

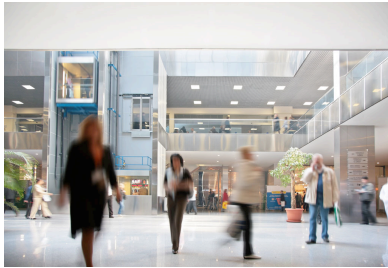
DATAEYE CONSULTING SECURING WORLD'S FUTURE



***DataEye Forensic Services
Data Sheet***



STEP BY STEP APPROACH, ALWAYS IN CONTROL



OBJECTIVE

Discover the vulnerabilities
Identify the attacker
Collect and archive the evidences
Prepare evidences for court
Damage Estimation

PRINCIPLES DURING EVIDENCE COLLECTION

Capture accurate information
Keep detailed notes with an automated script
Collection first, analysis later
... and all RFC 3227

EVIDENCE COLLECTING ORDER

CPU register and cache, Process lists,
Network connection, RAM memory,
Open files, Routing and ARP tables,
Temporary file systems, Hard disks,
Remote log files, Physical configuration,
Backup media



PREPARATION

The investigator must be properly trained
The tools to be used should be validated
The investigator should determine the proper tools to be used.
General information should be gathered
Investigation scope needs to be determined.

COLLECTION AND ARCHIVING EVIDENCE

Establish and maintain the chain of custody.
Document everything
One should not examine digital information unless one has the legal authority to do so.

SECURING EVIDENCE

The investigator should use a write blocking tool.
Calculate a cryptographic hash of an evidence file and to record that hash in the investigator's notebook.
The defensibility of the evidence often relies on a consistent and appropriate process.



ANALYSIS AND DATA EVALUATION

All digital evidence must be analyzed to determine the type of information that is stored upon it.
Manual review of material on the media, reviewing the Windows registry, discovering and cracking passwords, keyword searches for topics related to the crime, and extracting e-mail and pictures for review.

WRITTEN REPORT

Formalia
Investigation Objectives
Proceeding
Discoveries (facts)
Interpretation of facts
Summary
Sources
Appendix with data collection for review.

LEGAL SITUATION IN ROMANIA

Anti-corruption law Title III on preventing and fighting cyber-crime:

Art.42: Illegal access

(1) The illegal access to a computer system is a crime and is punished with imprisonment from 6 months to 3 years.

(2) If the fact mentioned at item (1) is performed by infringing the security measures, the punishment is imprisonment from 3 to 12 years.

Art. 43: Interception of any transmission of computer data

(1) The illegal interception of any transmission of computer data that is not published to, from or within a computer system is a criminal offense and is punished with imprisonment from 2 to 7 years.

(2) The same punishment is applied also for the illegal interception, of electromagnetic emissions from a computer system carrying non-public computer data.

Art.44: Illegal alteration, deletion or deterioration of computer data

(1) The illegal alteration, deletion or deterioration of computer data of the access restriction to such data is considered a criminal offense and is punished with imprisonment from 2 to 7 years.

(2) The unauthorized data transfer from a computer system is punished with imprisonment from 3 to 12 years.

(3) The unauthorized data transfer by means of an information data storing mean is also punish as in paragraph (2).

WHEN DO YOU NEED FORENSICS

IN LEGAL CASES, COMPUTER FORENSIC TECHNIQUES ARE FREQUENTLY USED TO ANALYZE COMPUTER SYSTEMS BELONGING TO DEFENDANTS (IN CRIMINAL CASES) OR LITIGANTS (IN CIVIL CASES).

TO RECOVER DATA IN THE EVENT OF A QUESTIONABLE HARDWARE OR SOFTWARE FAILURE.

TO ANALYZE A COMPUTER SYSTEM AFTER A BREAK-IN, FOR EXAMPLE, TO DETERMINE HOW THE ATTACKER GAINED ACCESS AND WHAT THE ATTACKER DID.

TO GATHER EVIDENCE AGAINST AN EMPLOYEE THAT AN ORGANIZATION WISHES TO TERMINATE.

WHEN YOU DO NOT NEED FORENSICS

DETERMINE SYSTEM VULNERABILITY

PENETRATION TESTING PURPOSES

APPLICATION PERFORMANCE AND BEHAVIOR

WHEN NOTHING HAPPENED ALREADY IN TERMS OF EXPOSED OR LOSS OF INFORMATION, ATTACKS ON YOUR SYSTEMS AND RESOURCES, MISUSE OF IT EQUIPMENT FROM EMPLOYEES

FORENSIC INVESTIGATION GUIDELINES

PRINCIPLE 1: NO ACTION TAKEN BY LAW ENFORCEMENT AGENCIES OR THEIR AGENTS SHOULD CHANGE DATA HELD ON A COMPUTER OR STORAGE MEDIA WHICH MAY SUBSEQUENTLY BE RELIED UPON IN COURT.

