Policie České republiky
Správa Severomoravského kraje
ODBOR KRIMINALISTICKÉ TECHNIKY A EXPERTIZ
pracoviště Frýdek Místek

Č.j.: 5679-3/KT-2004

Ve Frýdku-Místku dne: 9.12.2004
Výtisk č.: 2
Počet listů: 4
Přílohy:
Písemné: 0
Věcné: viz. Tab. 1 položka 0442_2(Jen u 1. výtisku)
1 ks CD-R tvořící přílohu č. 1

ZNALECKÝ POSUDEK
z oboru kriminalistika
odvětví kriminalistická počítačová expertiza

Odbor kriminalistické techniky a expertiz Policie ČR jako pracoviště specializované na znaleckou činnost (§ 21 odst. 1 zákona č. 36/1967 Sb., viz Seznam ústavů a jiných pracovišť specializovaných na znaleckou činnost vedený Ministerstvem spravedlnosti podle § 21 odst. 3 zákona č. 36/1967 Sb., uveřejněný v Ústředním věstníku, částka 2/1993), ve smyslu § 105 odst. 1 věta druhá tr. Řádu pro účely trestního řízení podává tento

znalecký posudek

v trestní věci:
1. [redacted] nar. [redacted]

podezřelého z trestných činů nedovolené výroby a držení OPL a jedů, nedovolené ozbrojování podle §§ 185/2a, 187/1 tr. zákona

na základě opatření: Policie ČR, okresní ředitelství, 1. odd. SKPV, Bruntál ze dne 11.8.2004 pod ČTS:ORBR-343/BR-OK-2004 které na OKTE Ostrava, pracoviště Frýdek-Místek došlo dne 16.8.2004.

1. ÚVOD

Popis skutku (události): Výše uvedených trestných činů se měl obviněný dopustit tím, že v prostorách firmy [redacted] přechovával jedy nikotin, strichnin, brucin a další, dále tím, že zde měl trhaviny hexogen, kyselinu pikrovou, fulminát stříbrný, chemické rozněcovače, rozbušku se zápalnicí, světlice a další věci.

Věci, stopy a vzorky, které byly zkoumány:

Číslo stopy	Popis	Označení pro potřeby zkoumání
	Jednotka PC mající na předním panelu štítek s nápisem POWERRED BY MATROX	0442_1
	Jednotka PC mající na čelním panelu štítek s nápisem DFI	0442_2

Tab. 1

Otázky, které mají být zodpovězeny:

1. Určete jaké informace jsou uloženy na disku počítačů, zajistěte informace.
2. Další zjištění

2. NÁLEZ

1. Základní prohlídka

0442_1

PC byl v provedení miditower a v přední části měl namontována následující zařízení: 2 x CD mechaniku a 1x FD mechaniku 3,5". První CD mechanika měla na čelním panelu nápis „52X max" a druhá" TEAC 52x writer". FD mechanika byla bez označení. Vedle štítku MATROX byl v čelním panelu čtvercový otvor. Jedna spodní zápatka přidržující čelní panel ke skříni byla nalomená. Skříni chyběly okrasné boční kryty, horní kryt měl ulomenu západku, která jej má na skříni přidržovat. Kovové bočnice skříně byly přišroubovány místo 6 jen 2 šrouby. Na zadním panelu chyběly 4ks záslepek.

V pozici AGP1 byla zasunuta videokarta, v pozici PCI síťová karta a v pozici ISA zvuková karta. V základní desce byl ještě zasunut jeden modul paměti a procesor. Vše ostatní bylo umístěno na základní desce.

Podle výpisů zobrazovaných na monitoru po zapnutí PC byl jako procesor použit INTEL CELERON 927MHz a paměť měla velikost 262144K.

V PC byl nalezen jeden pevný disk (HDD) SEAGATE model ST 380011A, s.n. 5JV3X89Q, který byl pro potřeby zkoumání označen jako 0442_1. Jeho, níže uvedená, velikost a uspořádání (partitions) byly zjištěny pomocí programu FDISK, který je součástí operačního systému LINUX RED HAT.

