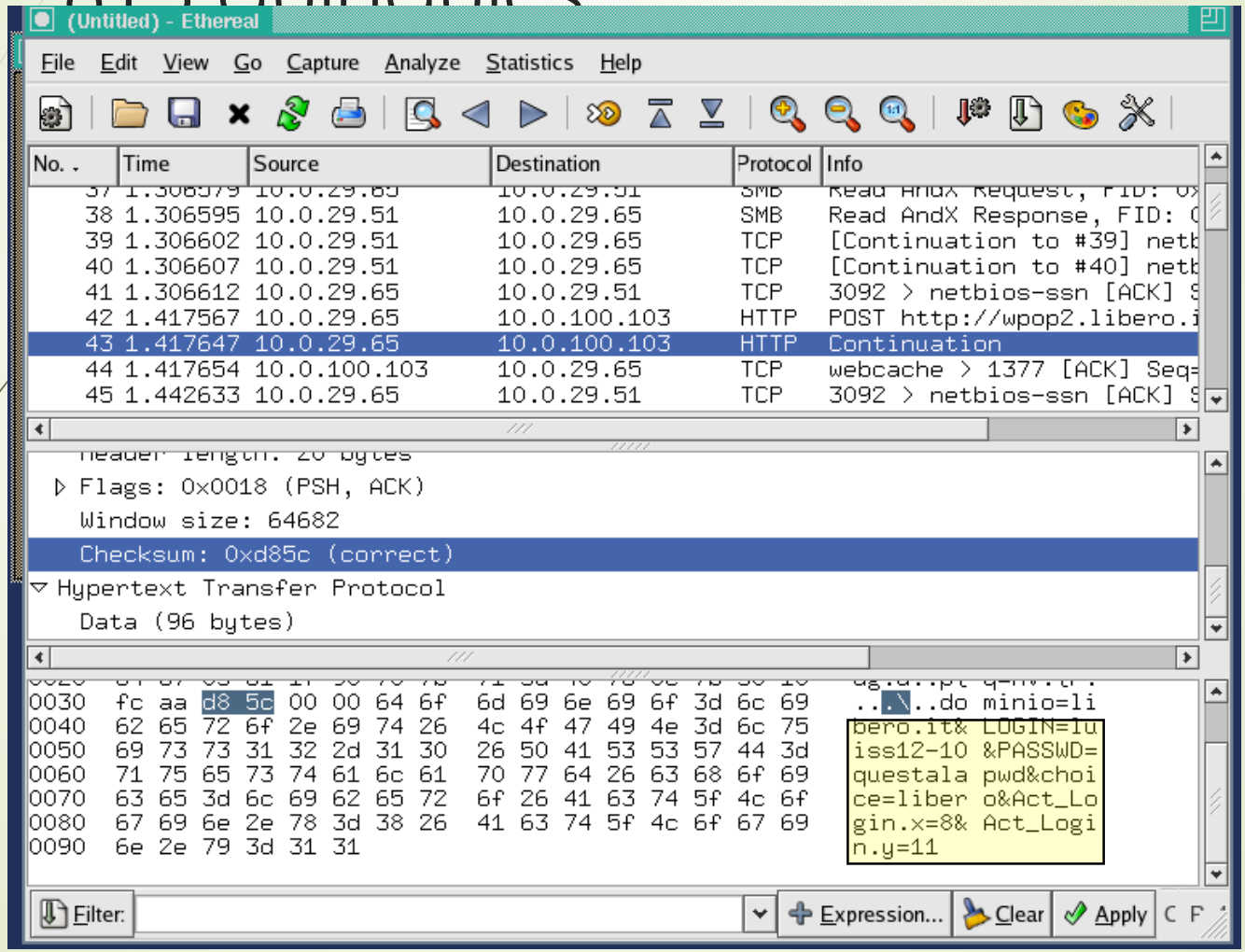
- E-mail: **luiss12-10@libero.it** (verrà attivata entro pochi muniti).
- Nome utente per leggere la posta: **luiss12-10**
- Password: **questalapwd**
- Indirizzo server di posta in entrata (POP3): **popmail.libero.it** oppure **imapmail.libero.it**
- Indirizzo server di posta in uscita (SMTP): **mail.libero.it**, oppure **"nome_server_provider"** qualora non fosse Libero il Provider fornitore della connettività
- Indirizzo server delle news: **powernews.libero.it**

Per configurare la connessione ad internet

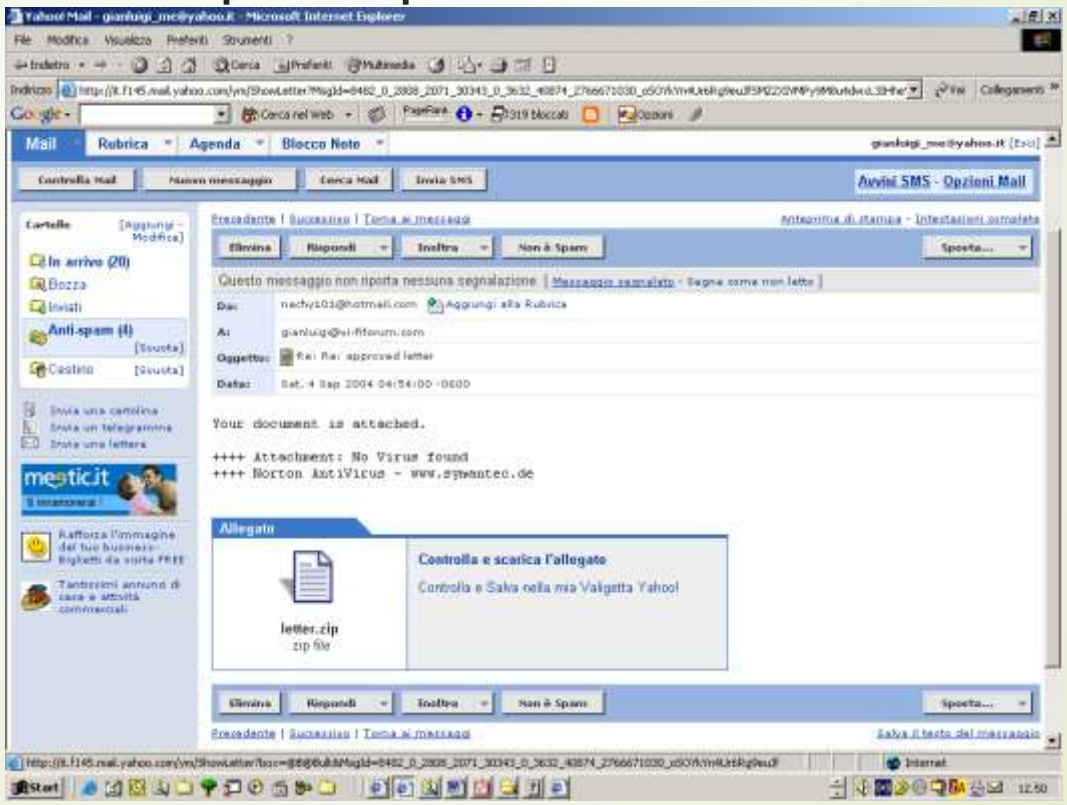
- USERNAME: **luiss12-10**
- PASSWORD: **questalapwd**
- Indirizzo IP: **assegnato dal server**
- Indirizzi DNS: **assegnati dal server**
- Durata dell'abbonamento: **illimitata**

Attenzione, ti ricordiamo che, per collegarti con Libero dovrai impostare lo Username completo, **luiss12-10@libero.it**, in caso contrario la tua chiamata verrà respinta.

