Incident Management

Trooper 2008
München

Oberstleutnant Volker Kozok

final word on language and nutrition

The Japanese eat very little fat and suffer fewer heart attacks than the British or Americans.

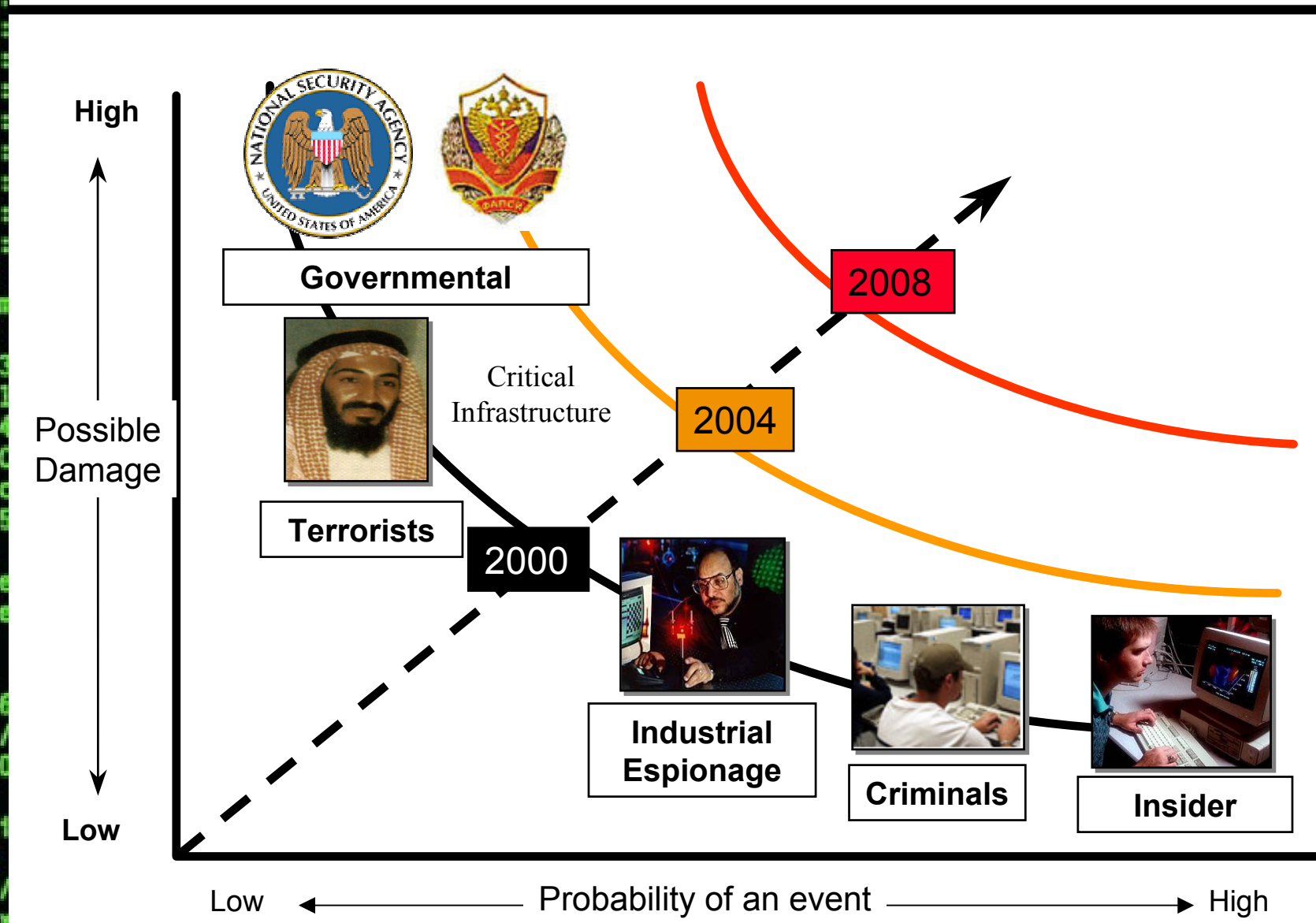
The French eat a lot of fat and also suffer fewer heart attacks than the British or Americans.

The Swedish drink very little red wine and suffer fewer heart attacks than the British or Americans.

The Italians drink excessive amounts of red wine and also suffer fewer heart attacks than the British or Americans.

CONCLUSION: Eat and drink what you like. Speaking English is apparently what kills you.

Cyber Threat Profile



Be prepared!


THE CHRISTIAN SCIENCE MONITOR
Bennett
ALWAYS BE PREPARED
I thought you were bringing the paint.
ANTI-TERRORISM

A Question of definition

An incident is any event that deviates from the standard and expected operation of a system or service

Standard - who defines the standard?
Expected operation - I had expected Microsoft Fatal Error!

An incident is the act of violating an explicit or implied security policy.

Security policy – what´s that?
My system can´t be violated because I have no policy!

An incident occurs, if IT security is impaired/jeopardized by an IT security gap or a breach of IT security.

What is with the loss of credit or reputation?
What is with a breach of duty or infringements?

A Definition with questions

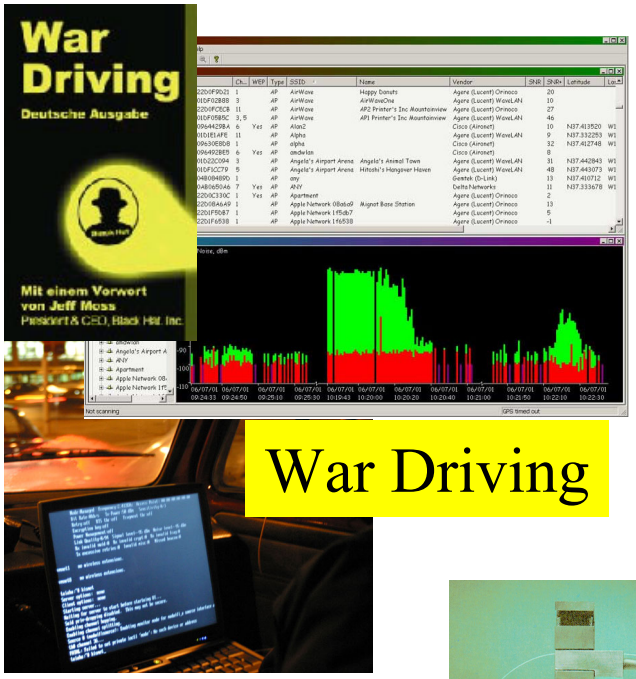
What can be happen?
What is the risk for my division or company?
How can I minimize the risks?
If IT-Security, Personnel Data Protection, Security Service, Disaster Recovery ... doesn´t work – what´s than?
How can I react if my company is impaired or jeopardized?

