




Computer crime and electronic evidence



Georgia, 29 September 2009

Challenges of cybercrime legislation

- ▶ Cybercrime is a technical subject matter – is the reduction best done by computer engineers through technical measures?
- ▶ Cybercrime is international (Cyber → Internet → cross-jurisdictional)
 - ▶ Is there interest to regulate:
 - ▶ Crimes committed against our citizens from abroad?
 - ▶ Crimes committed by our citizens against foreign residents?
 - ▶ The need for harmonized legislation
- ▶ Presentation:
 - ▶ Examples of cyber evidence in the administration of justice
 - ▶ Computer forensics and sources of evidence
 - ▶ Cooperation with foreign law enforcement and private industry



How is electronic evidence used
today?

The use of electronic evidence in legal procedures is increasing

- ▶ Computers are used to communicate, for social interaction, writing contracts, and making purchases.
- ▶ Electronic evidence is common in cybercrime matters but is increasingly being used also in matters that don't concern cybercrime.
- ▶ EU directive 1999/93 on electronic signatures sets formal requirements for electronic contracting, but also allows other types of electronic evidence to be used even if it doesn't adhere to the specifications set forth.
- ▶ Electronic evidence may provide legal professionals access to more information and thus enhances the administration of justice.



Browser's Internet search history

- ▶ The wife of an university professor was murdered and investigations on the husband's computer revealed Internet searches for "*how to kill someone quickly and quietly*" and "*how to murder someone and not get caught*".
- ▶ A wife searches the Internet for "*decomposition of a body in water*" after her husband disappears. Later the body is found in a lake.
- ▶ A pedestrian is run over by a car but the driver does not stop to help the victim who later dies of the her injuries. Pieces of the car broke of during the accident and remained on the scene. The car debris allowed police detectives to find the driver. When the perpetrator driver claimed he hadn't stop after the accident because thought he had only hit a large animal, the police was able to show that he had searched the Internet for "*hit and run*", "*auto glass reporting requirements to law enforcement*", and "*out of state car repairs*" after the accident.
- ▶ A former employee makes a denial of service attack on the Wifi network of the past employer and evidence on his computer showed he had searched for "*Wifi interference*".

Defamation

- ▶ Defamation is placing a person in a false light in the public eye.
- ▶ The internet is particularly prone to defamation cases as:
 - ▶ The internet makes it affordable and easy to reach the public eye
 - ▶ The internet allows for a certain level of anonymous communication
- ▶ A defamation case was initiated against a former partner who had created a fake Facebook profile. The claimant won 22 000 GBP.

Electronic contracting

- ▶ UK Case Graeme Grant v. Russell Bragg where contract was formed by exchange of email.
 - ▶ Acceptance of a contract can be made through email
 - ▶ A formal contract had been in preparation but not signed
- ▶ French employee contract had formal requirements for the resignation letter, but the court accepted email as being equivalent.

Spam

- ▶ 97% of all email is spam according to the most recent Microsoft study.
- ▶ Spam is used for illegal activity such as:
 - ▶ Selling illegal content, including child pornography
 - ▶ Phishing, to steal money or other items of value
 - ▶ Distributing computer viruses
- ▶ 8,6 in 1000 computers are infected by viruses and one of the main distribution vector is spam.

Illegal access to computer system

- ▶ The Pentagon hacked by Roumanian youth
 - ▶ The hacker used the illegal access to place malware on the servers, and the DOD spent over \$ 35 000 to clean up their systems.
 - ▶ One of the leads was the hacker's email address left on a Japanese server used by him to hide his tracks.
 - ▶ The hacker was then identified as he had previously posted a CV on the Internet with the same email address.
- ▶ Paris Hilton's telephone hacked
 - ▶ The hackers obtained access to the telephone companies customer system through social engineering

Illegal interception

- ▶ A Colombian travelled to luxury hotels around the world to install keylogger software on the public computers of the hotels' internet lounges and business centers.
- ▶ From Colombia he intercepted the hotel computer communication and gained access to users' password, credit card numbers, birthdates, social security numbers, online banking passwords.
- ▶ He stole money and transferred them to prepaid credit cards mailed to mail boxes in the United States.
- ▶ When picking up his prepaid credit cards in the US he was arrested, together with his laptop containing personal information of over 600 victims.