Some Attacks (Eavesdropping) 615 quinquies



Some Attacks (Eavesdropping) 635 bis e ter, 615 quater/quinquies



PHISHING
615 ter, 617 sexies, 640 &ter , art. 167 D.lg. 196/2003,

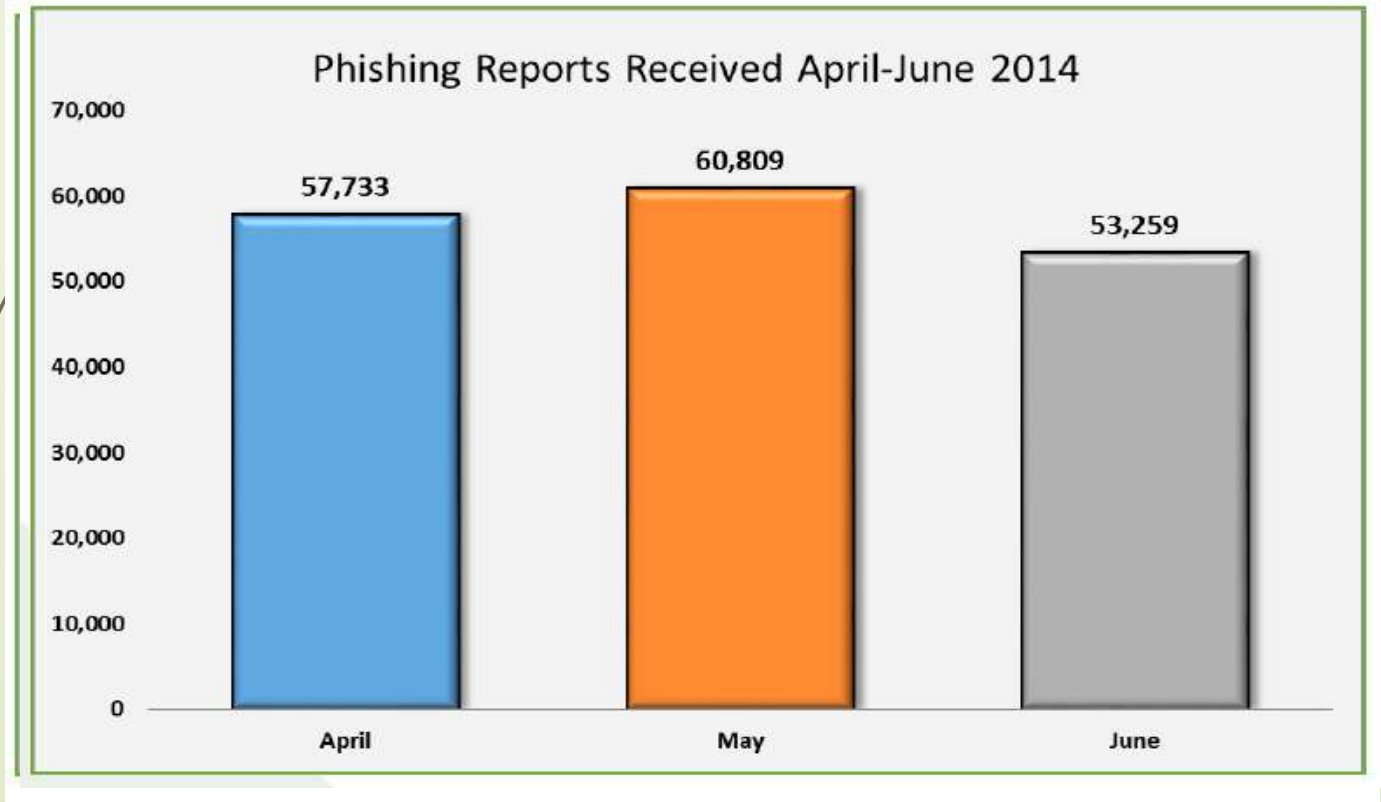
- In 2013, phishing alone resulted in $5.9 billion in losses to global organizations, and three in four data breaches were attributed to financial or fraud motives

Phishing (Social Engineering)

- Phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials.
- Social engineering schemes use spoofed e-mails purporting to be from legitimate businesses and agencies, designed to lead consumers to counterfeit websites that trick recipients into divulging financial data such as usernames and passwords.
- Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using systems to intercept consumers online account user names and passwords -- and to corrupt local navigational infrastructures to misdirect consumers to counterfeit websites (or authentic websites through phisher-controlled proxies used to monitor and intercept consumers' keystrokes).

Phishing (Social Engineering)

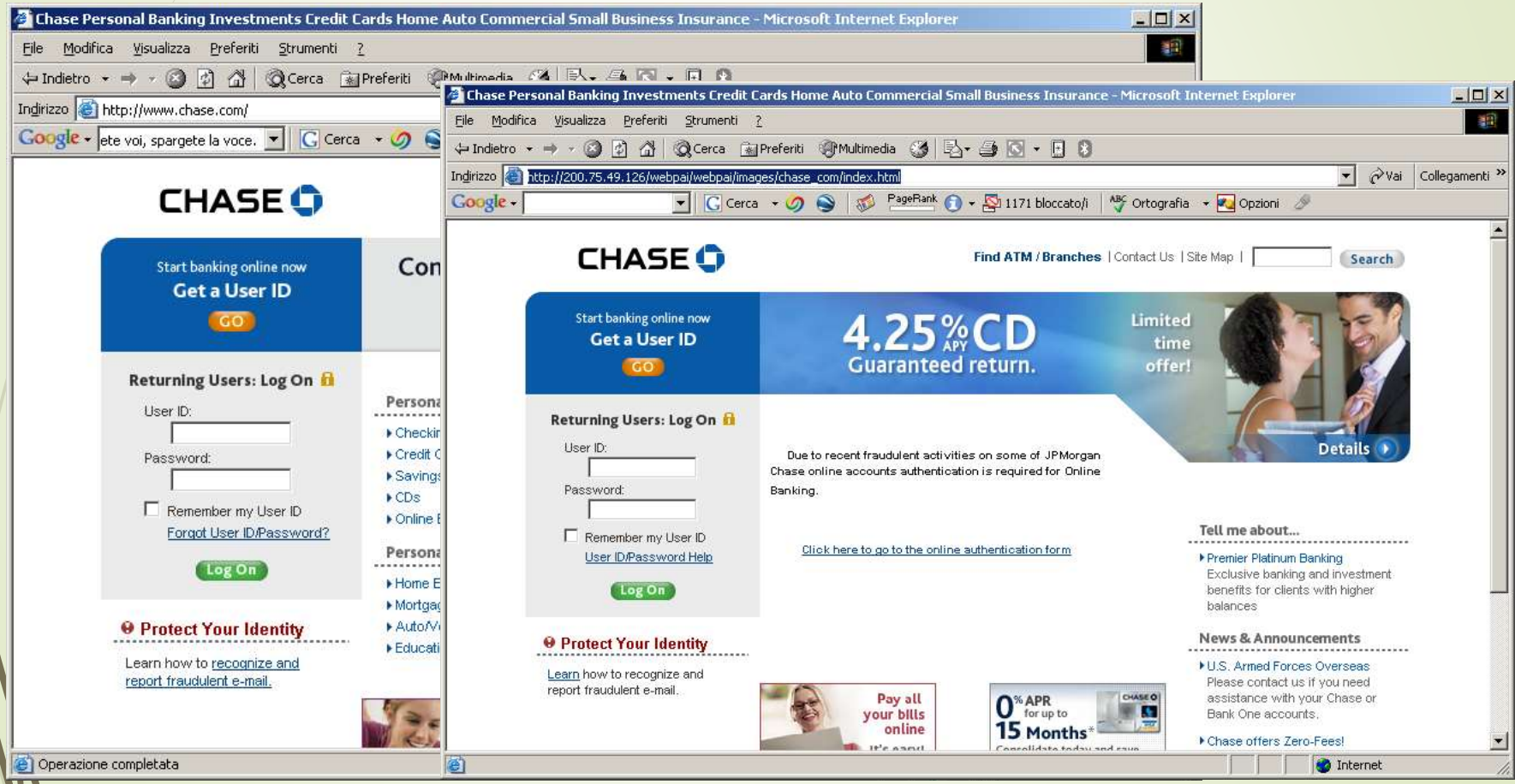
- According to Ghosh, there were "445,004 attacks in 2012 as compared to 258,461 in 2011 and 187,203 in 2010", showing that phishing has been increasingly threatening individuals