What is an incident?

Incident Categorization

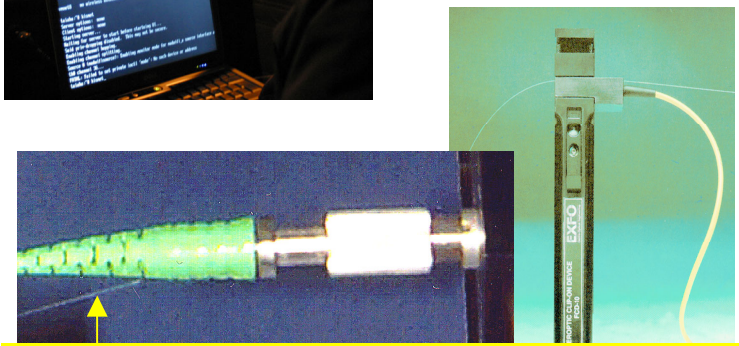
- Increased access
- Disclosure of information
- Corruption of information
- Denial of service
- Theft of resources

Increased access



War Driving

Social Engeneering



Tapping Fibre Optical Cable

Scanning and Sniffing

Disclosure of information

Keylogging

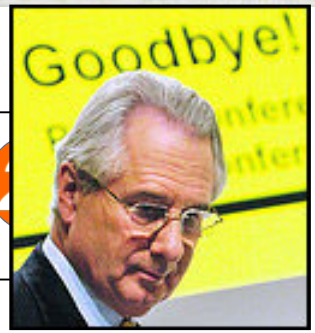
Printer - Copying

spying

Bundesnachrichtendienst

Liechtensteining

finanzamt
Der Finanzamt-Finder



Disclosure of information

US-Ministerium vermisst mehr als 1000 Laptops

25. Sep 2006 15:24

Mobile Loo(U)ser

Corruption of information

boston.com Local News

GREATER BOSTON | BOSTON GLOBE | EVENTS | YELLOW PAGES

SEARCH BETA

Home News A&E Business Sports Travel Your Life Cars Jobs

Today's Globe Local Politics Opinion Magazine Education NECN

HOME > NEWS > LOCAL

Data for 450,000 mistakenly released

The Boston Globe

Social Security numbers on disks

By Michael Naughton, Globe Correspondent | Octo

The Massachusetts Division of Professional Licensure h
internal probe and announced plans to review its protoco
Social Security numbers of about 450,000 licensed profe

APR-01-2002 MON 10:21 AM FAX NO.

Form W-9095 (Rev. July 2001) Department of the Treasury Internal Revenue Service

Application Form For Certificate Status/ Ownership For Withholding Tax

(Fax this Form to 1-014-470-0245)

Please check the box(es) that apply to this application: ☐ New ☐ Reapply ☐ Revised

Revision Reason:

☐ Online Filing (check only if you w returns information for taxpayers w returns at home, via an On-line Internet site, or fax mail (see fax mail number below))

☐ Fax mail number in the foreign country if applicable

Type or print name (first, middle, last)

☐ Tax Payer Identification Number (TIN) ☐ Social Security Number (SSN) (State as applicable)

Title ☐ Mr. ☐ Mrs. ☐ Others Sex ☐ Male ☐ Female

U.S. Citizenship? ☐ Yes ☐ No ☐ Legal resident alien

Date of Birth: Month Day Year

Place of Birth:

Spouse's Name (if any):

Marital Status

Country of Per

Account Name and Date it Was Opened:

PIN Number (if any):

Password or Code (if any):

Index Number (if any):

Faked US-Standard Form W-9095

BDJ

BDJ unterstützt Folterforderung von Bundesinnenminister Schäuble

Berlin/Karlsruhe, 30. Dezember 2005

Der Bund Deutscher Juristen (BDJ) unterstützt die Folterforderung von Bundesinnenminister Dr. Wolfgang Schäuble. Anlässlich der aktuellen Debatte stellt der BDJ-Vorsitzende und Strafrichter am Bundesgerichtshof Dr. Claus Grötz klar: „Das Leben unschuldiger Opfer besitzt einen höheren Wert als die körperliche Integrität von Verbrechern. Wir müssen jetzt Tabus brechen. Die Gewinnung von Aussagen mittels leichter Foltermaßnahmen und die Verwertung solcher Aussagen sind zukünftig möglich zu machen. Unsere Behörden stehen unter ungerechtfertigtem moralischen Druck, wie der Fall Gäfgen und die Terroristenverfolgung zeigen."