Data interference

- ▶ Hacker cover their tracks by deleting log files of the computer they attack.
- ▶ Viruses often delete files on the computer they attack
- ▶ The deletion of files from your work computer can be data interference.
 - ▶ The senior vice president of a company with 2500 employees in Florida resigned to take a job at the primary competitor.
 - ▶ 475 files had been permanently erased from his work computer days before resigning. The deletion was made with a special tool that would make it impossible to recover the files.
 - ▶ He was suspected of stealing company data.

System interference

- ▶ An IT technician of the largest American mortgage company is fired but his access to the companies' servers is not revoked until a couple of hours later.
- ▶ He manages to modify a script that runs each morning on the companies 4000+ servers so that data will be deleted around 3 months after his departure. The script will display “server graveyard” as a response to all login attempts.
- ▶ By chance the modified script was discovered before it could cause havoc. As only about 10 to 20 employees had root access to the servers to modify that script, the perpetrator was quickly identified.

Misuse of devices

- ▶ Phish-kits make creating phishing websites easy and allow the phishers to obtain website login credentials.
- ▶ Some phishkits, such as the Steely-frog Hotmail phishkit was downloaded over 9 000 times in a matter of a few days after it was released on a a hacking information website.

Internet and privacy

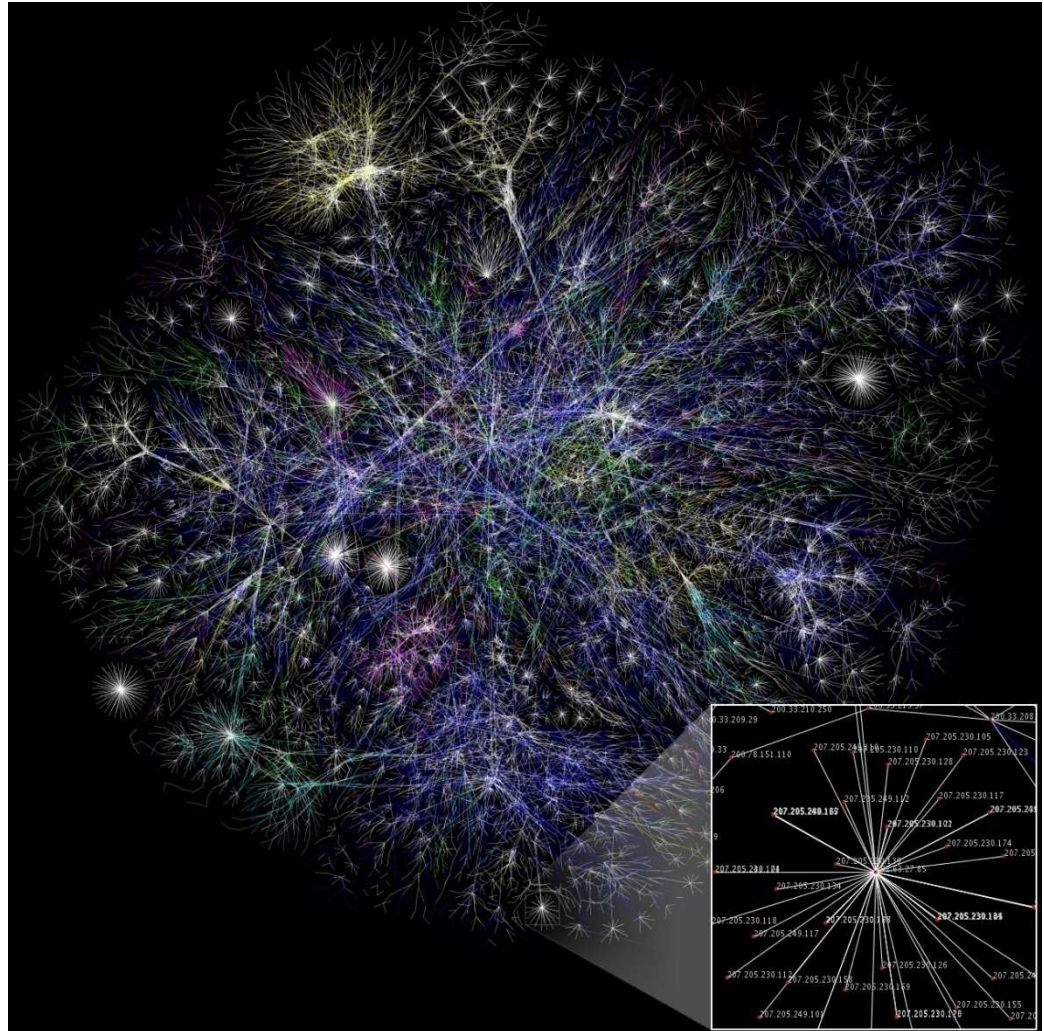
- ▶ The Internet can make large amounts of information available to the entire world, which may have a profound effect on privacy.
- ▶ There are different types of privacy legislation:
 - ▶ Privacy in one's home
 - ▶ Personal affairs privacy
 - ▶ Communication privacy laws
 - ▶ Health privacy laws
 - ▶ Financial privacy laws
 - ▶ Information privacy laws