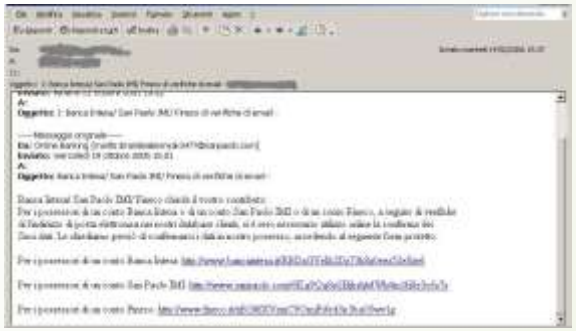
2nd Quarter 2014 Phishing Trends

- The 128,378 phishing sites were observed in Q2.
- This is the second----highest number of phishing sites detected in a quarter, eclipsed only by the 164,032 seen in the first quarter of 2012.
- New online payment services and crypto----currency sites are being targeted more frequently.
- There has been a recent increase in PUPs. (Potentially Unwanted Programs) such as spyware and adware. This contributed to higher global infection rates.
- The total number of brands targeted dropped to 531 brands, down from the 557 targeted in the first quarter of 2014.
- The United States continued to be the top country hosting phishing sites.

Phishing (Social Engineering)



Phishing (Social Engineering)



Phishing technique

```
Per i possessori di un conto Banca Intesa: <a
href="http://www.google.mn/url?q=
http://www.google.gm/url?q=
http://www.google.ru/url?q=
http://%09%36%252%356%2563h%2567ka%09%6f%2e%64a%2E%
09%72U/"
target="_blank">http://www.bancaintesa.it/RBDaGVeIk
2Dz73h8x0eez52e8zy6</a><br>
```

Phishing technique

```
<br> Per i possessori di un conto San Paolo IMI: <a
href="http://www.google.it/url?q=
http://www.google.lt/url?q=
http://www.google.dk/url?q=
http://%09%2509%09%25%09%32576%09%76o%2570v%65o%2E%64%09a%0
9%2e%09Ru/"
target="_blank">http://www.sanpaolo.com/6Kq9Qq8y2Hikshh4Wh4
m1fj8e3c6s7s</a><br>
<br> Per i possessori di un conto Fineco: <a
href="http://www.google.ms/url?q=
http://www.google.sc/url?q=
http://www.google.hn/url?q=
http://i%09%252%350%09%39%256%66%66gn%71q%2e%64a%2e%72U/"
target="_blank">http://www.fineco.it/xRGt8XVzjnC9OmjFi6rd3p
3bq05wv1g</a>
<o:p></o:p></span></font></p>
```

Phishing technique

http://www.google.mn/url?q=
http://www.google.gm/url?q=
http://www.google.ru/url?q=
http://%09%36%252%356%2563h%2567ka%09%6f%2e%64a%2E%09%72U/

Phishing technique

http://www.google.mn/url?q=
http://www.google.gm/url?q=
http://www.google.ru/url?q=http://6lhgkao.da.rU/

Phishing (Social Engineering)

```
Location: Colombia (high)

ARIN says that this IP belongs to LACNIC; I'm looking it up there.


Using 0 day old cached answer (or, you can get fresh results).
Hiding E-mail address (you can get results with the E-mail address).


% Joint Whois - whois.lacnic.net
%  This server accepts single ASN, IPv4 or IPv6 queries


% Copyright LACNIC lacnic.net
%  The data below is provided for information purposes
%  and to assist persons in obtaining information about or
%  related to AS and IP numbers registrations
%  By submitting a whois query, you agree to use this data
%  only for lawful purposes.
%  2006-03-13 16:22:10 (BRT -03:00)

inetnum:     200.75.49.112/28
status:      reallocated
owner:       SECRETARIA DISTRITAL DE SALUD SDS
ownerid:     CO-SDSS1-LACNIC
responsible: Javier Guido
address:     CLL 13, 32, 69 PSO 3
address:     9999 - BOGOT?- CU
country:     CO
phone:       +57 1 3649607 []
owner-c:     JAG11
tech-c:      JAG11
created:     20040930
changed:     20040930
inetnum-up:  200.75.32/19
```

Phishing (Social Engineering)

IP address:	200.75.49.126
Reverse DNS:	clientes_corpor_7549-126.etb.net.co.
Reverse DNS authenticity:	[Could be forged: clientes_corpor_7549-126.etb.net.co. does not exist]
ASN:	19429
ASN Name:	LACNIC-19429
IP range connectivity:	1
Registrar (per ASN):	ARIN
Country (per IP registrar):	CO [Colombia]
Country Currency:	Unknown
Country IP Range:	200.75.32.0 to 200.75.63.255
Country fraud profile:	High
City (per outside source):	Unknown
Private (internal) IP?	No
IP address registrar:	whois.lacnic.net
Known Proxy?	No

Phishing (Social Engineering)