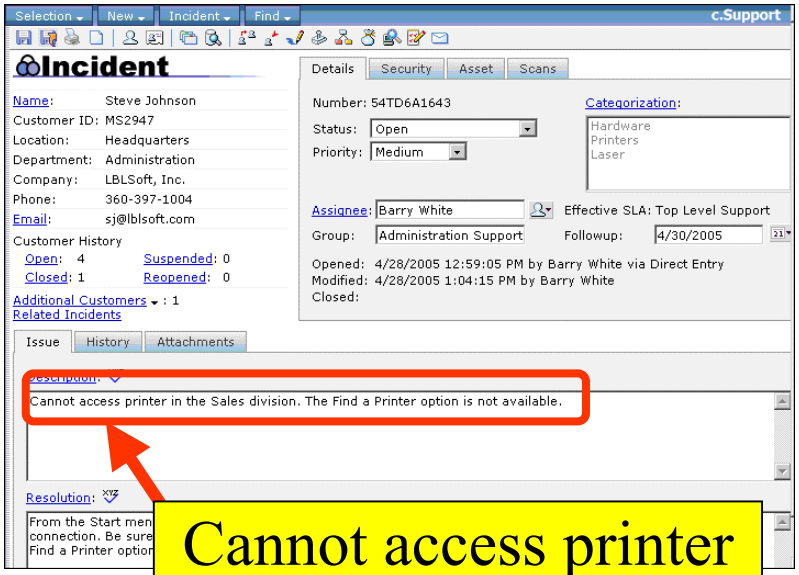
The Register

Supermarket loses 4.2 million credit card details

Supermarket identity sweep

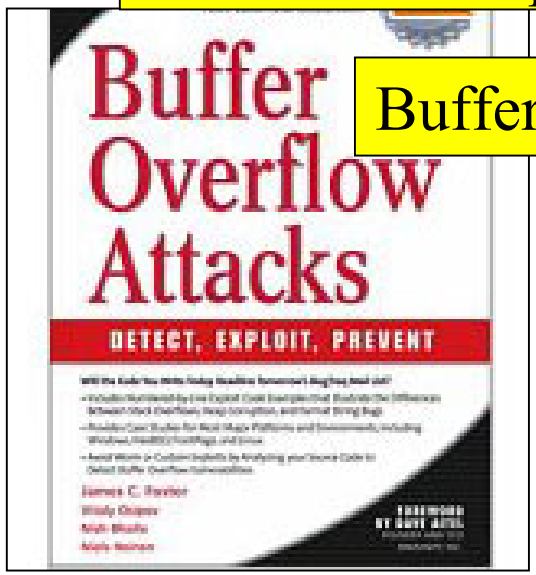
Personal data for 650,000 customers vanishes into thin air

Denial of service

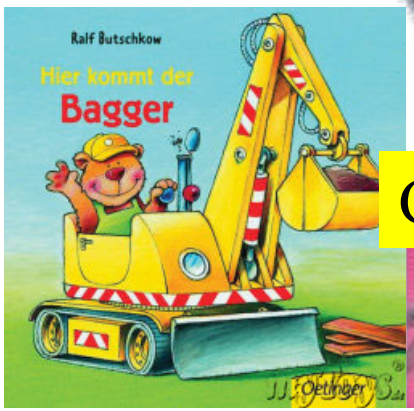


Cannot access printer

DDoS



Buffer Overflow

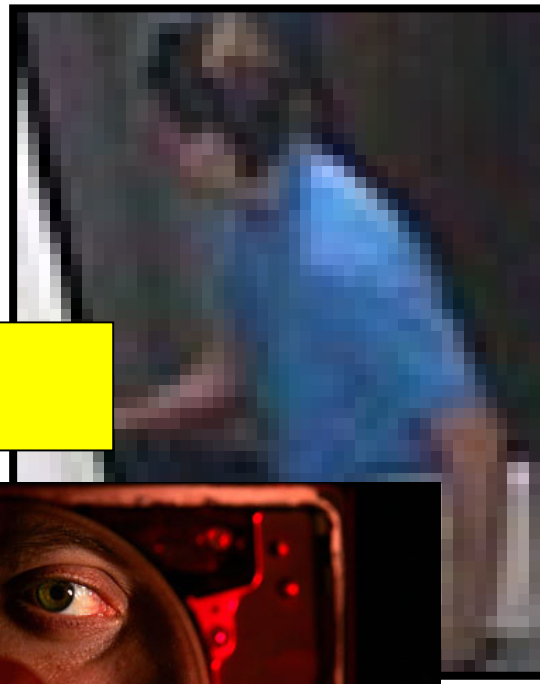


Cable separation

Denial of service - Disaster

Denial of service

Theft of resources



Hardware Theft

Sofware & Media Theft

Vietnam Cable Theft

Case Example – Web-Defacement

heise online - Nach Hack überprüft Bundeswehr Sicherheit ihrer Website

Sie sind Gast
Einloggen | Registrieren

Suche ...

7-Tage-News
News-Archiv
News unterwegs
Newsletter
News einbinden

Telefontarife
Internettarife
Internetstörungen

Software/Download
IT-Markt
heisetreff

Leserforum
English Pages

Abo & Heft
Veranstaltungen
Kontakt
Mediadaten

Jetzt testen: 3 iX-Ausgaben

Nach Hack überprüft Bundeswehr Sicherheit ihrer Website

vorlesen

"Am Sonntag, den 19. Januar, haben sich bislang unbekannte Täter in den Bundeswehrserver in Strausberg gehackt und eine Umleitung von der Website bundeswehr.de auf eine andere gelegt", bestätigte ein Sprecher der Bundeswehr gegenüber heise online. Für 90 Minuten war die Site der Bundeswehr nicht

Hilfe

Top-Meldungen

Dell liefert ab heute Ubuntu-PCs aus

Grünes Licht für Verschärfung der Hackerparagraphen

Plattformunabhängiger OpenOffice-Wurm aufgetaucht

US-Analysten prophezeien das Ende von Skype & Co.

Aktuelle Meldungen

Microsoft vertagt Entwicklerkonferenz

Facebook veröffentlicht Programmierschnittstelle

VA Software benennt sich in Sourceforge um

RFC gegen Spam

Arabische Regulierer wollen Roaming-Preise senken

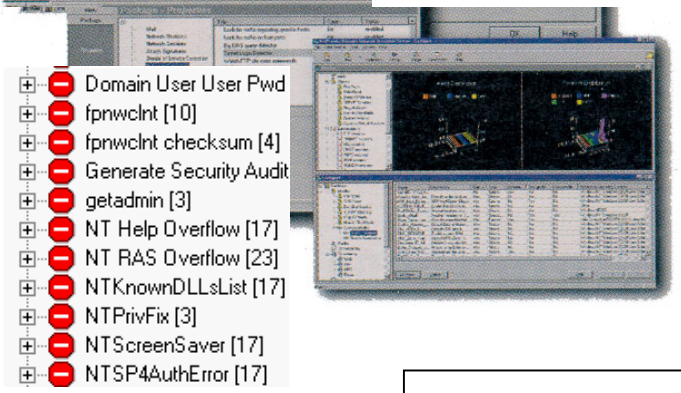
Chat-Verhalten von Kindern wird erforscht

