Collecting evidence in cybercrime investigations + public-private cooperation

Uwe Manuel Rasmussen
Legal Counsel
Microsoft Corporation

The use of electronic evidence in legal procedures is increasing

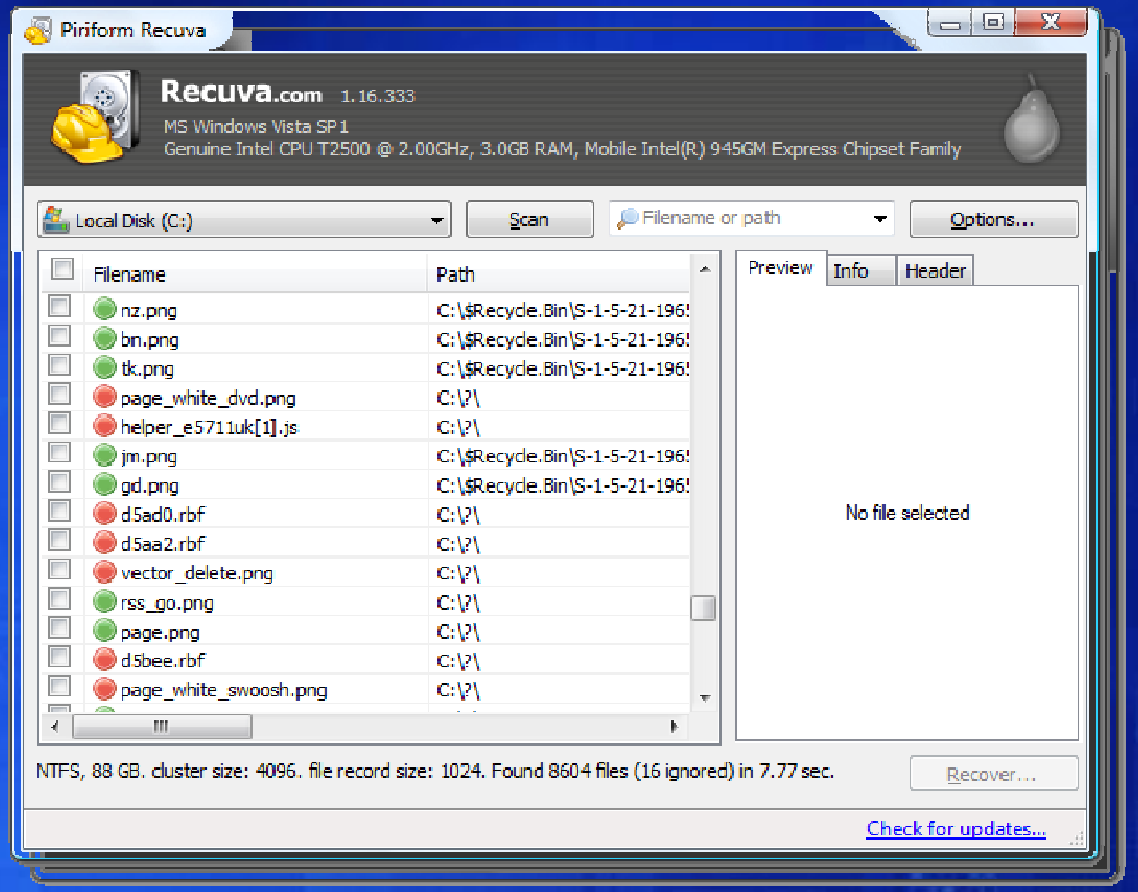
- Computers are used to communicate, for social interaction, writing contracts, and making purchases.
- Electronic evidence is common in cybercrime matters but is increasingly being used also in matters that don’t concern cybercrime.
- EU directive 1999/93 set requirements for electronic signatures
- EU directive 2000/31 provides validity to electronic contracts
- Electronic evidence may provide legal professionals access to more information and thus enhances the administration of justice.

Legally binding electronic documents

- 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.