Hop	T1	T2	T3	Best	Graph	IP	Hostname	Dist	TTL	Ctry	Time
1	0	0	0	0.5 ms		66.36.240.2 AS14361 HOPONE-DCA	c-vl102-d1.acc.dca2.hopone.net.		255	US	Unknown: 81bbe1ce
2	11	0	16	0.7 ms [+0ms]		66.36.224.233 AS0 IANA-RSVD-0	gec2.core2.dca2.hopone.net.	0 miles [+0]	254	US	Unix: 15:42:0
3	3	1	12	1.2 ms [+0ms]		66.36.224.34 AS0 IANA-RSVD-0	ge2-0-241.core1.iad1.hopone.net.	0 miles [+0]	253	US	Unknown: 8397bf15
4	70	62	2	2.3 ms [+1ms]		206.223.115.48 AS0 IANA-RSVD-0	ge6-14.colo02.ash01.pccwbtn.net.	0 miles [+0]	252	US	Unix: 16:43:3
5	46	33	56	33 ms [+31ms]		63.218.113.10 AS3491 BTN-ASN	ifx.ge6-2.br01.mia02.pccwbtn.net.	0 miles [+0]	248	US	Unix: 16:43:3
6	355	180	204	180 ms [+147ms]		63.218.113.2 AS3491 BTN-ASN	ifx.ge6-2.br01.mia02.pccwbtn.net.	0 miles [+0]	244	US	Unix: 16:43:3
7	392	394	*	209 ms [+28ms]		63.171.232.6 AS19429 LACNIC-19429	sw01.etb.net.co.	0 miles [+0]	243	US	Unix: 16:43:3
8	209	*	*	209 ms [+0ms]		200.75.49.126 AS19429 LACNIC-19429	[Reached Destination]clientes_corpor_7549-126.etb.net.co.	0 miles [+0]	115	CO	Microsoft: 16:43:30.458

And Now?

- Well, case (technically) solved.
- Success
- Go next!

Is this case really solved?

Budapest Convention

Convention on Cybercrime

Budapest, 23.XI.2001

Council of Europe

Aim of the Cyber Crime Convention

- Harmonisation of criminal substantive law, basis R (89) 9.
- Harmonisation of criminal procedural law, basis R (95) 13.
- Instruments for mutual legal assistance, basis existing co-operation instruments.
- Codification of international law
- Framework for future developments

Scope of the Cyber Crime Convention

- Minimum character
- Substantive law:
  - categorisation; distinction **cyber crime** in narrow and in broad sense.
- Procedural law
  - specific **investigative** powers related to IT, preliminary measures

Scope CCC- continued

- Mutual assistance
  - supplementing existing bilateral and multilateral instruments
  - extradition
  - scope of application of coercive powers
  - further assistance

Harmonising of substantive criminal law

- Cyber crime in the narrow sense
  - C.i.a.-offences: artt. 2-6
- Cyber Crime in the broader sense:
  - Computer-related offences: artt. 7-8
  - Content-related offences: art. 9
  - I.p.r.-related offences: art. 10
- Accessory provisions: artt. 11-13

Art. 2 – Illegal access
Art. 3 – Illegal interception
Art. 4 – Data interference
Art. 5 – System interference
Art. 6 – Misuse of devices
Art. 7 – Computer-related forgery
Art. 8 – Computer-related fraud
Art. 9 – Offences related to child pornography
Art. 10 – Offences related to infringements of copyright and related rights

General provisions

- Definitions: art. 1
  - computer system
  - computer data
- Element: “without right”
- Element: “intentionally”

Issues considered but not included

- Surreptitiously gathering of personal data ("Cookies")
- Spam (unsolicited e-mail)
- Spoofing
- Racism and xenophobia (see hereafter)
- Other Content-related offences (e.g. gambling)
- Non-liability of ISP's

Jurisdiction

- Scope art. 22: only substantive provisions
- Principle: **territoriality**
- Includes ships and aircrafts
- Restricted nationality principle
- Dedere aut judicare
- Conflicts: Consulting mechanism (*substantial link*)

Criminal procedural law

- Starting point: CoE R(95) 13
- Aim: gathering of electronic evidence of a specific criminal offence
- Scope: cyber crimes art.14:

a) offences established in the CCC;

b) computer system instrument of the crime;

c) any other crime for which electronic evidence is needed.

Criminal Procedural law- general principles

- Scope: art. 14
- Scope, conditions and safeguards art. 15: **domestic law**
- Distinction between stored data and flowing data

Definitions

- art. 1
- computer system
- computer data
- service provider: communication services: TO and ISP equal footing
- traffic data: functional definition (*path, source)*

Measures concerning stored computer data

- Search of computer system and files: art. 19
- Production order: art. 18
- Expedited preservation: art. 16
- Expedited preservation of stored traffic data: art. 17

Preservation of traffic data

- EU-directive Telecommunications and Privacy 1997:
  - deletion of non-billing data
- Other Parties: no restrictions
- Principle CCC: “preserve traffic data as is”

Real time collection of traffic data/interception of content

- Art. 20/21 parallel in structure
- Art. 21: serious crime only (domestic law)
- Specific communication by means of a computer system
- Law enforcement authorities or service provider
- "As is available", no technical requirements
- Confidentiality clause possibility

Evidence and Computer Forensics

rensics defined

Vondering why do you need computer forensics?

Definitions & Principles

- What is “Forensic Computer Investigation”?
- Forensic == “pertaining to the law”
- Forensic X
  - Anthropology, ballistics, genetics, chemistry, liquid splatter analysis, dentistry…
- Good book: “Criminalistics”, by Richard Saferstein

Computer forensics defined

- Data management targeting the evidence for trial
- Computer crimes : law n. 547/93; law n.48/08
- Crimes using digital devices
  - Data
  - Relevant data storage

Computer forensics defined

- The personal or local search is regulated by article n. 352 of the Criminal Procedure Code.
- While the law n. 48 of March 18, 2008 represents the rules and best practices to follow for the acquisition of the source of evidence, in particular of the computer data, sanctioning the introduction of the founding principles of digital forensics within our system, providing important aspects related to the management of those elements of evidence that, by their nature, present characteristics of extreme volatility and fragility.

Digital Evidence

- **Digital evidence** or electronic **evidence** is any probative information stored or transmitted in **digital** form that a party to a court case may use at trial. (SWGDE, 1998)
- Properties
  - Volatile
  - Infinite /fast Replicability
  - Decoding (readable for humans)
  - Altering the evidence can be caused by devices or by the improper manipulation of the operators. EFFECT: burned evidence, impossibility to restore ex-ante status

Digital Evidence

Appendix to Recommendation No. R (95) 13
concerning problems of criminal procedural law connected with information technology

V. Electronic evidence

- 13. The common need to collect, preserve and present electronic evidence in ways that best ensure and reflect their integrity and irrefutable authenticity, both for the purposes of domestic prosecution and international co-operation, should be recognised. Therefore, procedures and technical methods for handling electronic evidence should be further developed, and particularly in such a way as to ensure their compatibility between states. Criminal procedural law provisions on evidence relating to traditional documents should similarly apply to data stored in a computer system.

Definitions & Principles

"Process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings (i.e. a court of law).“

Why Investigate?

- Catch and prosecute
  - Expensive
  - Hard work
  - Can take a long, long, long time
  - Might need to leave system in a compromised state - what if its a production server?And cloud?And dozens of smartphones?
  - Might not be feasible in all cases

Why Investigate?