The Internet and IP numbers

What the Internet looks like

- ▶ The Internet consists of billions of interconnected computers.
- ▶ Data travelling on the internet doesn't travel through a specific channel, but looks for the quickest travel path.



The Internet and IP numbers

- ▶ Each computer on the Internet is assigned a unique IP (Internet Protocol) number.
- ▶ The unique number allows the computers to identify the destination when communicating and sending packets. It is similar to phone numbers that we use when we want to communicate with somebody.
- ▶ Like a phone number, an IP number can be said to identify a geographical location.



What IP numbers look like

- ▶ IP4 uses a 4 byte (32 bit) address providing a total of 2^{32} 4.2 billion unique addresses.
- ▶ IP6 uses 16 bytes (128 bit) network address providing a total of 2^{128} or trillion trillion unique addresses, or 5 000 addresses for every square micrometer of the earth's surface.

An IPv4 address (dotted-decimal notation)

172 . 16 . 254 . 1
↓ ↓ ↓ ↓
10101100 . 00010000 . 11111110 . 00000001
└───┘ └───┘
One byte = Eight bits
└────────────────────────────────┘
Thirty-two bits ($4 * 8$), or 4 bytes


An IPv6 address (in hexadecimal)

2001:0DB8:AC10:FE01:0000:0000:0000:0000
↓ ↓ ↓ ↓ └──────────┘
2001:0DB8:AC10:FE01:: Zeroes can be omitted
↓ ↓ ↓ ↓
10000000300001:0000110110111000:1010113000010000:1111111000000001:
0000300000000000:0000000000003000:0000000030000000:0000000030000000

Domain Name System (DNS)

- ▶ The Domain Name System makes it possible to assign a name to an Internet computer making the address much easier to remember.
- ▶ For example the host name microsoft.com.eg is easier for humans to understand than the IP number of the same server 214.8.55.127
- ▶ The function of the DNS is to translate domain names provided by humans to IP numbers of which the Internet consists.
- ▶ The conversion is necessary as the network layer (network cards, WiFi cards, DSL routers only understand and are able to route traffic to IP addresses.





Evidence of illegal access to other computers

Evidence of cybercrimes over the Internet

- ▶ To commit the following crimes a computer would have to communicate with the victim computer:
 - ▶ Illegal access and interception (Art. 2 and 3)
 - ▶ Data and System interference (Art. 4 and 5)
 - ▶ Data forgery and fraud (Art. 7 and 8)
- ▶ Unlawful access crimes can be committed by having physical access to the computer. However, most commonly they are committed over the Internet.



Evidence of communication between computer systems

- ▶ For technical reasons most computers record data related to its communications with other computers in:
 - ▶ Log files of the operating system
 - ▶ Cache of communication programs
 - ▶ History files such as recently opened documents including its network path, websites viewed.



Identification of a computer

- ▶ The victim computer system may additionally have identified the attacking computer through:
 - ▶ His IP number,
 - ▶ His network computer name or host name
 - ▶ The network card's MAC address



Examining if the attack computer was itself a victim of an unlawful access

- ▶ If incriminating evidence is found on a suspect's computer, he may claim that his computer had been used by somebody else, that he himself is a victim of an illegal access.
- ▶ By securing the evidence of current activities on the computer such as running programs, processes, and open user accounts, it may be possible to exclude some of such claims by defendant.
- ▶ Networking equipment to which the computer is connected should be examined to ensure that it doesn't allow external access.



Evaluating the criminal intent

- ▶ The criminal intent in computer crime can span from:
 - ▶ young, clever, computer whizzes wanting to benefit from their skills,
 - ▶ Criminal organizations looking for make money,
 - ▶ Politically motivated organizations looking to test the critical infrastructure of an adversary.



