AUTORITATEA NAȚIONALĂ DE REGLEMENTARE ÎN DOMENIUL ENERGIEI

DIRECȚIA INVESTIGAȚII

NR. 44598/22.04.2021

Specificații tehnice

- Aplicaţia trebuie să fie destinată realizării investigaţiilor informatice (Digital Forensics) şi să cuprindă componentele software necesare achiziţiei, procesării, stocării şi analizei evidenţelor informatice de pe dispozitive portabile.
- Aplicaţia trebuie să fie capabilă pentru identificarea, conservarea, recuperarea, analiza şi prezentarea dovezilor privind activităţile şi acţiunile realizate de o persoană (utilizator) atât de pe o staţie de lucru (PC) cât şi de pe una portabilă (laptop, notebook, etc.).
- Aplicaţia trebuie să ofere facilităţi pentru gestionarea mai multor cazuri de investigaţii simultan.
- Resursele, datele, informaţiile şi rezultatele cazurilor să fie separate între cazurile existente.
- Aplicaţia trebuie să ofere mecanisme pentru obţinerea unei replici exacte, din punct de vedere binar, a mediilor de stocare utilizate pe sisteme portabile, pe un alt mediu de stocare extern, fără alterarea datelor originale certificată prin realizarea automată a unei sume de control.
- Aplicaţia trebuie să ofere mecanisme care să permită automat analiza fişierelor după reputaţia acestora în vederea identificării celor cu un comportament maliţios sau care pot compromite integritatea datelor.
- Aplicaţia trebuie să ofere mecanisme pentru recuperarea fişierelor şterse sau ascunse, fişierelor corupte şi fişierelor protejate cu parolă.
- Aplicaţia trebuie să ofere mecanisme pentru decriptarea fişierelor cripate cu sisteme comerciale (facilităţi de atac prin metode de tip brute-force, bazate pe dicţionare şi facilităţi de utilizare a tabelelor Rainbow).
- Aplicaţia trebuie sp ofere mecanisme pentru identificarea fişierelor după căutare de conţinut, activităţi sau acţiuni.
- Aplicaţia trebuie să ofere facilităţi pentru analiza fişierelor după anumiţi parametrii a dovezilor relevante unui caz într-o zonă/arie separată fără să aducă modificări ale datelor, informaţiilor şi fişierelor originale/iniţiale.
- Aplicaţia trebuie să fie o soluţie integrată, cuprinzând elementele software necesare desfăşurării activităţii de analiză şi investigare informatica (digital forensics) a sistemelor de calcul pornite sau oprite.
- Aplicaţia trebuie să fie capabilă să refacă automat structura volumelor NTFS şi FAT care au fost formatate.

- Aplicaţia trebuie să ofere mecanisme pentru gruparea datelor şi informaţiilor în funcţie de timp sau tipul acestora.
- Aplicaţia trebuie să ofere facilităţi pentru adaugarea de note sau etichete descriptive pentru fiecare dovadă (obiect, artefact) relevantă descoperită, extrasă şi stocată separat.
- Aplicaţia trebuie să ofere mecanisme pentru generarea de rapoarte în format pdf, rtf.
- Aplicaţia trebuie să permită utilizarea filtrelor – filtre predefinite sau personalizare, pentru sortarea şi căutarea datelor. De asemenea Aplicaţia trebuie să permită şi sortarea şi căutarea datelor utilizând scripturi realizate sau personalizate de utilizator.
- Aplicaţia trebuie să permită vizualizarea fişierele de tip imagine prin intermediul unor view-uri de tip galerie.
- Aplicaţia trebuie să fie capabilă să extragă informaţii despre fişierele conţinute în interiorul fişierelor uzuale de tip imagine (ISO), în interiorul fişierelor de tip arhivă (RAR, ZIP, etc), precum şi din fişiere utilizate în mediile virtuale uzuale (vmdk, vhd, 001, etc.).
- Aplicaţia trebuie sp permitp investigarea e-mailurilor din fişiere de tip PST, DBX (Microsoft Outlook, Standard şi Express), EDB (Microsoft Exchange), EMLX (Macintosh OS X).
- Aplicaţia trebuie să fie tip software cu drept de utilizare nelimitată, iar suportul pentru update-uri şi upgrade-uri să fie oferit pe o perioada de 5 ani, pentru toate componentele incluse.