- Determine how they broke in
- Determine what damage was done
- Determine who did it (attribution)
- Support prosecution

The Seven Steps (DFRWS)

- Identify the evidence
  - Must identify the type of information that is available
  - Determine how to best retrieve it
- Preserve the evidence
  - With the least amount of change possible
  - You must be able to account for any changes

The Seven Steps (DFRWS)

1. Identification,
2. Preparation
3. Approach strategy
4. Preservation,
5. Collection,
6. Examination,
7. Analysis,
8. Presentation,
9. Returning evidence

The Seven Steps (DFRWS)

- Identify the evidence
  - Must identify the type of information that is available
  - Determine how to best retrieve it
- Preparation the evidence
  - entails the preparation of tools, techniques, search warrants, and monitoring authorizations and management support;
- Approach strategy
  - that develops a procedure to use in order to maximize the collection of untainted evidence while minimizing the impact to the victim

The Seven Steps (DFRWS)

- Preservation
  - which involves the isolation, securing and preservation of the state
  - of physical and digital evidence;
- Collection
  - entails the recording of the physical scene and duplicate digital evidence using standardized and accepted procedures
- Examination
  - involves an in-depth systematic search of evidence relating to the suspected crime
- Analyze the evidence
  - Extract, process, interpret
  - Extract - may produce binary 'gunk' that isn't human readable
  - Process - make it humanly readable
  - Interpret - requires a deeper understanding of how things fit together

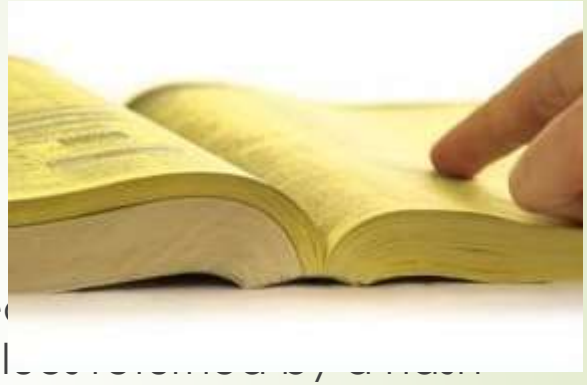
Collection

- Rules/laws (Italy)
- D. Lgs. n. 82 del Marzo 2005 (Codice dell'Amministrazione Digitale), new **Codice** dell'**Amministrazione Digitale** (Decreto legislativo n. 235/2010) and D. Lgs. n. 159 del 4 Aprile 2006 (Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'Amministrazione Digitale)
  - Documents Preservation
  - Digest and hash functions
  - Digital Signature
  - Timestamp

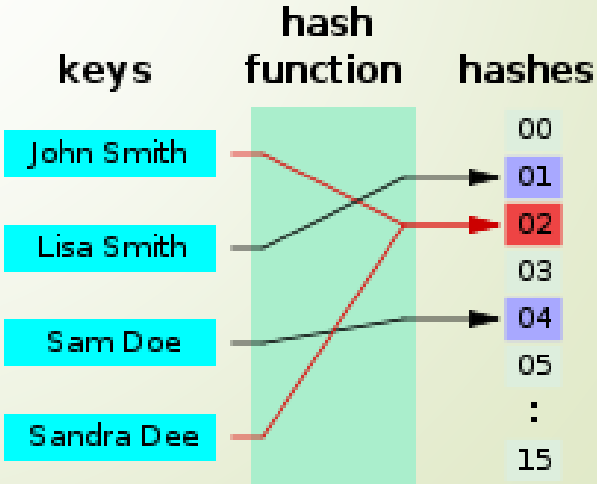
Collection

- Digest and hash function
  - digest as a resuming document (fixed length)
  - A **hash function** is any function that can be used to map digital data of arbitrary size to digital data of fixed size. The values returned by a hash function are called **hash values**, **hash codes**, **hash sums**, or simply **hashes**.
- DPCM 8 febbraio 1999: "*l'impronta di una sequenza di simboli binari è una sequenza di simboli binari di lunghezza predefinita generata mediante l'applicazione alla prima di un'opportuna funzione di hash*"

Collection



- Digest and hash function
  - digest as a resuming document (fixed length)
  - A **hash function** is any function that can be use arbitrary size to digital data of fixed size. The val function are called **hash values**, **hash codes**, **hash sums**, or simply **hashes**.



Collection

(Italy) Law 48/2008

Julius. Caesar
Via Appia 1
Rome, The Roman Empire

May, 22, 2005

To Whom it May Concern:

Alice Falbala fulfilled all the requirements of the Roman Empire intern position. She was excellent at translating roman into her gaul native language, learned very rapidly, and worked with considerable independence and confidence.

Her basic work habits such as punctuality, interpersonal deportment, communication skills, and completing assigned and self-determined goals were all excellent.

I recommend Alice for challenging positions in which creativity, reliability, and language skills are required.

I highly recommend hiring her. If you'd like to discuss her attributes in more detail, please don't hesitate to contact me.

Sincerely,

Julius Caesar

letter_of_rec.ps

Julius. Caesar
Via Appia 1
Rome, The Roman Empire

May, 22, 2005

Order:

Alice Falbala is given full access to all confidential and secret information about GAUL.

Sincerely,

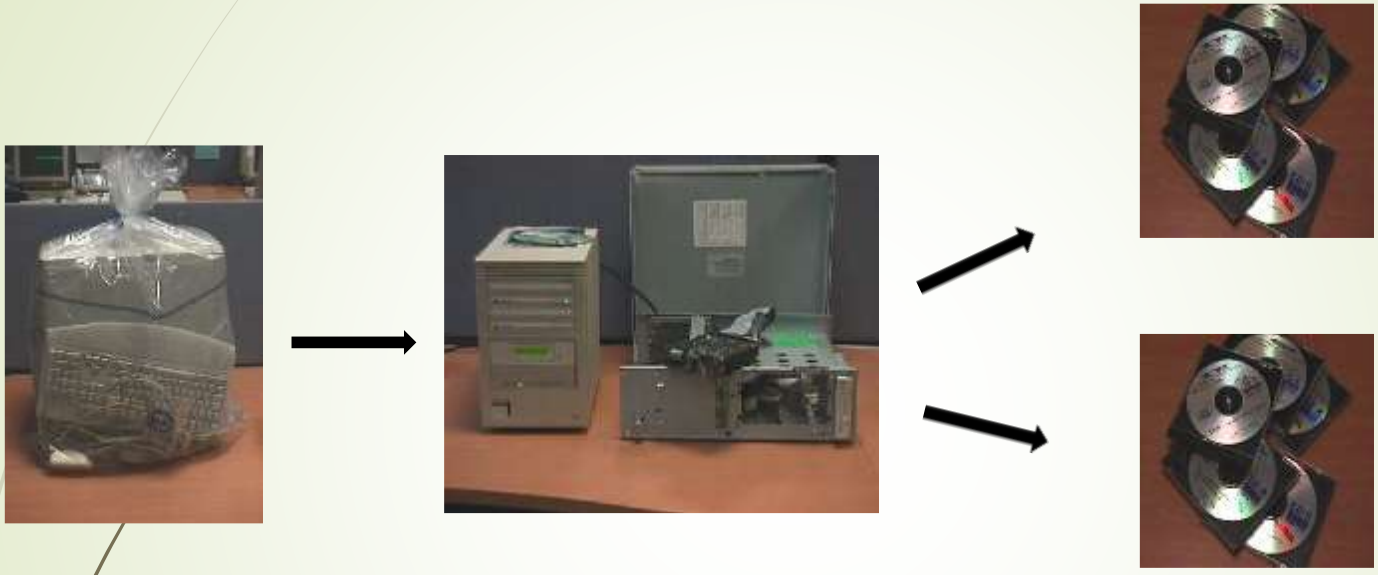
Julius Caesar

order.ps

Acquisition vs burning the evidence

- *Art. 259 CPP "Custodia delle cose sequestrate"*
- *«Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria».*