Evidence provided by Internet Service Providers

Electronic Evidence

Evidence to solve a computer crime is often in the possession of ISPs

- ▶ Computer crime is frequently committed through the Internet, over equipment owned by Internet Service Providers
- ▶ ISPs possess evidence regarding the travel-path of data and who received it or stored it.

Types of Internet Service Providers

Access providers

- ▶ Providers of access to the Internet.
- ▶ Traditionally the Access Providers are phone companies that provide internet access over the phone network through dial-up service or DSL connections
- ▶ Access providers may provide evidence as to who was using a particular Internet address to connect to other computers

Web hosting providers

- ▶ Web hosts provide space on an Internet server for clients to host a website or a file storage.
- ▶ The hosting company can provide evidence regarding who rented the web server and who accessed it

Email hosting providers

- ▶ Email companies store the email content of users
- ▶ They will be able to provide evidence on who owns the email account and who accessed it
- ▶ Because of secrecy of correspondence the content of the email boxes can only be obtained through a Court Order

Jurisdiction of ISP data

ISP jurisdiction

- ▶ The ISP will have to take into consideration the laws of the jurisdiction under which it operates even when the legal request come from a different jurisdiction.
- ▶ Additionally ISPs need to consider the laws of the jurisdiction in which its servers are located should it not be the same as the jurisdiction of incorporation.

Obtaining evidence from ISPs

- ▶ Most ISPs have designated employees to respond to criminal compliance requests
- ▶ When receiving a request, a criminal compliance department will examine legal obligations under the jurisdiction of where the data is located and under the jurisdiction of the petitioner
- ▶ Because of the nature of MLATs, ISPs will usually receive court order from both of these jurisdictions



Securing ISP evidence

Preservation of ISP evidence

- ▶ Preservation of content and traffic data according to Art. 16 and 17
- ▶ Preservation ensures that evidence can be secured even before it is obtained by law enforcement

Disclosure of traffic data

- ▶ Art. 17.1.b requires member states to:
 - ▶ Ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.
- ▶ This enables a quicker identification of the location of the data evidence should it have travelled through a chain of multiple ISPs

Preserving ISP provided evidence

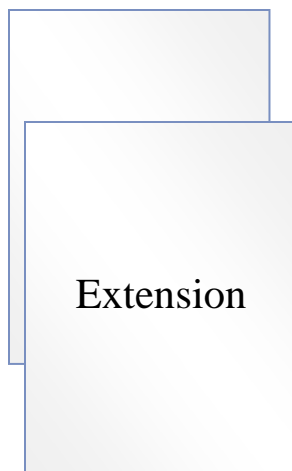
- ▶ During court proceedings an ISP may be requested to provide a testimonial to attest the veracity of the provided documentary evidence
- ▶ To reduce cost to the Court, especially matters where the ISP is located in a foreign country, it may instead be requested that the ISP's custodian of records provide an affidavit, witness statement, or continuity statement as the authenticity of the evidence