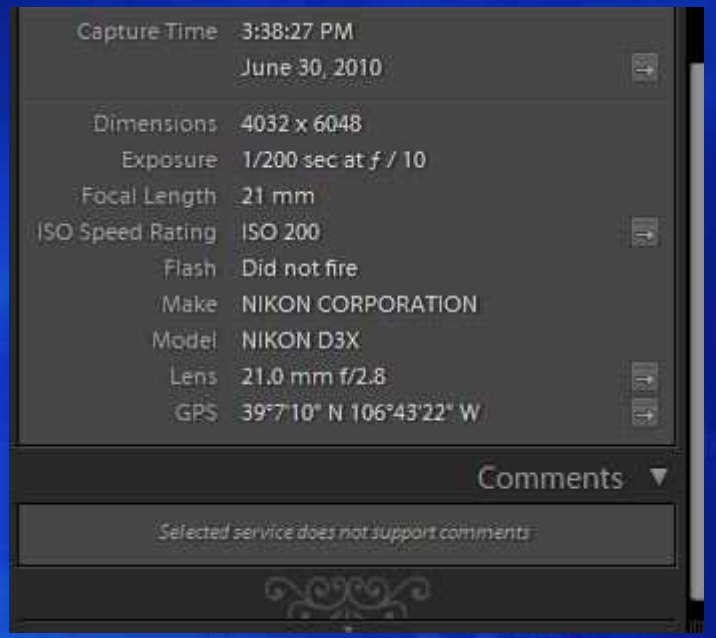
When is a computer file deleted?

- Files are not deleted but marked as « unwanted » when deleted.
- Files are stored in a grid on the storage medium.
- « Unwanted » files can be recovered from their place in the grid as long as a newer file has not been stored in the same place and thus overwritten the first file.



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




```
Rev. #1: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd"
Rev. #2: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd"
Rev. #3: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd"
Rev. #4: "JPratt" edited file "C:\TEMP\Iraq - security.doc"
Rev. #5: "JPratt" edited file "A:\Iraq - security.doc"
Rev. #6: "ablackshaw" edited file "C:\ABlackshaw\Iraq - security.doc"
Rev. #7: "ablackshaw" edited file "C:\ABlackshaw\A;Iraq - security.doc"
Rev. #8: "ablackshaw" edited file "A:\Iraq - security.doc"
Rev. #9: "MKhan" edited file "C:\TEMP\Iraq - security.doc"
Rev. #10: "MKhan" edited file "C:\WINNT\Profiles\mkhan\Desktop\Iraq.doc"

Most Word document files contain a revision log which is a listing of the last 10 edits of a document, showing the
cannot be viewed in Microsoft Word. However I wrote a small utility for extracting and displaying revision logs and
```

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.

Example of search history

Today

11:21pm Searched for sarajevo national museum

11:21pm Searched for sarajevo bill gates cafe

12:06am Searched for Sabam / NetLog - Viewed 2 results

- Netlog remporte un premier combat contre la Sabam - Datanews.be - mews.be
- The 1709 Blog: Another ECJ reference on monitoring and SABAM - blogspot.com

Yesterday

8:12pm Searched for Peter Tudvad - Viewed 1 result

tudvad_talerstol.jpg
600 x 443 - 255k

8:09pm Searched for Andreas Brigelsgaard - Viewed 3 results

- News from Søren Kierkegaard Research Centre - reference-global.com
- Søren Kierkegaard Forskningscenteret - ku.dk
- Tårnby Gymnasium: TG-Nyt 9 - taarnby-gym.dk

