WINDOWS KOMPYUTERLARI ISHGA TUSHIRISH JARAYONI: BIOS, UEFI VA KRIMINALISTIK TEKSHIRUVLARDAGI AHAMIYATI

Zoirov Diyorbek Dilshod o‘g‘li
Saidov Yaxshimurodbek Umidjonovich
Jalilov Muhammad Hasan og‘li
Oripov Faxriddin A’zamjon o‘g‘li
Muxammad al – Xorazmiy nomidagi TATU talabalari

Annotatsiya: *Ushbu maqolada zamonaviy Windows kompyuterlarining ishga tushish jarayoni, xususan BIOS va UEFI texnologiyalari, ularning funktsional farqlari, kriptografik xavfsizlik mexanizmlari va raqamli kriminalistika tekshiruvlaridagi o‘rni yoritiladi. CMOS sozlamalari, yuklash ketma-ketligi, bootable qurilmalar bilan ishlash va ma’lumotlar yaxlitligini saqlab qolish texnikasi haqida tahliliy ma’lumotlar taqdim etiladi. Shuningdek, tergov jarayonlarida BIOS/UEFI orqali aniqlanadigan izlar va ulardan qanday foydalanish mumkinligi ham ko‘rib chiqiladi.*

Kalit so‘zlar: *BIOS, UEFI, CMOS, boot ketma-ketligi, kriminalistika, Windows, ishga tushirish jarayoni, raqamli tergov, bootable media, firmware*

Windows operatsion tizimlari asosida ishlovchi kompyuterlarning ishga tushish jarayoni — bu nafaqat texnik muhim bosqich, balki raqamli kriminalistika uchun ham alohida ahamiyat kasb etuvchi muhitdir. Har qanday kompyuter qurilmasi elektr quvvati berilgach, ishga tushishning dastlabki bosqichida BIOS yoki UEFI orqali o‘zining apparat va dasturiy muhitini ishga tayyorlaydi. Shu bosqichda amalga oshiriladigan har bir operatsiya, sozlama va tekshiruv raqamli tergovchi uchun potentsial dalil yoki iz manbai bo‘lishi mumkin.

An’anaviy BIOS (Basic Input/Output System) tizimi dekabrli va cheklangan interfeysga ega bo‘lsa, zamonaviy UEFI (Unified Extensible Firmware Interface) — kengaytirilgan grafik interfeys, xavfsizlik funktsiyalari va tezkor ishga tushirish imkoniyatlarini taklif qiladi. Har ikkala tizim ham kompyuterning ichki konfiguratsiyasini, yuklanadigan qurilmalarni va boot sektorlarni belgilaydi, bu esa raqamli dalillarni to‘plashda o‘ziga xos rol o‘ynaydi.

Bundan tashqari, CMOS (Complementary Metal-Oxide-Semiconductor) xotirasi BIOS/UEFI konfiguratsiyalarini saqlab turadi. CMOS'dagi ma’lumotlar — masalan, ishga tushirish ketma-ketligi, vaqt, sana va disklar ro‘yxati — tergovchi uchun tizimdagi o‘zgarishlar, xakerlik izlari yoki noan’anaviy yuklash usullari haqida ma’lumot beradi.

Kompyuterlarning ishga tushishida birinchi bo‘lib ishga tushadigan dasturiy ta’minot BIOS yoki UEFI hisoblanadi. Ular kompyuterning apparat qurilmalari va operatsion tizimi o‘rtasida bog‘lovchi bo‘lib xizmat qiladi. Ushbu komponentlar faqat

tizimni ishga tayyorlash bilangina cheklanmay, balki raqamli kriminalistik tahlil uchun ham foydali izlarni o‘zida saqlab qoladi.

BIOS (Basic Input/Output System) – IBM tomonidan 1980-yillarda ishlab chiqilgan dastlabki yuklovchi dastur bo‘lib, hozirgacha ko‘plab tizimlarda saqlanib qolgan. BIOS kompyuterning ichki xotirasida, odatda ROM (Read-Only Memory) chipida joylashgan bo‘ladi. U quyidagi funksiyalarni bajaradi:

- Qurilmalarning boshlang‘ich sinovini (POST – Power-On Self Test) o‘tkazadi;
- Tizim vaqtini va sanasini belgilaydi;
- Yuklash ketma-ketligini (boot order) boshqaradi;
- CMOS konfiguratsiyasini yuklaydi va saqlaydi.

Kriminalistik tahlilda BIOS’ning CMOS xotirasida saqlanayotgan sozlamalar — masalan, disklar ro‘yxati, yuklash ketma-ketligi, soat va sana — tergovchilar uchun muhim axborot manbaidir. Xususan, bootable qurilmalar ketma-ketligida kutilmagan o‘zgarishlar aniqlansa, bu hujumchi tashqi qurilmadan foydalanib tizimga kirgan bo‘lishi mumkinligini anglatadi.