Microprocessor Report:

IMT - Incident Management Team

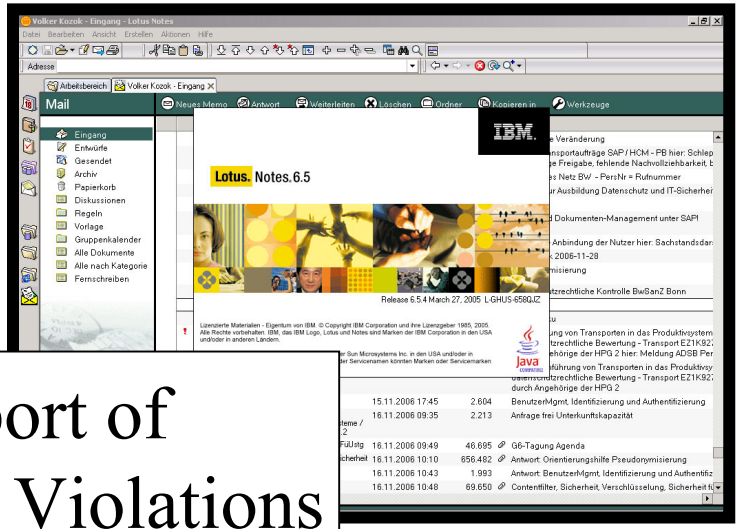
„Wake up call“ - Identification

Alert/
alarms



News &
Reports

Logs/
Triggers

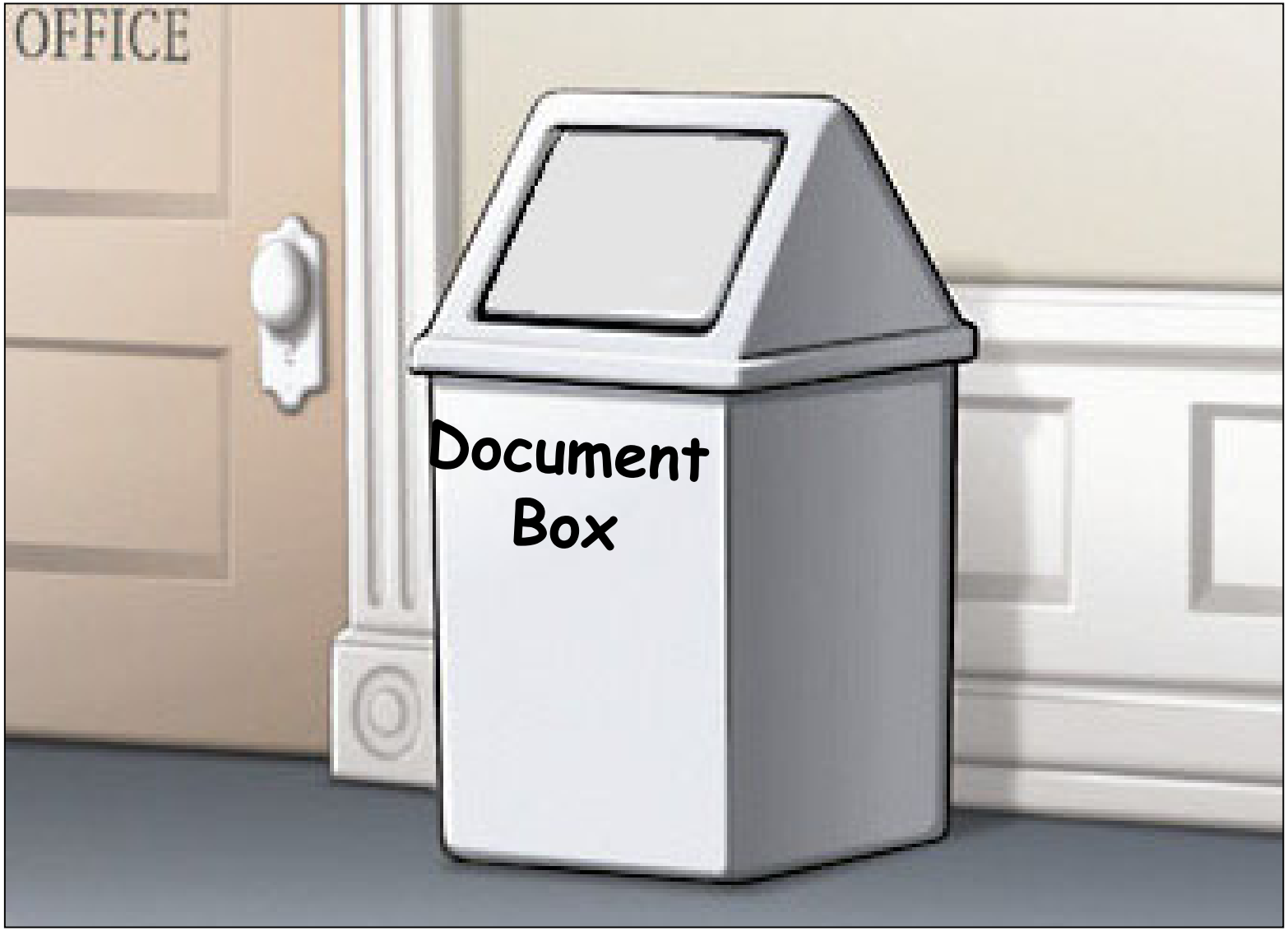


Report of
Security Violations

Immediate Response - Bw

- Step 1.1 Carry out Initial Analysis and Start Documentation
- Step 1.2 Preserve the Scene - Screening
- Step 1.3 Contact IT specialist personnel
- Step 1.4 Preserve the Evidence
- Step 1.5 Determine the Extent and Perform a Risk Analysis
- Report to the Management

Step 1.0 Document everything



Questions

- Who has carried out the action?
(Suspects, administrator, disciplinary superior, IT security officer, superior agency, service provider, legal adviser)
- What action was carried out?
(e.g. report, backup, audit, interrogation)
- Where was the action carried out?
(e.g. search of official room building 16, data backup in the server room building 73, readout of log files in the IT security officer's official room, photos in room 166, etc.)
- How and with what means was the action carried out?
(data backup on CD, preserving evidence with digital camera, analysis of computer with the forensic tool "Encase", etc.)