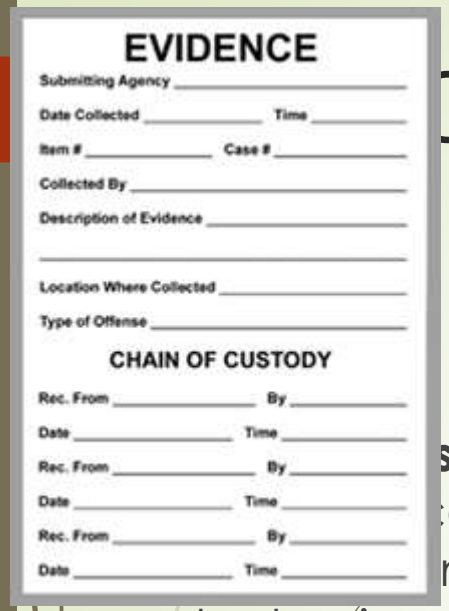
Creating file image



Ian Pomfret, Computer Forensics, British Telecom, 2001

Tools

Forensic workstation


EVIDENCE
Submitting Agency
Date Collected Time
Item # Case #
Collected By
Description of Evidence
Location Where Collected
Type of Offense
CHAIN OF CUSTODY
Rec. From By
Date Time
Rec. From By
Date Time
Rec. From By
Date Time

Chain of custody

stody (CoC), in legal contexts, refers to the
cal documentation or paper trail, showing the seizure,
ntrol, transfer, analysis, and disposition of physical or
electronic evidence.

Analysis Data related to a document

- Internal Data
  - Images
  - Documents
  - Private data
  - Confidential data
  - ……
- External data
  - System data
  - File data (file metadata)

What time is it?

Which creation data?

The Seven Steps (DFRWS)

- Present the evidence
  - To LE, attorneys, in court, etc.
  - Acceptance will depend on
    - Manner of presentation (did you make it understandable, convincing?)
    - The qualifications of the presenter
    - The credibility of the processes used to preserve and analyze the evidence
    - Credibility enhanced if you can duplicate the process
  - Especially important when presenting evidence in court

The Seven Steps (DFRWS)

- Returning evidence: that ensures physical and digital property is returned to proper owner.

Device Forensics

- Disk Forensics
- Network Forensics
- Email Forensics
- Internet Forensics
- Portable Device Forensics (e.g. flash cards, PDAs, Blackberries, email, pagers, cell phones, IM devices)

Tools by law

- Firma elettroniche e certificati
  - Electronic signature : set of data related to other set of data composing digital identity (art. 1, comma 1, lett. q) del D. Lgs. 82/2005)
    - ES. PIN ATM, login/pwd
  - Digital SIgnature: electronic signature using asymetric crytography ensuring integrity and non-repudiation (art. 1, comma 1, lett. s)
  - Certificato Qualificato: set of information univocally linking Identity and Public key.
  - Timestamp (by CA)

Q&A

Gianluigi Me

gme@luiss.it

Digital forensics problems

Digital forensics problems

- identity
- location
- integrity
- stickiness
- data type
- traceability
- analysis

Identity

- Establishing a valid forensic link between data and virtual identity
- Establishing a valid forensic link between virtual identity and phisycal identity

Identity example

- Identity substitution
- *Massima (Cass V penale, 2013/18826) L'inserimento, in una chat di incontri personali, del numero di telefono cellulare di un'altra persona, ignara, in associazione a uno pseudonimo (il telematico nickname) al fine di danneggiare la stessa persona facendola apparire sessualmente disponibile, integra il reato di sostituzione di persona di cui all'articolo 494 del C. p., nella modalità dell'attribuzione di un falso nome Considerazione giuridica*

location

- Physical localization of suspects
- Law implication due to transnationality?
- Distinction between:
  - Static data, residing on PC to be searched
  - Dynamic data : lawful interception

integrity

- Forensic acquisition of data
  - Risks to alter the integrity
- Different international laws -> non uniform digital evidence treatment

integrity

- ….
- Less than 20 percent of source drive sectors were copied accurately when the Lg XferBlk setting was selected (DA-01-SATA48).
- When two drives were selected as targets for a restore from a single image file, one of the clones that was created was inaccurate and incomplete
- ….

Computer Forensics Tool Testing (CFTT) program (booklet)

- Proprietary vs Open Source?

stickiness

- Multiple evidence copies made during transmission (e.g. Internet connections)
- Generally an advantage for investigators
- Data coming from carriers can be debatable regarding the forensic validity of its acquisition

data type

- Digital evidence elements:
- Connection content
- Communication metadata
- Privacy of network users
- Binary code of DATA is the genuine, primary source
- Possible different laws for analogous activity (phone call, voip call)

traceability

- Multiple sources
- User data regarding his/her activity
- dati created (regarding a communication system) by a suspect
- User Communication activity
- Source/Destination Identification
- What if the device can be used by multiple

How can be determined the user in a precise time window?

Example: IP resolution

- How to identify phisical identity from IP address
- Identification through IP log inspection (tip:could be anonymized)
- Service Provider Identification where to access registries
- Who is the owner of that IP? What if DHCP?And Wifi hotspots?Or insecure Wifi?
- Personal data acquisition
- Key factor: DATA RETENTION (defines the policies of persistent data and records management for meeting legal and business data archival requirements; although sometimes interchangeable, not to be confused with the Data Protection Act 1998)
- Nightmare for companies!

analysis

- Huge amount of data, sometimes prohibitive
- Easy to obtain data, very hard to provide results on time and with budget limits

analysis

- If you log in, you modify
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runonce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
- HKEY_LOCAL_MACHINE \Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