Case study: Microsoft criminal compliance

Preservation requests

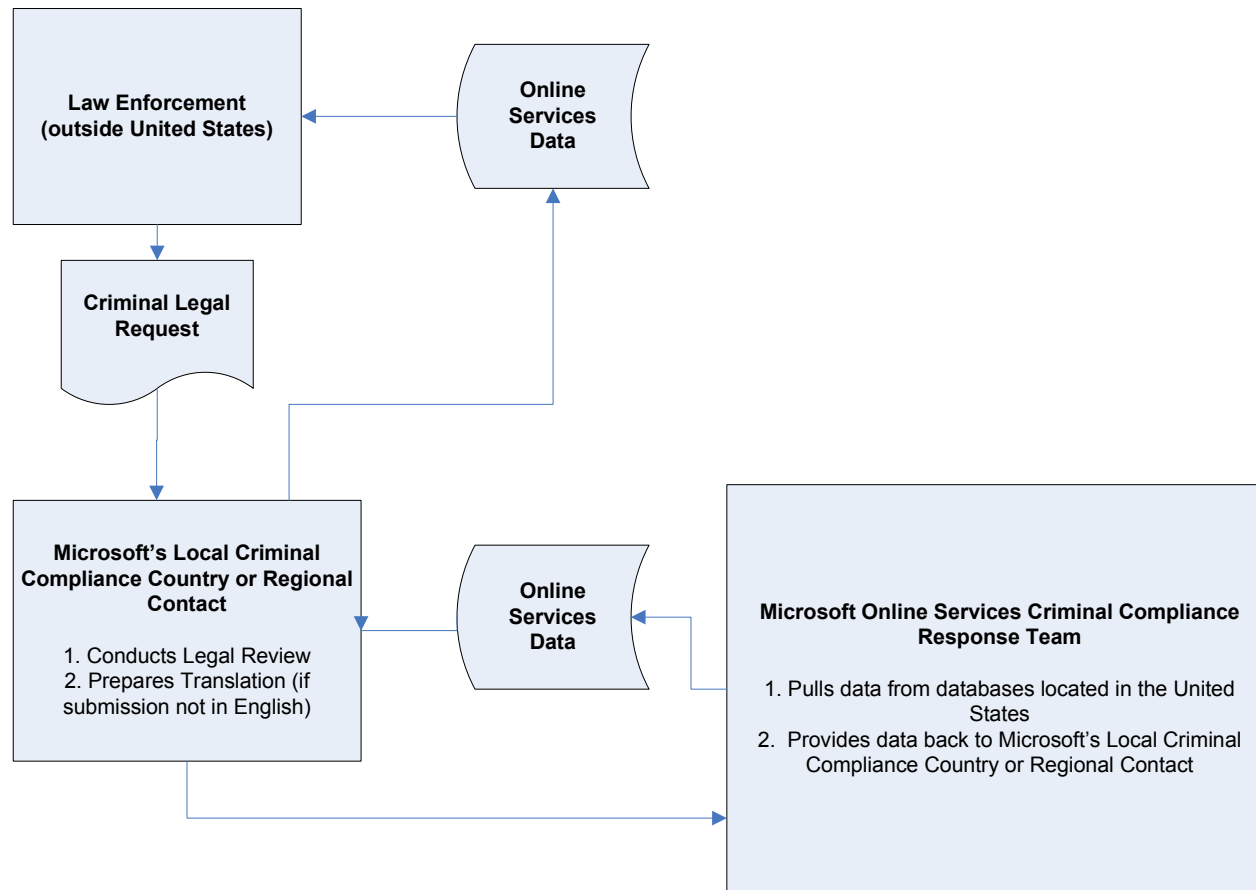
- Microsoft will preserve a snapshot of an account to afford the foreign government the opportunity to seek disclosure through the MLAT/Letters Rogatory process.
- Microsoft will accept a written request, signed by the international law enforcement agency, which specifies the information to be preserved.



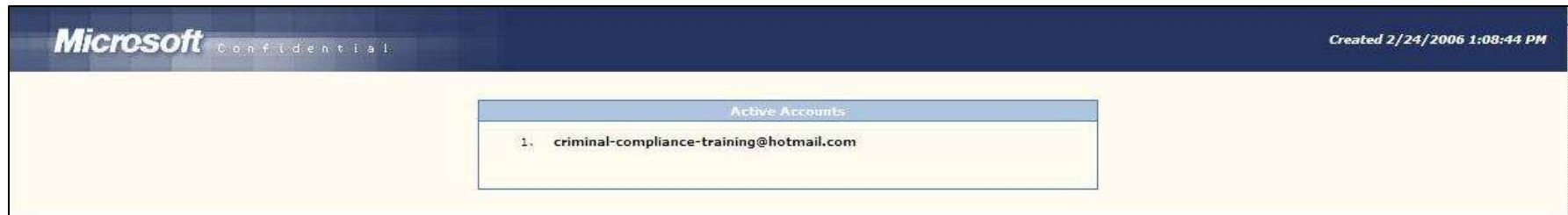
Preserve a snapshot of information, including IP logs and e-mail contents, for 180 days from the date of the preservation.

Microsoft will extend the initial preservation for an additional 180 days upon request from International Law Enforcement.

International Criminal Compliance : Non-Emergency Process



Reading E-mail Account Records – Registration Records



The "Registered From IP Address" is not provided by the user, but is captured by Microsoft's systems.