Step 1.0 Document everything

Capture everything that occurs in detail:

- names
- times
- events as they actually occurred
- Date-Time-Group (DTG)
- action
- List of all computer systems, devices and applications affected by the investigation
- Hard-/Software information
- Remarks (incl. reference to documentation)

Log Book (example)

Serial No.	DTG	Action	Remarks
1	23 Feb 08 09.45	Sys admin Mr.Smith reports IT security violation	
2	23 Feb 08 10.25	Checking of the user account by IT security officer from Admin workstation 03 (R.105)	Image copied and saved on CD.
3	23 Feb 08 10.45	Report to management. Order to initiate investigation	
4	23 Feb 08 11.45	Checking of Client 1074, network address 123.123.145.23 in room 143	
5	23 Feb 08 12.13	Securing data at Admin Mr.Newman. Seizure of data carriers.	Storage in room 143
6	23 Feb 08 12.55	Locking of user account by sys admin Mr. Hubble.	
7	23 Feb 08 14.05	Consulting hotline at CERT XY about further action	
8	24 Feb 08 09.05	Interrogation of suspect by CIO Mr.Jones	Record of interrogation held by Personnal Officer
9	24 Feb 08 10.50	IT security violation report filed with IT security officer of the organization area	Enclosure 12

Step 1.0 Document everything

Step 1.1 Initial analysis

Detection – First Reaktion – Action

„Need to know princip“
„Undercover investigation“

Immidiate Reaktion

Motto from the Signal Corps
„Thinking – pushing – speaking“

Step 1.2 Preserve the scene-screening

- closing off the scene to prevent access of unauthorized personnel
- identifying the staff working/employed in the office
- preventing the perpetrator or perpetrators from further accessing the IT systems of the agency
- In addition, photographs should be taken of rooms, IT configurations and evidence, before making any changes to the scene.

Stop the „Experts“

Step 1.3 Notify appropriate personnel

Internal

- CIO
- Administrators (Network & Security)
- Security officer
- Security analyst/ Forensic specialist
- Auditor

External

- Industrial CERT
- Law Enforcement
- Forensic specialist
- Recovery specialist

Additional

- Legal Advicer
- Public Relations

Step 1.3 Notify appropriate personnel

Assistant Technical Incident Officer

- available
- silent
- trained
- decisive
- knowledgeable
- assertive

Built up IRC
Incident Response Capability

Step 1.4 Preserve the evidence

Ensure the integrity and availability of the evidence!

- Destruction
- Theft
- Changes
- Loss of data
- Tainting the evidence

Done by suspects, attacker
AND
own „IT-experts“

Stop the „Experts“

Step 1.5 Determine the extent

- Which and how many systems and data are actually or likely affected?
- Are there internal or external activity?
- Are other computer affected?
- Are IT security systems affected?
- Is the threat likely to spread?
- Are IT systems of external parties affected?
- Is the incident occurred or ceased?

The risk assessment/**initial risk analysis** may result in additional measures to maintain IT security.

Step 1.5 Verify the Incident

Results of Verification:

- verified and proceed
- undetermined and proceed
- refuted and terminate

Reporting

A report should include the following information:

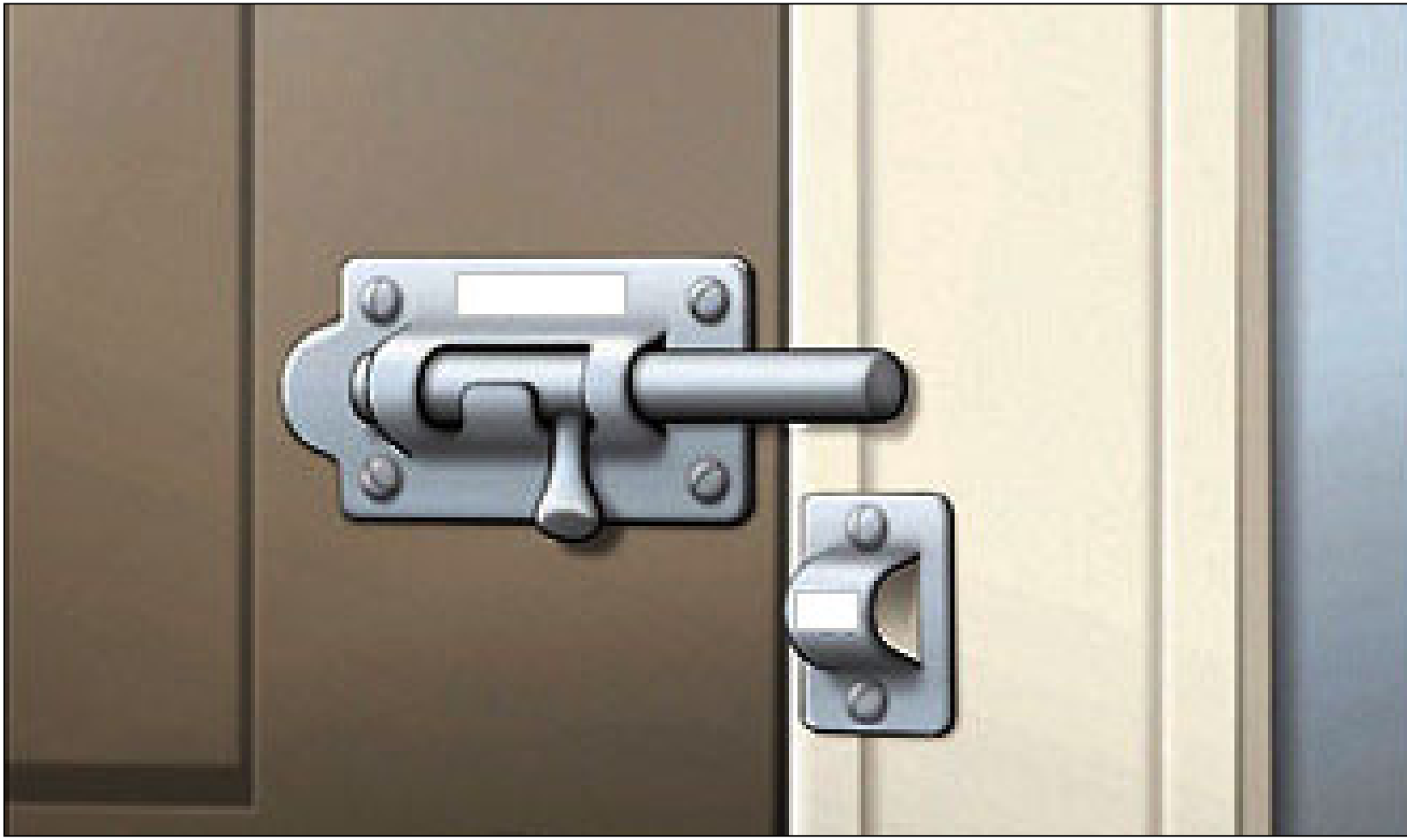
- Incident designation;
- activity designation;
- point of contact/telephone number;
- an account of the facts (e.g. a description of IT equipment/software/project);
- damage established;
- measures taken.