HDD s.n. 5JV3X89Q

Logická jednotka (Označení pro potřeby zkoumání)	Boot	Začátek	Konec	Bloky	Id	Systém
0442_1	*	1	9729	78148161	C	WIN95 FAT32 (LBA)

0442_2

PC byl v provedení miditower a v přední části má namontována následující zařízení. CD-ROM mechaniku a FD mechaniku 3,5". CD-ROM má na svém čelním panelu nápis „48Xmax". 3,5" mechanika není na čelním panelu nijak označena.

V záslepce na zadní části skříně byl otvor pro konektor, ale konektor chyběl. Skříň byla značně špinavá (uvnitř hlavně prach a pavučiny).

V pozici PCI1 byla zasunuta karta portů (sériové, paralelní). V základní desce byly ještě zasunuty dva moduly pamětí a procesor. Vše ostatní bylo umístěno na základní desce.

Podle výpisů zobrazovaných na monitoru po zapnutí PC nebo uvedených v BIOSu byl jako procesor použit CELERON 566E MHz a paměť měla velikost 195584K.

V PC byl nalezen jeden pevný disk (HDD) SEAGATE model ST310212A, s.n. 6EG04A6Z. Jeho, níže uvedená, velikost a uspořádání (partitions) byly zjištěny pomocí programu FDISK, který je součástí operačního systému LINUX RED HAT.

HDD s.n. 6EG04A6Z

Logická jednotka (Označení pro potřeby zkoumání)	Boot	Začátek	Konec	Bloky	Id	Systém
0442_2	*	1	1245	10000431	C	WIN95 FAT32 (LBA)

2. Způsob zkoumání HDD ze zajištěných PC

Aby během zkoumání HDD ze zajištěných PC nemohlo dojít k poškození nebo pozměnění dat na nich uložených, bylo prováděno vlastní zkoumání na kopiích těchto HDD. Tyto kopie byly vytvořeny následujícím způsobem.

Zkoumané HDD byly připojeny k technologickému počítači s operačním systémem LINUX. Pomocí programu IMAGER 1.3 vyvinutém v Kriminalistickém ústavu Praha (KUP) byl obsah jednotlivých zkoumaných HDD převeden do souborů.

Tyto soubory obsahují obraz původních HDD, byly uloženy na HDD technologického PC a odtud překopírovány na CD-R média, která jsou uložena v archivu oddělení počítačových expertíz OKTE Ostrava pracoviště Frýdek - Místek pod číslem 0442.

K vytvoření kopie původního HDD na HDD podobných vlastností byl použit opět program IMAGER1.3. Pomocí něj byly z výše uvedených souborů vytvořeny, dříve zmiňované, kopie obou zkoumaných HDD na kterých probíhalo vlastní zkoumání.

Během zkoumání byly používány tyto programy: WINDOWS 98, WINDOWS XP, LINUX RED HAT, 602PRO PC SUITE, Norton Utility (NU) , Microsoft Office, TOTAL COMANDER. Před započetím zkoumání byl obnoven „koš" operačního systému WINDOWS a zkomprimované soubory byly dekomprimovány.

Před uložením do přílohy č.1 musely být z technických důvodů upraveny některé názvy a zkráceny adresářové cesty. Chybějící část cest je uvedena v souborech CESTY, které jsou také uloženy v příloze č.1. Soubory CESTY se ve zkoumaných HDD nenalézaly a byly vytvořeny až během zkoumání.

3. ZÁVĚR

1. Vybrané informace nalezené ve zkoumaných PC jsou uvedeny v příloze č.1 (CD médium).

Výběr byl proveden na základě konzultace s dožadujícím policejním komisařem.

Soubory CESTY v příl. č.1 byly vytvořeny až během zkoumání a obsahují chybějící části adresářových cest.

Expertiza byla zpracována ve dnech 1.9.2004 až 9.12.2004

Zkoumané počítačové jednotky byly vráceny v nepoškozeném stavu. Informace v nich uložené nebyly pozměněny ani jinak poškozeny.

Zkoumání provedl a znalecký posudek zpracoval:

[redacted]

expert v oboru kriminalistika,
odvětví kriminalistická počítačová expertiza

Znalecký posudek byl zpracován v oboru kriminalistika, odvětví kriminalistická počítačová expertiza za použití metod a prostředků uznávaných v kriminalistické expertizní činnosti a k tomu kvalifikovaným expertem.

[redacted]

Vedoucí odboru
kriminalistické techniky a expertiz