Reading E-mail Account Records – IP Connection History

Microsoft Confidential

criminal-compliance-training@hotmail.com

2/24/2006 1:08:43 PM

| Menu | History Info | | |
|---|----------------|-----------------------------|-----------|
| Cover Letter | IP | Date {Pacific} | Pass/Fail |
| User Info | 64.4.1.11 | 2/22/2006 9:36:14 AM (PST) | pass |
| History Info | 64.4.1.11 | 2/22/2006 9:37:21 AM (PST) | pass |
| Folders | 64.4.1.11 | 2/22/2006 2:13:41 PM (PST) | pass |
| Email | 64.4.1.11 | 2/22/2006 2:13:57 PM (PST) | pass |
| Other Info | 64.4.1.11 | 2/22/2006 2:14:18 PM (PST) | pass |
| Home | 216.33.243.217 | 2/22/2006 2:17:48 PM (PST) | pass |
|  Print | 64.4.1.11 | 2/22/2006 2:50:26 PM (PST) | pass |
| | 64.4.1.11 | 2/23/2006 8:21:57 AM (PST) | pass |
| | 64.4.1.11 | 2/23/2006 8:22:49 AM (PST) | pass |
| | 64.4.1.11 | 2/23/2006 8:23:00 AM (PST) | pass |
| | 64.4.1.11 | 2/23/2006 8:23:42 AM (PST) | pass |
| | 64.4.1.10 | 2/23/2006 12:42:43 PM (PST) | pass |
| | 64.4.1.10 | 2/23/2006 12:43:56 PM (PST) | pass |
| | 64.4.1.10 | 2/24/2006 1:00:54 PM (PST) | pass |
| | 64.4.1.10 | 2/24/2006 1:01:23 PM (PST) | pass |
| | 64.4.1.10 | 2/24/2006 1:05:34 PM (PST) | pass |
| | 64.4.1.10 | 2/24/2006 1:06:46 PM (PST) | pass |
| | 64.4.1.10 | 2/24/2006 1:07:02 PM (PST) | pass |

- Microsoft retains e-mail account Internet Protocol (IP) connection history for 60 days.

Emergency Requests

- ▶ Microsoft Online Services will respond to emergency requests outside of normal business hours.
- ▶ Send a letter on official agency letterhead- signed and dated, including:
 - ▶ A summary of facts, in English, describing the emergency
 - ▶ A statement that there is an emergency “involving danger of death or serious physical injury requiring disclosure of the information without delay.”
 - ▶ The full name of the requested account (e.g., “bob_compliance@hotmail.com”) and what data is requested (e.g., “Subscriber Information and IP History”).

Cooperation between ISPs and Law Enforcement

Guidelines for the cooperation between law enforcement and Internet service providers against cybercrime

- ▶ The guidelines were adopted at Council of Europe conference on April 2nd, 2008
- ▶ Provides suggestions on improving the cooperation between law enforcement and ISPs through:
 - ▶ Improve the communications in terms of detail and clarity
 - ▶ Provide points of contacts
 - ▶ Organize training events

Case Study: Microsoft's cooperation with Law Enforcement

- ▶ LE Tech 2008
 - ▶ Held in Redmond on April 28 – 30, 2008 for law enforcement only. It provides in-depth knowledge of Microsoft technology for forensics purposes.
- ▶ 12 training sessions in EMEA last year
- ▶ Microsoft LE Portal is a privileged point of contact for Law Enforcement where they can submit requests and questions

ISPs discovering cyber crime

- ▶ As ISPs monitor their networks and receive customer complaints, they are in a good position to discover emerging cyber crimes
- ▶ ISP initiated cyber crime cases is frequently the case for unsolicited communications (spam)
- ▶ The CoE guidelines suggest that ISPs share information regarding criminal incidents to law enforcement

The Spam King

- ▶ Microsoft initiates civil proceedings against Robert Soloway, a.k.a. The Spam King. A civil judgment was rendered in 2005 awarding Microsoft \$7.8 million in damages.
- ▶ Microsoft supplied evidence for the criminal proceeding and on March 14th, 2008, Robert Soloway pleads guilty during a criminal procedure and faces 26 years in prison and \$625,000 in fines. He is currently in prison awaiting sentencing.




Zotob virus

- ▶ Zotob was a computer virus affecting hundreds of companies. It was allegedly written as a work for hire by two Moroccan individuals and used for economic gain by a Turkish individual.
- ▶ Arrests of the suspects was made possible by the exemplary cooperation between Moroccan, Turkish, and American law enforcement together with Microsoft investigations teams.