Document everything

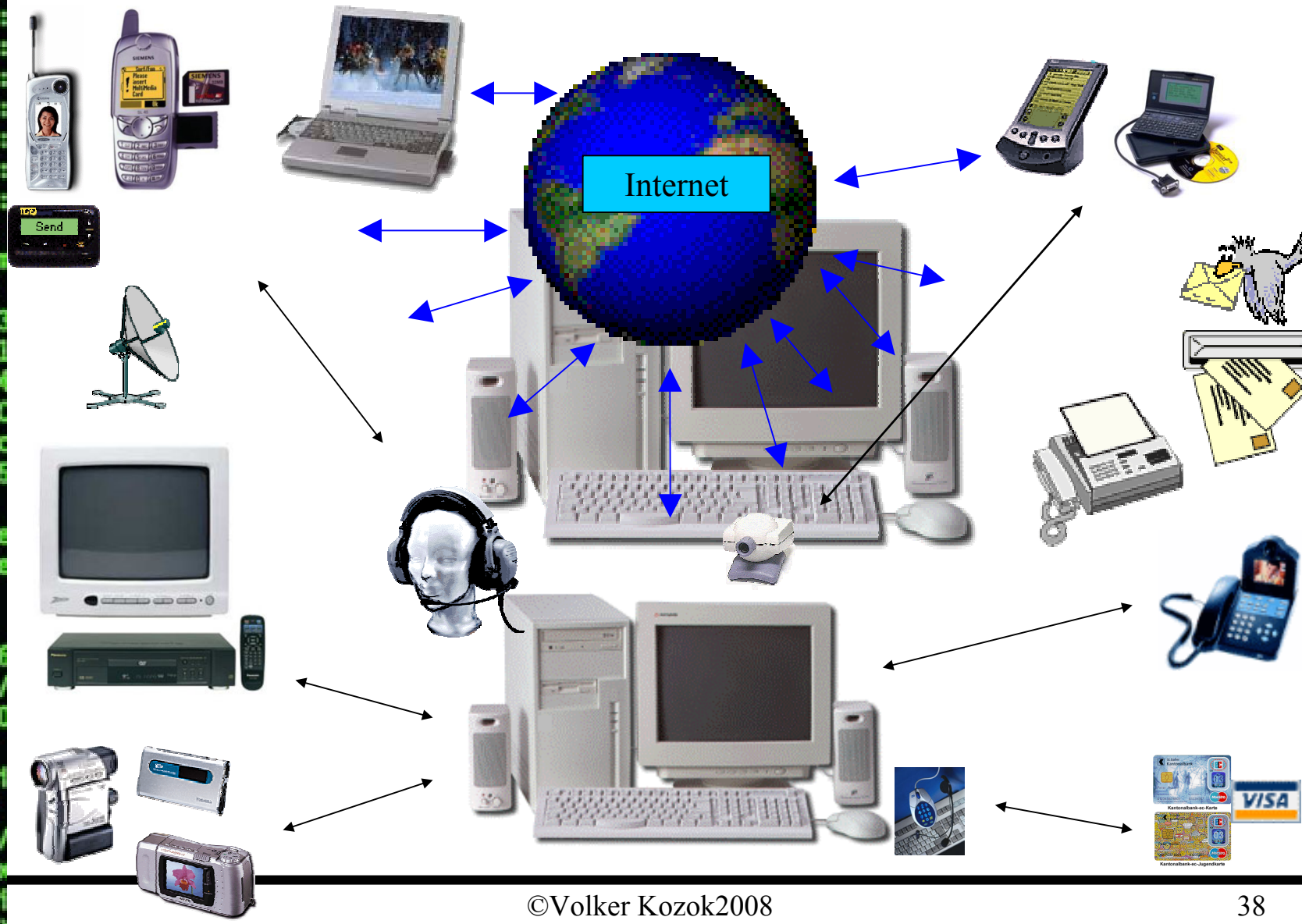
Step 2.1 Implementation of immediate measures to safeguard IT Security

- Installation of patches or updates
- Setting of filters in Firewall/Proxy systems
- Performance of workarounds
- Closure of ports
- Deactivation of user accounts, applications or other software
- Shutdown of clients
- Shutdown of domains
- Closure/blocking of Firewall

Step 2.1 Implementation of immediate measures to safeguard IT Security



Step 2.2 Collecting evidence



Step 2.3 Analysis evidence

DIGITAL FORENSICS

Electronic Crimes Task Force

NW3C

INTERNET CRIME COMPLAINT CENTER
... an FBI - NW3C Partnership
Home | File a Complaint | Press Room | About IC3 | Contact Us