8:09pm Searched for Peter Tudvad

7:10pm Searched for mcdonalds 1955 - Viewed 1 result

McD_Germany_1995.jpg
651 x 429 - 39k

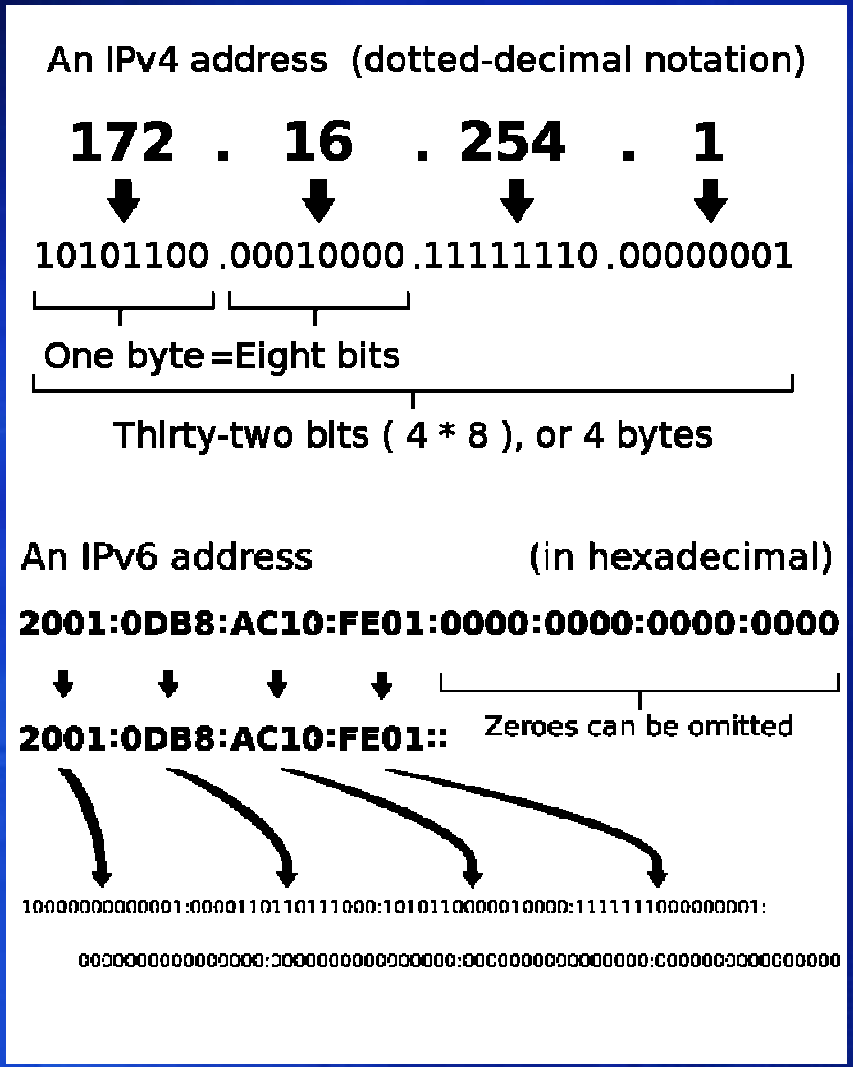
Browser's Internet search history

- 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.

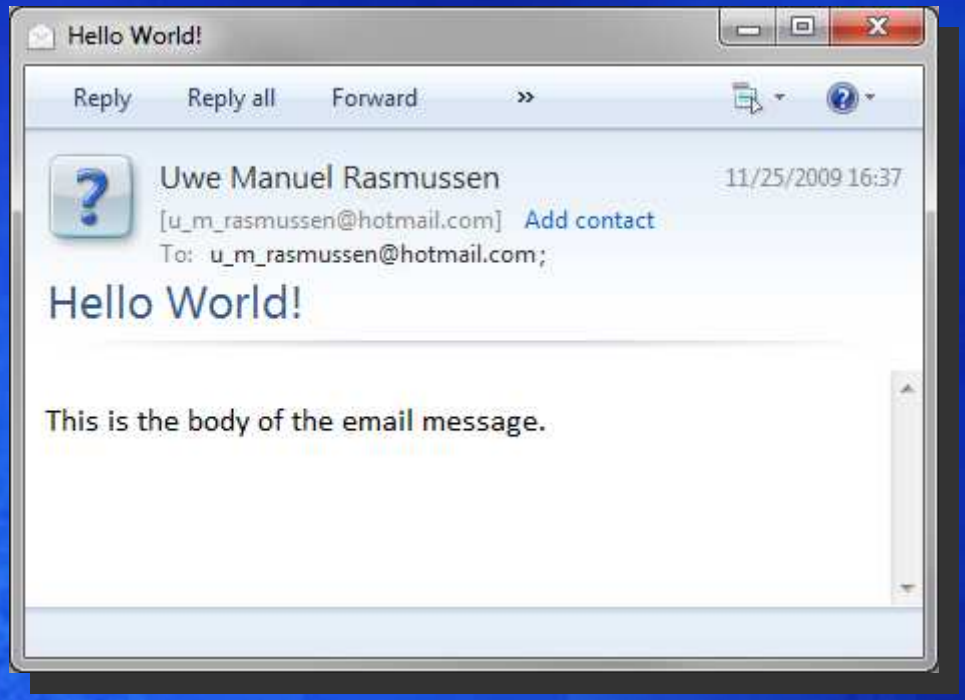
What IP numbers look like

- 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.