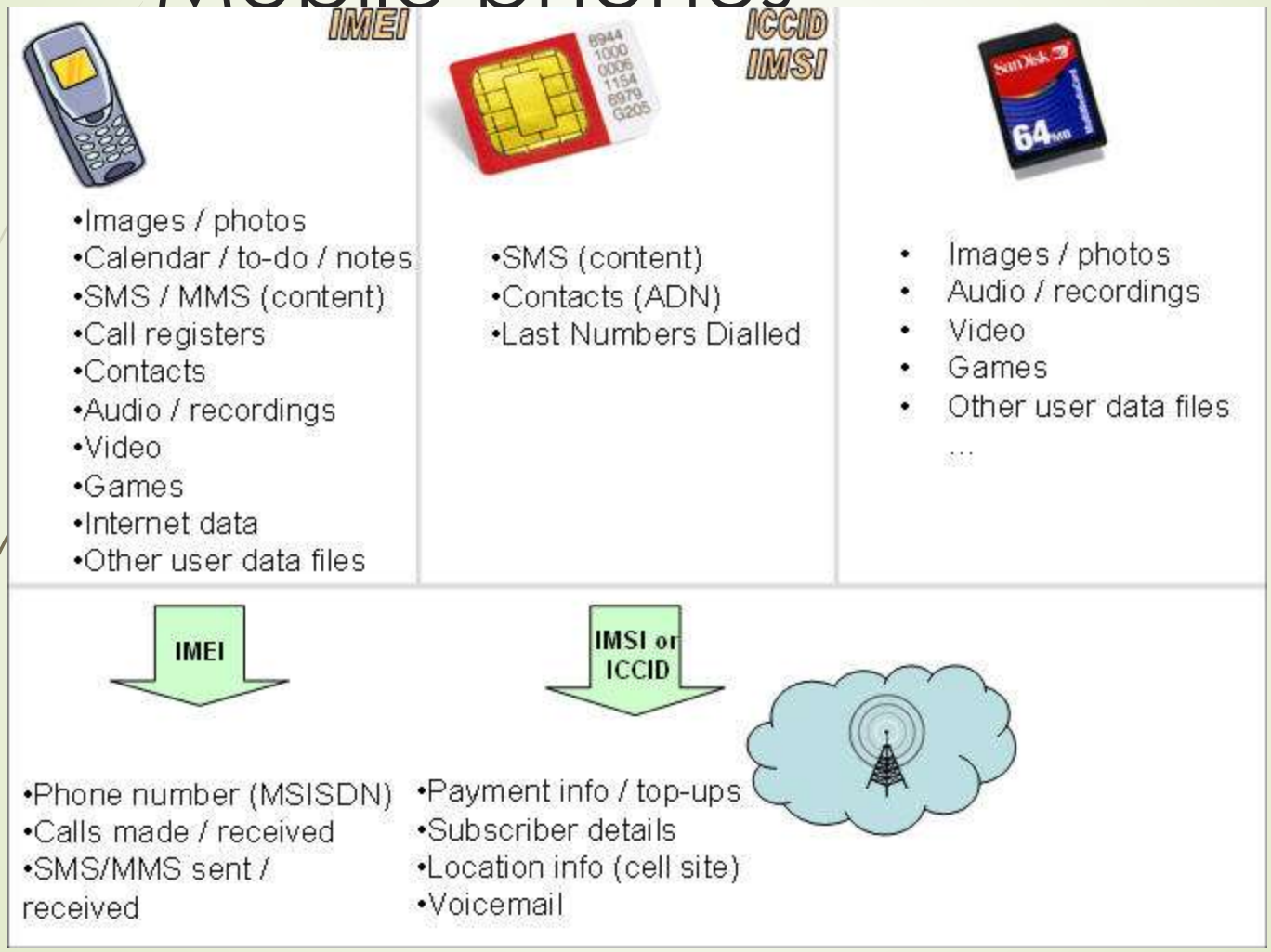
analysis

- Plugging an USB stick modifies a “Registry key” under the key:
- `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\USB\`
- The sub-key is approx:
  - `Disk&Ven_###&Prod_###&Rev_###`

analysis

- **index.dat**
- **Windows 7/Vista**
- C:\Users\<username>\Roaming\Microsoft\Windows\Cookies\index.dat
- C:\Users\<username>\Roaming\Microsoft\Windows\Cookies\Low\index.dat
- C:\Users\<username>\Local\Microsoft\Windows\History\History.IE5\index.dat
- C:\Users\<username>\Local\Microsoft\Windows\History\History.IE5\Low\index.dat
- C:\Users\<username>\Local\Microsoft\Windows\History\History.IE5\index.dat\MSHist*\index.dat
- C:\Users\<username>\Local\Microsoft\Windows\History\History.IE5\Low\index.dat\MSHist*\index.dat
- C:\Users\<username>\Local\Microsoft\Windows\Temporary

Mobile phones



Report Manger

UFED Report Manager- (G:\Dubai Training\Example UFED Extraction\AOL1 Nokia 6230i UFED.urp)

File SMS UFED Help

New Open Save Copy Options Read UFED

Report
Contacts (103)
SMS (71)
Calendar (0)
Calls log (113)
Images (103)
Audio (5)

#	Folder	Number	Name	Message	Date/Time	SMSC	Status	Storage
Filter by								
71	Archive			Ey 05lwt	15/11/2006 16:0...			Unknown
14	Inbox	+447765610424		CAB BRO JAZAKALLAH BRO. I DIDNT W...	08/10/2006 18:5...	+447785016005	Read	Unknown
17	Inbox	+447772933924	Zaf	LOYDS . ACCOUNT. NO. 07792397. SO...	19/09/2006 22:0...	+447973074999	Read	Unknown
19	Inbox	+447772933924	Zaf	LOYDS T.S.B. ACCOUNT NO. 39990560 SOR...	01/09/2006 12:2...	+447973074999	Read	Unknown
29	Inbox	+447793102142		Ramadan mubarik.May Allah grant U and ur fa...	05/10/2005 12:5...	+447802000332	Read	Unknown
2	Inbox	+447803991037	S M	Ur so brave,pik up da fne u sharif zada	01/02/2007 15:1...	+447802000332	Read	Unknown

Selected data

Number:
+447772933924

Name:
Zaf

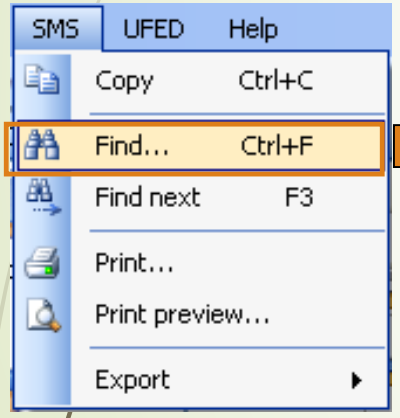
Message:
LOYDS . ACCOUNT. NO. 07792397. SORT CODE. 309392. JAZAKALLAH BIG TIME MY BROTHER MAY ALLAH TALA GIVE U MORE THAN U CAN HANDLE.

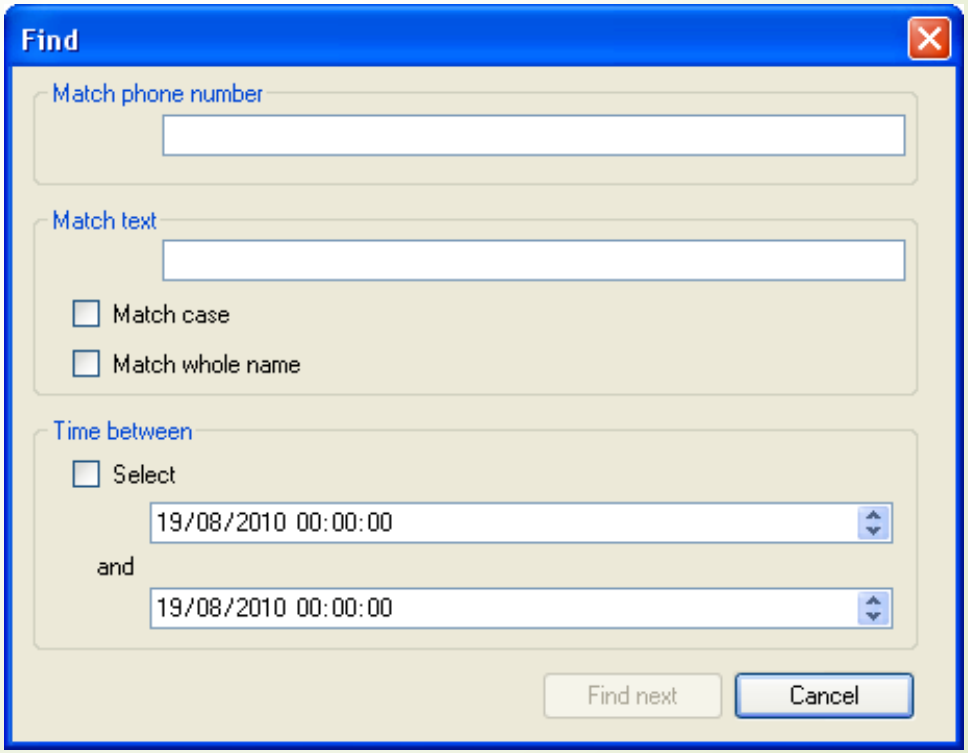
SMSC:
+447973074999

All data from selected line above

Find Menu Option

- The options will vary depending on the data type being looked at
- Here find is for SMS