Forensic guidelines / principles

1. No action should change data
   - Write protection, sterile media, Bit stream copy
   - first incident response
2. People dealing with evidence should be competent
3. A complete audit trail / documentation is necessary
   - Photo, video, printouts, log book
4. Identification / verifycation (Hash)
5. A forensic officer should not be part of a investigation unit

Forensic equipment and principles

- Portable equipment
  - Forensic workstation, write protection, video, camera,
  - software tools (Encase, Ilook, FTK, Linux, Smart, …)
- Laboratory
  - All kind of standard machines, password/decryption clusters
  - Different networks, storage capacity
  - software tools (Encase, Ilook, FTK, Linux, Smart, …)
- Communication plattforms
  - Local
  - European High Tech Crime Web - EVPN

Image production

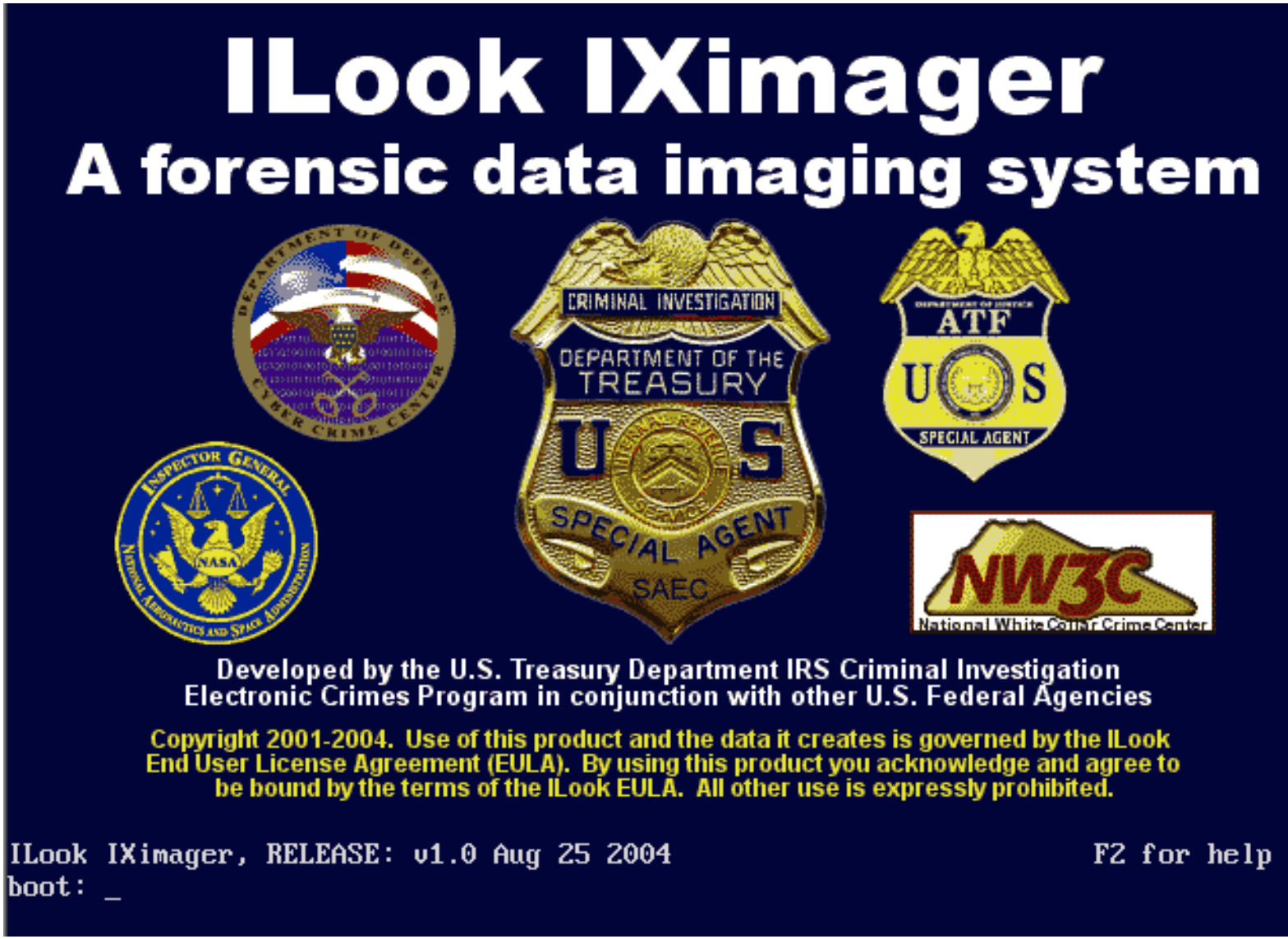
Writeblocker with Firewire-Interface connected to the Storage PC

Boot CD with ILook XImager

Court exhibit

Back-Up Hard-disk

Step 2.3 Analysis evidence



Analysis of internet use!

ILook © v8.0.9 | => TestCase (1) => Humpe (2) => Humpe (3)

Case Management | Setup | Help (F1) | File View | Map View | Thread Status | Hex View | File View | Folder Properties | Search Results | Stream Analysis

Case Organizer
Cases
Humpe (2)
Archived Cases
SAVE

Associated Documents (0)
Evidential Media
Humpe (3)
Attached Media
Auto load saved filesystem mapping
TestCase
Work on this one?
User Category Definition (0)
Add Evidence

Humpe (3), Size 6,006 GB, Unused 63,000 KB
0-FAT16, Size 1,961 GB, Free 800,157 MB
Free Space
Config.Msi
Dokumente und Einstellungen
Administrator
Anwendungsdaten
Cookies
Desktop
Druckumgebung
Eigene Dateien
Eigene Bilder
Favoriten

stem Container Salvage
Categories
iminated Files
le Name Categories
America OnLine (AOL)
Archives
Audio
Database
Email
Encrypted Volumes

File List | Thumb Nail View | Disk View | Log | Salvage Ops | Hash Ops | Search Ops | Script Ops | Dictionary Ops | FileTime Diary

db
Drag a column header here to group by that column
\Dokumente und Einstellungen\Administrator\Cookies\ 128 object(s), Folders (0) Files (127)