UEFI (Unified Extensible Firmware Interface) — BIOS’ning zamonaviy o‘rnini egallagan kengaytirilgan interfeys bo‘lib, u ko‘proq qulaylik, xavfsizlik va kengaytirilgan imkoniyatlarni taqdim etadi. UEFI quyidagi afzalliklarga ega:

- 2 TB dan katta disklarni qo‘llab-quvvatlaydi (GPT – GUID Partition Table yordamida);
- Yaxshilangan grafik interfeys va sichqoncha bilan boshqarish imkoniyati mavjud;
- "Secure Boot" funksiyasi orqali operatsion tizim faqat ishonchli raqamli imzo bilan yuklanishini ta’minlaydi;
- UEFI scripting (skript orqali sozlash) va tarmoqdan boot qilish imkonini beradi.

UEFI CMOS o‘rniga NVRAM (non-volatile RAM) dan foydalanadi, bu esa tizim o‘chirib qo‘yilganidan so‘ng ham sozlamalarning saqlanishini ta’minlaydi. Raqamli kriminalistika uchun bu — ya’ni secure boot konfiguratsiyasi, yuklash siyosati, imzolanmagan bootloader izlari va boshqa meta-sozlamalar — tahlil jarayonida beqiyos ahamiyatga ega.

BIOS/UEFI konfiguratsiyasini tekshirish kriminalistik tekshiruv jarayonida quyidagi sabablar bilan dolzarbdir:

- Disk yuklanish ketma-ketligi — gumonlanuvchi bootable USB orqali tizimga kirgan bo‘lishi mumkin;
- Secure Boot o‘chirilganmi? — bu holatda ishonchli bo‘lmagan operatsion tizim yoki qulaylik dasturlari yuklangan bo‘lishi mumkin;
- Vaqt-sana sozlamalari — hujum vaqtini manipulyatsiya qilishga urinishlar aniqlanishi mumkin;
- BIOS paroli mavjudligi — tizimga ruxsatsiz kirishlar oldini olish mexanizmi faollashtirilganmi?

Tergovchi BIOS/UEFI interfeysiga kirib, bu parametrlarni diqqat bilan ko‘zdan kechirishi, fotosurat yoki nusxa olishi va ularni tahlil hujjatlariga kiritishi kerak. Ayniqsa, gumonlanuvchining diskga qanday operatsion tizimni va qanday yo‘l bilan o‘rnatgani, qaysi qurilmalardan foydalangani yoki tizimga buzib kirishga urinishi BIOS/UEFI darajasidagi sozlamalarda aks etgan bo‘lishi mumkin.

Kriminalistik tahlil jarayonida kompyuter tizimini ishga tushirish bosqichi nihoyatda muhim hisoblanadi. Bu bosqichda bajarilgan noto‘g‘ri harakatlar dalil sifatida xizmat qilishi mumkin bo‘lgan ma’lumotlarni buzishi, ustiga yangi ma’lumot yozilishi yoki vaqt muhrlari o‘zgartirilishi xavfini tug‘diradi. Shuning uchun tergovchi kompyuter ustida ishlashdan avval ma’lumotlar yaxlitligini saqlashga qaratilgan ehtiyot choralarini ko‘rishi kerak.

Kompyuter odatdagi holatda yoqilganda avtomatik tarzda qattiq diskdagi operatsion tizimni yuklaydi. Bu yuklanish davomida tizim o‘zining log fayllarini yangilashi, fayl tizimida o‘zgartirishlar kiritishi yoki muhim vaqt yozuvlarini avtomatik ravishda yangilab yuborishi mumkin. Shunday holatlarning oldini olish uchun, kompyuterga operatsion tizimni tashqi qurilmadan — ya’ni maxsus forensik muhitga ega bootable USB yoki Live CD orqali yuklash tavsiya etiladi. Bu muhitlar maxsus ravishda ishlab chiqilgan bo‘lib, ular yordamida diskka hech qanday ma’lumot yozilmaydi, faqat o‘qish rejimida ishlanadi.

Kompyuterni forensik muhitda yuklashdan avval uning BIOS yoki UEFI menyusiga kiriladi. Tizim sozlamalari o‘zgartirilmasdan, mavjud boot ketma-ketligi, soat va sana, disklar ro‘yxati va xavfsizlik parametrlarining hozirgi holati hujjatlashtiriladi. Bu ma’lumotlar fotosuratga olinishi yoki matnli hujjat shaklida qayd etilishi mumkin. Agar BIOS yoki UEFI parol bilan himoyalangan bo‘lsa, parolni buzishga harakat qilishdan avval sud ruxsatnomasi mavjud bo‘lishi zarur.

Tizim yuklangach, forensik vositalardan foydalaniladi. Bu vositalar orasida FTK Imager Live, CAINE, Guymager, Paladin Forensic Suite kabi muhitlar mavjud bo‘lib, ular yordamida qattiq diskning butun nusxasini olish, MBR/GPT yozuvlarini ko‘rish, boot sektor holatini tekshirish va disk konfiguratsiyasini tahlil qilish mumkin. Eng muhimi, bu jarayonda diskka hech qanday yozuvlar kiritilmaydi, ya’ni dalil yaxlitligi saqlanadi.

