

Pracoviště pro digitální forenzní analýzu

HW část

Požadované parametry:

- CPU nejnovější generace výrobce, min. 16 jader, výkonnost podle PassMark CPU Mark minimálně 46000
- základní deska s podporou interface (header) min. 1x port kompatibilní s Thunderbolt3, min. 3x PCIe 16x, min. 8x SATA, min. 2x m.2 slot
- grafická karta min. 640 CUDA kompatibilních jader, paměť min. 4 GB GDDR5 na frekvenci min. 2500 MHz, šířka paměťové sběrnice min. 128 bitů, PCI Express sběrnice 3.0 nebo vyšší
- operační paměť min. 128 GB RAM DDR4 3600MHz
- 2x NVMe SSD min. 1TB, čtení min. 3200 MB/s, zápis min. 2300MB/s životnost min. 500 TBW
- min. 2x SATA SSD min. 1TB, čtení i zápis min. 500 MB/s
- min. 2x SATA HDD 7200rpm, min. 8TB
- min. 3x hotswap rámečky 3.5"
- vestavěná forenzní čtečka paměťových karet s HW blokováním zápisu min. pro SD/microSD, host rozhraní min. USB 3.0
- vestavěný forenzní blokátor s HW blokováním zápisu pro paměťová média typu SATA, SAS, USB 3.0, IDE, PCIe vč. diskových adaptérů (min. microSATA, blade-type SSD, LIF, ZIF, 1.8" IDE, PCIe card, PCIe m.2, PCIe podpora Apple mid2013-2016)
- 2x monitor min. 23", rozlišení min. fullHD, DP, HDMI, nastavitelná výška, pivot
- klávesnice podsvícená a myš, obě připojení USB kabelem
- reproduktory min. 2.0, aktivní, samostatné, výkon min. 20W
- 2x externí forenzní blokátor pro SATA a IDE disky s vypínatelnou ochranou proti zápisu, host rozhraní min. USB 3.0
- napájecí zdroj s energetickou účinností minimálně dle certifikace 80 PLUS

SW část

Požadavek na SW část je dán podporou co nejširšího spektra běžně zpracovávaných digitálních stop forenzně čistým způsobem.

Požadavky na specializovaný SW pro digitální forenzní analýzu:

- licence pro akademické použití obsahující licenční klíč pro lektora a minimálně 30 licencí pro studenty, příručku pro učitele a studenty a připravené ukázkové stopy pro výuku
- podpora běžných forenzních formátů – minimálně E01, Ex01, L01, Lx01, AD1, dd, RAW, vmdk a vhd
- podpora souborových systémů minimálně NTFS, ExFAT, FAT32, EXT3, EXT4, HFS+, APFS (vč. možnosti dešifrování FileVault2)
- detekce šifrovaných oddílů min. BitLocker, TrueCrypt, PGP
- rozsah podpory vstupních dat – obrazy disků, samostatné soubory a adresáře, obrazy RAM, JTAG a chip-off image, fyzické a logické dumpy paměti mobilních zařízení, VSC

- schopnost zpracování a vyhledávání v Pagefile.sys, \$MFT, \$Logfile, Hiberfil.sys, nealokovaného diskového prostoru, file slacku, swap file
- vizualizace vazeb mezi nalezenými artefakty
- podpora fyzické a logické extrakce mobilních zařízení Android a iOS
- vytváření forenzních image z pevných disků, SSD disků a USB paměťových médií
- **Podpora identifikace a analýzy artefaktů:**
 - o sociální sítě – Facebook, Instagram, Twitter, vKontakte
 - o webový email – Gmail, Outlook
 - o IM – GoogleTalk, AIM, iMessage, Mail.ru, MSN, Skype, TorChat, WeChat, Live Messenger, Viber
 - o webové prohlížeče – Chrome, Edge, IE, Opera, Safari, Firefox
 - o cloudové služby – Dropbox, GDrive, SharePoint, OneDrive
 - o obrazové soubory vč. EXIF dat – 3gp, amr, avi, bmp, divX, gif, jpeg, jpg, mp4, mov, mkv, mpg, png, tif, tiff, wmp
 - o engine k rozpoznání obsahu obrazových souborů
 - o zálohy mobilních zařízení – Android, iOS vč. UFED formátu
 - o MS Office artefakty
 - o emaily – mbox, Outlook
 - o Windows OS artefakty – event. logy, jump listy, LNK soubory, prefetch soubory a další informace z registrů (uživatelé, časové zóny, historie spouštění, USB zařízení a další)
- **Podpora artefaktů z mobilních zařízení:**
 - o SMS a MMS pro Android i iOS
 - o kontakty a historie volání
 - o Android Mail, Gmail, iOS Mail
 - o prohlížeče Chrome, Dolphin, Firefox, Puffin, Safari a Silk
 - o Apple Maps, Google Maps
 - o poznámky z iOS Notes a Outlook Notes
 - o chatovací aplikace – Hangouts, Grindr, WhatsApp, Kik, Snapchat, Skype, telegram, Tinder, Viber, WeChat a Zoom
 - o social media aplikace – Facebook, Instagram, Twitter, vKontakte

Platforma pro obnovu dat z flash pamětí

Hardwarově-sofwarová platforma pro obnovu dat ze zařízení s NAND pamětí v případech nedostupnosti či nefunkčnosti originálního interface. Zejména se jedná o zařízení, jako jsou:

- UFD (USB Flash disk)
- SD karty
- CF karty
- MS karty
- xD karty

Hardwarově-sofwarová platforma umožňuje pomocí specializovaného zařízení přístup k obsahu paměťového čipu vypájenému z původní desky za použití specializovaného zařízení. Platforma obsahuje vlastní databázi pravidelně aktualizovanou na základě volně dostupných zdrojů k automatizované identifikaci a čtení běžně používaných mikročipů.

Požadavky na platformu minimálně:

- SW pro čtení dat z mikročipů vč. funkce automatické identifikace a čtení
- reader pro rozhraní mezi adaptéry a USB portem počítače
- TSOP-48 adaptér
- TSOP-48 W (wide adaptér)
- LGA/TLGA-52/60 (14x18) adaptér
- LGA/TLGA-52/60 (12x17) adaptér
- BGA-152 adaptér
- BGA-152/132 adaptér
- TSSOP-56 adaptér
- VBGA-100 adaptér
- LGA-52/TSOP-48 modul
- BGA-152/VBGA-100 modul
- adaptér na paměťové karty
- univerzální adaptér pro připojení mikročipů bez specifického adaptéru (tzv. spider board)
- včetně technické podpory výrobce minimálně 1 rok

Ostatní podmínky

- vše bude dodáno jako funkční celek, jednotlivé součásti dle specifikace musí být spolu propojitelné a vzájemně kompatibilní
- zadavatel vyžaduje volný přístup do dodaných počítačů bez ztráty záruky
- záruka na veškerý hardware „Pracoviště pro digitální forenzní analýzu“ min. 36 měsíců
- pokud je nabízené zboží složeno z dílů, u kterých primární výrobce garantuje delší záruční dobu, zadavatel vyžaduje zachování této záruční doby (možnost reklamace jednotlivých dílů i po konci globální záruční doby)
- místo převzetí záruční opravy je v místě dodání
- nabídková cena je konečná a zahrnuje i cenu dopravy případně další přidružené platby (např. recyklační poplatky apod.)
- součástí dodávky musí být veškeré vybavení a příslušenství k okamžitému uvedení do provozu