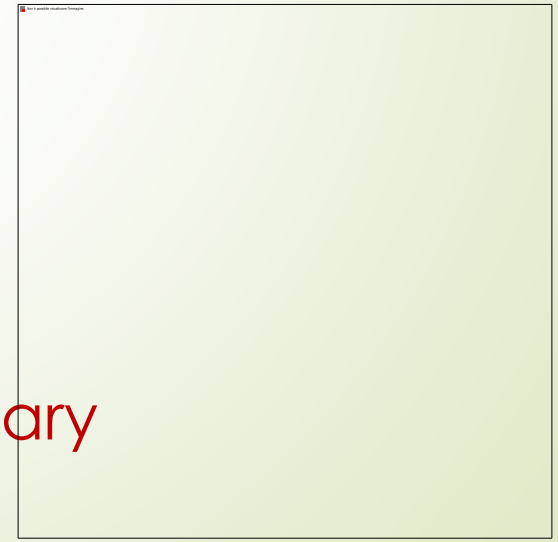




Analysis: example

- Web page acquisition

Printing the web page
HTML code of the page
Print web pages certified by a notary



Analysis: example

- A displayed web page (generally dynamic) depends from
- Web server
- User Computer
- User
- E.g www.facebook.com
- Depends from:
- User identity (username/password, source IP address, browser, cookies etc)
- Time of the request
- Further parameters

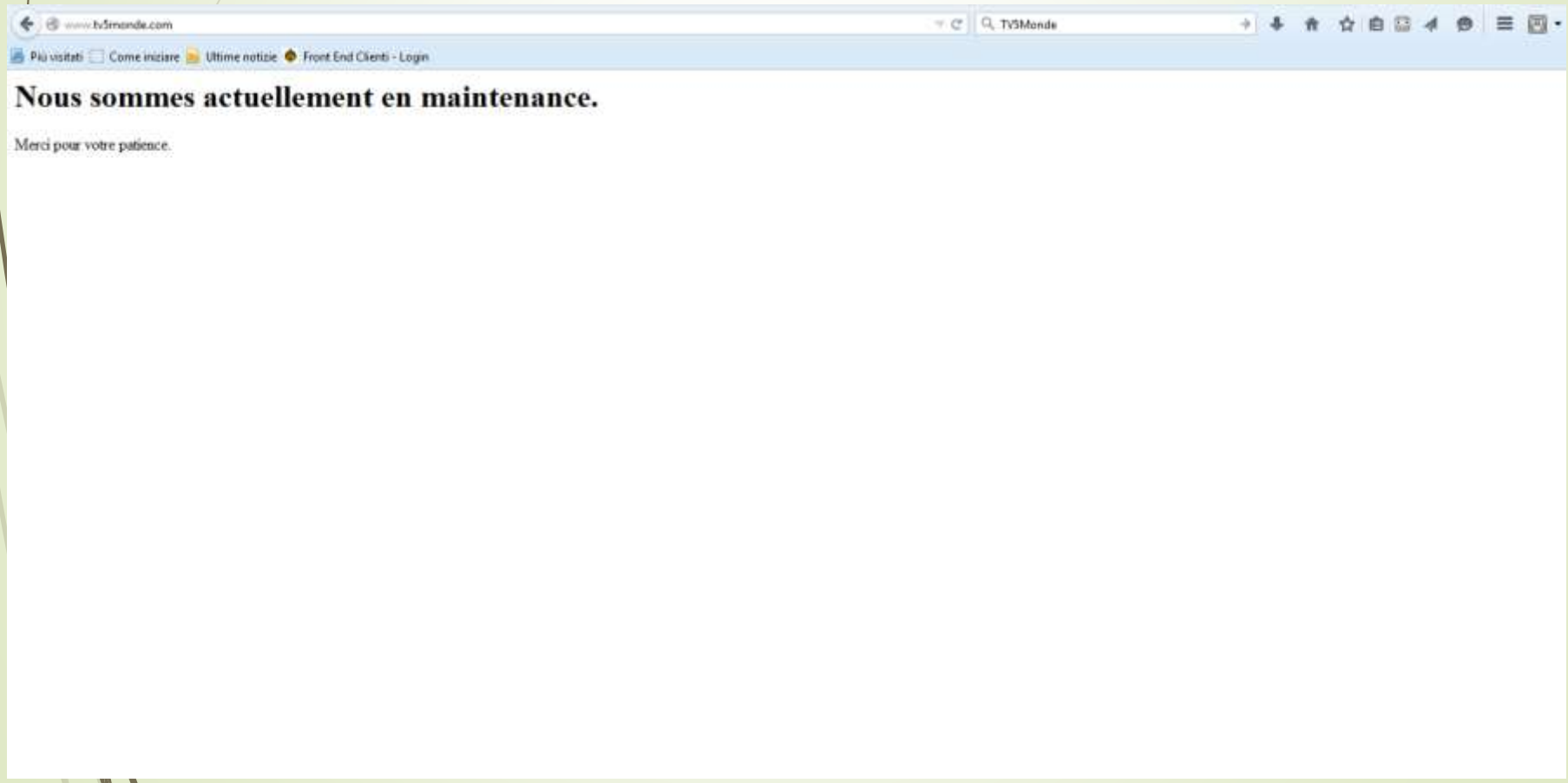
Analysis: example

- A web page contains
- text
- images
- videos
- etc…
- Every object can have a different IP source
  - Page source code explains to you
  - Verify data source
  - Eavesdropping and storage of traffic data related to the web page
  - Time

Analysis-correct procedure

- Recording data traffic
- Web Page surfing
- Time (online newspaper, NTP server)
- Store every page and the whole related traffic
- Digital signature and timestamp to all the data
- Optional: video recording of the operation.

ISIS attack to TV5monde (snapshot 12:02 09/04/2015)



ISIS attack to TV5monde (snapshot 12:02 09/04/2015)

- How to proceed?

Newsweek Twitter Hack

ISIS attack to TV5monde (snapshot 12:02 09/04/2015)

- How to proceed?

Digital forensics problems

Conclusions

- Growing pervasiveness of digital evidence (computer crimes pure and in broad sense)
- CCC aims and scope
- Big data!!
- Technology driven, hard to maintain standards up-to-date (e.g., self driven cars, IOE)
- Procedural modus operandi and analysis are the key for success
-

Q&A