Name	Size	Type	Attributes	Created Date	Last Modified Date	Last Accessed Date	Stream Name
..	15	Parent Folder		24.Apr.2005 20:20:36...	24.Apr.2005 20:20:38...	24.Apr.2005 00:00:00...	Default
INDEX.DAT	32.768	DAT	A---	24.Apr.2005 20:20:58 +02	24.Apr.2005 23:03:10 +02	24.Apr.2005 00:00:00 +02	Default
administrator@ivwbox[1].txt	75	txt	A---	24.Apr.2005 22:02:28 +02	24.Apr.2005 22:02:30 +02	24.Apr.2005 00:00:00 +02	Default
ILook717_administrator@gmx[1].txt	183	txt	A---	24.Apr.2005 22:03:54 +02	24.Apr.2005 22:03:56 +02	24.Apr.2005 00:00:00 +02	Default
administrator@gmx[2].txt	265	txt	A---	24.Apr.2005 22:04:10 +02	24.Apr.2005 22:04:12 +02	24.Apr.2005 00:00:00 +02	Default
administrator@gmx[1].txt	265	txt	A---	24.Apr.2005 22:22:18 +02	24.Apr.2005 22:22:20 +02	24.Apr.2005 00:00:00 +02	Default
administrator@servedby.advertising[1].txt	115	txt	A---	24.Apr.2005 22:22:56 +02	24.Apr.2005 22:22:58 +02	24.Apr.2005 00:00:00 +02	Default
administrator@advertising[1].txt	88	txt	A---	24.Apr.2005 22:22:56 +02	24.Apr.2005 22:22:58 +02	24.Apr.2005 00:00:00 +02	Default
ILook718_administrator@paycounter[1].txt	87	txt	A---	24.Apr.2005 22:39:30 +02	24.Apr.2005 22:39:32 +02	24.Apr.2005 00:00:00 +02	Default
administrator@counter11.sextracker[1].txt	90	txt	A---	24.Apr.2005 22:39:30 +02	24.Apr.2005 22:39:32 +02	24.Apr.2005 00:00:00 +02	Default
ILook719_administrator@sextracker[1].txt	108	txt	A---	24.Apr.2005 22:39:30 +02	24.Apr.2005 22:39:32 +02	24.Apr.2005 00:00:00 +02	Default
administrator@xxxcounter[1].txt	81	txt	A---	24.Apr.2005 22:39:34 +02	24.Apr.2005 22:39:36 +02	24.Apr.2005 00:00:00 +02	Default
administrator@www.gfi[1].txt	73	txt	A---	24.Apr.2005 22:40:24 +02	24.Apr.2005 22:40:26 +02	24.Apr.2005 00:00:00 +02	Default
administrator@www.gfi[2].txt	73	txt	A---	24.Apr.2005 22:40:50 +02	24.Apr.2005 22:40:52 +02	24.Apr.2005 00:00:00 +02	Default
administrator@www.gfisoftware[1].txt	80	txt	A---	24.Apr.2005 22:41:06 +02	24.Apr.2005 22:41:08 +02	24.Apr.2005 00:00:00 +02	Default
administrator@google[1].txt	133	txt	A---	24.Apr.2005 22:46:30 +02	24.Apr.2005 22:46:32 +02	24.Apr.2005 00:00:00 +02	Default
ILook720_administrator@www.tamos[1].txt	84	txt	A---	24.Apr.2005 22:46:54 +02	24.Apr.2005 22:46:56 +02	24.Apr.2005 00:00:00 +02	Default
ILook721_administrator@www.tamos[2].txt	187	txt	A---	24.Apr.2005 22:46:54 +02	24.Apr.2005 22:46:56 +02	24.Apr.2005 00:00:00 +02	Default
ILook722_administrator@www.tamos[1].txt	187	txt	A---	24.Apr.2005 22:46:54 +02	24.Apr.2005 22:46:56 +02	24.Apr.2005 00:00:00 +02	Default

IT forensic training

- Constant need
  - 1/3 of working time
  - Minimum of 30 days per year
- budgets
- Very few special forensic trainings
  - International, expensive
- Lack of national / international cooperation

Step 2.4 Evaluation

The evaluation of the technical analysis should be confined to the description of the technically comprehensible events.

The technical evidence shall be verified, as far as possible, by interrogations.

Step 2.5 Archiving evidence

All evidence should be securely archived and stored

- Original evidence
- Back-up copy
- Reports
- Supporting documents
- Log-Book

Step 3.1 Additional troubleshooting options

- deletion of infected files/directories
- reconfigurations
- updates
- installing images
- restart of IT systems.
- reconfiguring firewall rules
- installing hotfixes

Step 3.2 Additional recovery options

When information/data were destroyed or manipulated due to an incident, measures must be taken to recover these information/data. In this case, measures in accordance with the agency's data protection concept must be taken in cooperation with the administrator (e.g. backups/recovery).

Incident Management Pocket Card

1. This pocket card is not a replacement of the Incident Management Guide.
2. Stay calm! Take appropriate actions. Check the accountability of the report, verify the facts. If you don’t know what to do, ask an expert.
3. When personnel-related data are affected, consult the data protection commissioner of the agency.
4. Document everything! Take pictures, if possible.
5. Consider all unknown activities to be harmful. If the computer runs processes that are unknown to you, switch it off! (emergency switch-off) Do not perform a regular shutdown on a computer with a suspicious IT security incident!

Incident Management Pocket Card

6. When you notice download or upload activities, pull the power plug or interrupt the modem connection.
7. Prohibit unauthorized actions! IT or technical staff of othe areas required for support only acts **as directed.** Administrators are **no** investigators, they support you in the preservation of evidence.
8. Ask all persons you do not need for the preservation of evidence to leave the affected rooms.
9. Prevent the suspected person from gaining further access to the IT systems!
10. **Never** accept help from the suspect! Ask for the passwords and do not let the perpetrator, for example, perform the logon process him or herself!
11. If anything fails, pull the plug!

Thank you for your attention!