MBAM Phishing – Criminal Referral to Bulgarian law enforcement

- ▶ Phishing is the crime of stealing personal data to commit fraud over the Internet.
- ▶ A number of fake emails purporting to be from Microsoft customer service representatives were sent asking Microsoft customers to input their credit card numbers on Microsoft looking web pages. The emails were not from Microsoft and neither were the servers receiving the information from the customers.
- ▶ Microsoft collected evidence and made a criminal referral to the Bulgarian National Services to Combat Organized Crime (NSCOC). With the evidence NSCOC arrested 8 individuals in 3 cities.



Evidence related to content on the
defendant's computer

Content whose mere possession is illegal

- ▶ Data found on a computer can be unlawful in nature:
 - ▶ Child exploitation images (Art. 9)
 - ▶ Copyright infringements (Art. 10)
- ▶ The unlawful file's creation and access dates may provide additional evidence on who used the files or when the picture was taken.
- ▶ The additional information is called meta-data and is useful as evidence but is also problematic as it can be forged.



Data from a computer crime found on defendant's computer

- ▶ Data that may not be unlawful in itself, can constitute evidence of a computer crime if its possession could only have been obtained through a computer crime such as illegal access or interception (Art. 2 and 3)
- ▶ There may be no evidence of the defendant committing the computer crime so he may only be accused of possessing personal data, trade secrets and additional investigation is needed to discover who committed the computer intrusion.



Computer log files


- ▶ The log files of software record an important amount of activity it performs.
- ▶ The operating system may record events such as when a computer was logged into or a file copied.
- ▶ User software may have their own log files such as the search history in Internet Explorer, or an accounting program that registers each modification or entry of a record by all users.



Meta data in computer files

- ▶ Digital files often contain Meta Data that is separate from the content of the data file. Examples are:
 - ▶ Date of the creation or modification of the file
 - ▶ Which software created the file
 - ▶ Who was the author of the file
 - ▶ A GUID identifying the computer
- ▶ Digital photos contain Meta Data in the EXIF format which can reveal:
 - ▶ The date and time of image capture,
 - ▶ The make, model, and serial number of the camera that took the picture,
 - ▶ Some newer cameras even embed the exact geographical coordinates of where the picture was taken through GPS technology





Securing the evidence from a computer

Securing the evidence

- ▶ If such data is found, the evidence can be secured through:
 - ▶ Seizure of the computer or storage system,
 - ▶ Copying the data,
 - ▶ An affidavit stating that data was observed.
- ▶ If the evidence was obtained through a seizure or through a copy, it must be ensured that the evidence is not later contaminated or that its whereabouts at all times cannot be accounted for.
- ▶ The computer forensics expert must describe the process followed to obtain the evidence and provide a log in order to ensure that there are no doubts as to the reliability of the evidence.
- ▶ Having multiple copies of the evidence allows the evidence to be reviewed independently.



The computer forensics expert

- ▶ Forensics is science that examines questions of interest to a judge.
- ▶ Electronic evidence is viewed as a technical subject-matter that often requires the assistance of a computer forensics expert
 - ▶ In criminal procedures
 - ▶ Police investigators
 - ▶ Hired technical experts
 - ▶ Civil procedures
 - ▶ Computer expert appointed by the Court
 - ▶ Computer expert appointed by the petitioner.



Forensics Practice Principles at the Scene of Crime

- ▶ Not to cause unnecessary input to the target machine
- ▶ Collect the volatile data including network, and memory information for investigation
- ▶ Documentation of execution flow for court presentation
- ▶ Backup passwords from the machine for future forensic purpose.



COFEE Computer Forensics Tool

- ▶ Computer Online Forensic Evidence Extractor is a tool to obtain evidence from a computer in a uniform, quick, and transparent way
- ▶ Design as a script and command line based live forensics tools that can be used by forensics investigator with zero knowledge
- ▶ Conduct live evidence extraction before the computer is powered down
- ▶ Runs from and stores the volatile evidence on a USB storage key



Volatile information

- ▶ Date, time of the examination
- ▶ Volatile memory
 - ▶ Memory Dump from Physical memory
 - ▶ SWAP drive
- ▶ Network connection
 - ▶ Open ports UDP, TCP
 - ▶ NetBIOS, neighboring network connection
- ▶ User Account
 - ▶ Users currently logged on
- ▶ Processes
 - ▶ Running processes
 - ▶ Running services
 - ▶ Scheduled Jobs
- ▶ Files
 - ▶ Open files
- ▶ Screen capture