PRINCIPLE 2: IN EXCEPTIONAL CIRCUMSTANCES, WHERE A PERSON FINDS IT NECESSARY TO ACCESS ORIGINAL DATA HELD ON A COMPUTER OR ON STORAGE MEDIA, THAT PERSON MUST BE COMPETENT TO DO SO AND BE ABLE TO GIVE EVIDENCE EXPLAINING THE RELEVANCE AND THE IMPLICATIONS OF THEIR ACTIONS.

PRINCIPLE 3: AN AUDIT TRAIL OR OTHER RECORD OF ALL PROCESSES APPLIED TO COMPUTER BASED ELECTRONIC EVIDENCE SHOULD BE CREATED AND PRESERVED. AN INDEPENDENT THIRD PARTY SHOULD BE ABLE TO EXAMINE THOSE PROCESSES AND ACHIEVE THE SAME RESULT.

PRINCIPLE 4: THE PERSON IN CHARGE OF THE INVESTIGATION (THE CASE OFFICER) HAS OVERALL RESPONSIBILITY FOR ENSURING THAT THE LAW AND THESE PRINCIPLES ARE ADHERED TO.

LEGAL SITUATION IN ROMANIA

Art.45: Hindering of a computer system

The serious hindering, without right, of a computer system operation, by the introducing, transmitting, altering, deleting or deteriorating computer data or by restricting the access to these data is considered a criminal offense and is punished with imprisonment from 3 to 15 years.

Art.46: Criminal offenses

(1) The following are considered criminal offenses and punished with imprisonment from one to 6 years.

a) the production, sale, import, distribution or making available, in any other form, without right, of a device or a computer programmed designed or adapted for the purpose of committing one of the offenses established in accordance with art.42-45;

b) the production, sale, import, distribution or making available, in any other form, without right, of a password, access code or other such computer data allowing total or partial access to a computer system for the purpose of one of the offenses established in accordance with art.42-45;

(2) The possession, without right, of a device, computer program, password, access code or computer data referred to at paragraph (1) for the purpose of one of the offenses established in accordance with art.42-45 is also punished similarly.

Art.47: The intent to commit the offenses referred to in art.42-43 is also punished.

Art.48.: Input, alteration or deletion of computer data

The input, alteration or deletion, without right, of computer data or the restriction, without right, of the access to these data, resulting in inauthentic data, with the intent to be used for legal purposes, is considered a criminal offense and is punished with imprisonment from 2 to 7 years.


Art.49: Loss of property

Causing the loss of property to a person by the input, alteration or deletion of computer data, by restricting the access to such data or by preventing in any way the operation of a computer system, in order to obtain an economic benefit for oneself or for another is punished with imprisonment from 3 to 12 years.


Art.50: The intent to commit the offenses referred to in art.48 and 49 is also punished.


DO YOU SUSPECT ANYTHING?


 **DO NOT TAKE ANY PROHIBITIVE ACTION**


 **GATHER INFORMATION FROM FIREWALL, IPS, LOG CORRELATION EQUIPMENTS AND TRY TO CONFIRM YOUR SUSPICION**


 **PROTECT/BACKUP ALL LOGS**

 **CALL FORENSIC CONSULTANT AND FOLLOW EXACTLY THE INSTRUCTIONS HE GIVES YOU**

 **IF IT IS ONE OF YOUR EMPLOYEES, YOU SHOULD CONFISCATE THE COMPUTER AND INFORM HIM HE IS UNDER INVESTIGATION. USE THE LEGAL FORMS AND ASK TWO WITNESSES TO SIGN THEM.**

 **DO NOT SHUT DOWN THE COMPUTER! WRITE AN ACCESS LIST TO PREVENT THE COMPUTER TO ACCESS THE INTERNET. AUTHORIZE THE FORENSIC INVESTIGATOR TO START THE INVESTIGATION PROCESS**

 **EVIDENCE NEEDS TO BE UNALTERED. PROTECT IT! STOP LOG ROTATION SCRIPTS, COLLECT ALL LOGS TO A SYSLOG SERVER!**

 **IF CASE, YOU WILL TESTIFY IN COURT ABOUT YOUR ACTIONS. FOLLOW THE LEGAL ADVISE, DO NOT LIE AND DO NOT ASSUME, FACTS ARE SUFFICIENT.**

DATAEYE CONSULTING

**NICOLAE TITULESCU 163, BL 20, AP 11, SECT1, BUCHAREST, ROMANIA
TEL/FAX: +40212220946
WWW.DATAEYE.RO**