Kompyuter yuklanganda eng birinchi bo‘lib boot sektori faollashadi. BIOS asosidagi tizimlarda bu MBR, UEFI asosida esa EFI yuklovchi fayllar hisoblanadi. Ushbu sektorlar hujumchilar tomonidan o‘zgartirilgan bo‘lishi mumkin. Masalan, bootkit yoki zararli yuklovchi joylashtirilgan bo‘lsa, bu tizimga buzib kirish uchun foydalanilgan bo‘lishi mumkin. Bunday holatlarda sektorlarni tahlil qilish, imzo (hash) orqali taqqoslash va o‘zgartirishlar aniqlash tergovchi uchun dolzarb ahamiyatga ega.

Ma’lumotlarning o‘zgartirilmaganligini tasdiqlash uchun, tergovchi hash algoritmlar — masalan, MD5 yoki SHA-256 — orqali nusxa olingan fayl yoki disk bo‘limining identifikatsiya qiymatini hisoblaydi. Bu qiymat tergov hujjatlarida

ko‘rsatiladi va sudda dalilning haqiqiyligi, ishonchliligi va o‘zgartirilmaganligini tasdiqlashga xizmat qiladi.

Kompyuter ishga tushish jarayonining har bir bosqichi ehtiyotkorlik bilan bajarilishi lozim. Tizim sozlamalari bilan bevosita ishlash, boot sektorni tahlil qilish va disk nusxasini olishda tergovchi barcha harakatlarni hujjatlashtirishi, dalillarning butunligini saqlab qolishi hamda ularning huquqiy kuchini ta’minlashi zarur. Shu tarzda ishga tushirish jarayoni dalil sifatida foydalanishga tayyor va ishonchli shaklda qayd etiladi.

XULOSA

Windows kompyuterlarining ishga tushish jarayonida BIOS va UEFI tizimlarining tutgan o‘rni nafaqat texnik jihatdan, balki raqamli kriminalistika nuqtai nazaridan ham muhim ahamiyat kasb etadi. Ular kompyuterning asosiy apparat va dasturiy qismlarini boshqarish bilan birga, yuklash ketma-ketligi, vaqt-sana sozlamalari, yuklovchi qurilmalar va xavfsizlik parametrlaridagi o‘zgarishlarni qayd etuvchi tizim sifatida tergovchilar uchun muhim ma’lumot manbai hisoblanadi.

Tizimning ishga tushishida, ayniqsa CMOS yoki NVRAM xotiralarida saqlanadigan sozlamalar orqali tergovchi diskga yuklangan operatsion tizim haqida, bootable qurilmalardan foydalanganlik ehtimoli, secure boot funksiyasining yoqilgan yoki o‘chirilganligi kabi faktlarni aniqlashi mumkin. Bu ma’lumotlar jinoyatga oid harakatlarning vaqtini, usulini va texnik izlarini ko‘rsatishda muhim rol o‘ynaydi.

Kriminalistik tekshiruvlarda tizimga bootable muhit orqali kirish, diskka yozuv kiritilmasdan ma’lumotlarni ko‘rish, hash qiymatlar yordamida dalillar yaxlitligini tasdiqlash va BIOS/UEFI sozlamalarini hujjatlashtirish — bu sohada amal qilinadigan asosiy tamoyillardir. Ayniqsa, boot sektorlar, yuklovchi yozuvlar (MBR yoki EFI) va imzo tahlillari orqali jinoyat izlarini aniqlash mumkin bo‘ladi.

Shu bois, raqamli tergovchi BIOS va UEFI tizimlarini nafaqat texnik konfiguratsiya jihatidan, balki kriminalistik tahlil obyekti sifatida ham chuqur o‘rganishi zarur. Bu bilimlar zamonaviy tergov jarayonida dalillarni saqlab qolish, ularga yuridik kuch berish va jinoyat mexanizmini fosh etishda hal qiluvchi ahamiyatga ega bo‘ladi.

ADABIYOTLAR:

1. Casey, Eoghan. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd Edition. Academic Press, 2011.
2. Mandia, Kevin, Prosise, Chris, & Pepe, Matt. Incident Response & Computer Forensics. 3rd Edition. McGraw-Hill, 2014.
3. Stallings, William. Operating Systems: Internals and Design Principles. 9th Edition. Pearson, 2017.
4. NIST Special Publication 800-101 Rev.1. Guidelines on Mobile Device Forensics. National Institute of Standards and Technology, 2014.
5. Guidance Software. EnCase Forensic User Manual. Version 8.09.

6. AccessData. FTK Imager User Guide. AccessData Group LLC.
7. Tanenbaum, Andrew S. & Bos, Herbert. Modern Operating Systems. 4th Edition. Pearson, 2015.
8. Ligh, Michael Hale et al. The Art of Memory Forensics. Wiley, 2014.