A simple email



Email header

- Emails record their travel path in section of the email called the header.
- Headers may be forged but they will still reveal from where the email originated.
- Email may however have been sent from compromised computers and botnets.

```
Return-Path:     <emailsender@send.com>

Delivery-Date:   Tue, 24 Apr 2007 11:48:26 +0200

Received:        from [66.111.4.28] (helo=out4.smtp.messagingengine.com)   by
mx.kundenserver.de (node=mxeu4) with ESMTP (Nemesis), id 0MKqlY-1HgHdJ2QaU-0002JI
for inbox@receive.com; Tue, 24 Apr 2007 11:48:26 +0200

Received:        from compute2.internal (compute2.internal [10.202.2.42])   by
out1.messagingengine.com (Postfix) with ESMTP id 0BC67217E6A; Tue, 24 Apr 2007
05:48:32 -0400 (EDT)

Received:        from heartbeat1.messagingengine.com ([10.202.2.160]) by
compute2.internal (MEProxy); Tue, 24 Apr 2007 05:48:24 -0400

Received:        from [213.199.128.153] (tide95.microsoft.com [213.199.128.153])
by mail.messagingengine.com (Postfix) with ESMTP id C57BA37C0A   for
<inbox@receive.com>; Tue, 24 Apr 2007 05:48:23 -0400 (EDT)

Message-ID:      <462DD366.6020109@send.com>

Date:            Tue, 24 Apr 2007 11:48:22 +0200

From:            Email Sender <emailsender@send.com>

User-Agent:      Microsoft Windows Mail 6.0.6000.16386

To:              inbox@receive.com

Subject:         Hello World!

Content-Type:    text/plain; charset=ISO-8859-1; format=flowed

Content-Transfer-Encoding: 7bit


This is the body of the email message.
```

Service providers

- Service providers such as the Internet Access Provider hold information about the user that the user cannot delete.
- They are of the only link to identify the real link between cyber-personality having committed the crime and the real world person who can be prosecuted.

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.

Digital Crimes Consortium

- 400 participants from 40 countries attending 72 different sessions by 90 speakers. Participants were a mix of law enforcement, industry, government, and academia.

Digital Crimes Consortium

Conference 2010

October 12 - 15, 2010 | Montreal, Canada

AGENDA

** All sessions designated as a "Lab" are limited in capacity and required advance sign-up.

Monday, October 11, 2010 - Pre-Registration (Optional)

17:00 - 19:00	**Pre-Registration at Delta Centre-Ville, Lobby**	

Tuesday, October 12, 2010 - Registration, Early Hacker Underground Labs and Conference Opening

	TIME	TOPIC	PRESENTER	ROOM
Tuesday	09:00 - 13:00	**Registration at Delta Centre-Ville, Floor C**		
	Due to the holiday on Monday, we will officially begin the conference at 1:00 on Tuesday, however, if you are able to arrive earlier, we invite you to attend one of the following two hands-on sessions that will explore the darker side of the Internet. Please plan to arrive early and register for these sessions if your travel plans permit.			
	10:00 - 12:00 Lab 1	**Mobile Threats: The Risk You Carry in Your Pocket--A Presentation Dealing with Aspects of Mobile (In)Security** The capabilities of the mobile phone have developed substantially in the past few years and have provided us with the capability to run our lives from a sleek and stylish device. You can now use a mobile phone to read and send email, surf the web, navigate using Google Earth and - most crucially - to run exploit code. In addition to the	**Nils** Principal Information Security Researcher, MWR InfoSecurity	**Regence A,B&C**

Facilitating evidence exchange

- Budapest Convention on Cybercrime
  - Ensures dual-incrimination
  - Instaures procedural measures to preserve evidence
- Complaints regarding cybercrime need to be collected
- Some evidence needs to be examined in advanced labs for example for reverse engineering of malware.

Microsoft®

Your potential. Our passion.™