

ELEKTRON POCHTA SERVERLARI VA RAQAMLI KRIMINALISTIKA. UNIX, EXCHANGE, LOGLAR VA MUHIM FAYLLAR TAHLILI

<https://doi.org/10.5281/zenodo.15308790>

Akbarov Alimurod Aziz o'g'li

Muxammad al – Xorazmiy nomidagi TATU talabasi, tel:+998943672277

Annotatsiya: *Ushbu maqolada elektron pochta serverlarining ishlash prinsiplari, xususan, ularning log fayllarni yuritish mexanizmlari ko'rib chiqiladi. Raqamli kriminalistika nuqtai nazaridan loglarning ahamiyati, ularni olish va tahlil qilish usullari, jumladan UNIX (Sendmail, Postfix) va Microsoft Exchange serverlari uchun xos bo'lgan jihatlar yoritilgan. Aylanuvchi loglar kabi ma'lumotlar yo'qolishi mumkin bo'lgan holatlar va ularning oldini olish choralari muhokama qilinadi. Shuningdek, elektron pochta tergovida qo'llaniladigan maxsus forensika dasturlari (Magnet AXIOM, Autopsy, MXToolBox va boshqalar) va ularning imkoniyatlari, dalillarni hujjatlashtirish, sud lingvistikasi hamda ijtimoiy tarmoqlardan dalil yig'ish masalalari haqida ma'lumot beriladi.*

Kalit so'zlar: *Elektron pochta serveri, log fayllar, .edb fayl, Tracking.log, UNIX, Postfix, Sendmail, Microsoft Exchange Server, Magnet AXIOM, Autopsy, MXToolBox.*

Elektron pochta serveri — maxsus dasturiy ta'minot bilan jihozlangan kompyuter tizimi bo'lib, u elektron pochta protokollari orqali xabarlarni qabul qilish, jo'natish va saqlash kabi xizmatlarni ko'rsatadi. Bu serverlar odatda client/server arxitekturasida ishlaydi, ya'ni foydalanuvchilarning pochta dasturlari (mijozlar) markaziy serverga ulanib, xabarlar almashinadi. Serverlar foydalanuvchilarning xatlarini va boshqa ma'lumotlarni maxsus ma'lumotlar bazalarida yoki oddiy fayl tizimidagi kataloglarda saqlaydi. Masalan, UNIX tizimlarida keng tarqalgan Postfix yoki Sendmail kabi serverlar pochta xabarlarini /var/spool/postfix kabi kataloglarda saqlashi mumkin, Microsoft Exchange Server esa Microsoft Extensible Storage Engine (ESE) texnologiyasiga asoslangan .edb kengaytmali ma'lumotlar bazasi fayllaridan foydalanadi. Raqamli kriminalistika nuqtai nazaridan, tergovchi barcha serverlarning ishlashini chuqur bilishi shart emas, lekin tergov uchun zarur ma'lumotlarni (masalan, xabarlar, foydalanuvchi ma'lumotlari) serverdan qanday olish mumkinligini tushunishi muhim. Bu jarayonda ko'pincha tarmoq yoki pochta administratori yordam beradi.

Server faoliyatining ajralmas qismi bu log fayllar hisoblanadi. Elektron pochta serverlari o'z faoliyati davomida sodir bo'lgan hodisalar, xususan, xabar almashinuvi jarayonlari haqida yozuvlarni saqlaydigan maxsus fayllar – log fayllarni yuritadi. Bu loglar tergov jarayonida juda qimmatli dalil manbai bo'lishi mumkin. Ba'zi serverlar log yozishni avtomatik tarzda amalga oshirsa, boshqalarida bu funksiyani administrator tomonidan qo'lda sozlash talab etiladi. Administratorlar loglarni bir necha sabablarga ko'ra yuritadilar:

tizimda nosozlik yuz berganda yoki favqulodda holatlarda elektron pochталarni tiklash, xavfsizlik tizimlari (firewall, filtrlar) to'g'ri ishlayotganini tekshirish, hamda kompaniyaning ichki siyosatlariga rioya qilinishini nazorat qilish. Ammo shuni yodda tutish kerakki, ba'zi administratorlar loglarni umuman o'chirib qo'yishi yoki "aylanuvchi loglar" (circular logging) tizimini ishlatishi mumkin. Aylanuvchi loglashda fayl hajmi yoki vaqt oralig'i chegarasiga yetganda, eng eski yozuvlarning ustiga yangi ma'lumotlar yozib yuboriladi, bu esa eski dalillarning yo'qolishiga olib keladi. Shuning uchun tergovda loglar yo'qolib ketmasligi uchun ularni zaxiralash yoki tezkorlik bilan administratorga murojaat qilib nusxasini olish muhim, chunki ba'zi provayderlar loglarni faqat qisqa muddat (masalan, 30 kun) saqlaydi. Log fayllarida odatda quyidagi ma'lumotlar bo'ladi: qabul qilingan yoki jo'natilgan xabarlar haqida yozuvlar, xabarning kelib chiqqan (jo'natuvchi) IP manzili, xabarning server tomonidan qabul qilingan yoki mijoz tomonidan ochilgan aniq vaqti va sanasi, ba'zan esa xabar hajmi va tizimga oid boshqa ma'lumotlar. UNIX tizimlarida loglar ko'pincha /var/log/maillog faylida yoki /etc/syslog.conf da ko'rsatilgan boshqa joyda saqlanadi va SMTP (jo'natish), POP3/IMAP4 (qabul qilish/o'qish) protokollari bilan bog'liq voqealarni qayd etadi. Microsoft Exchange serverida esa tranzaksiya loglari (ma'lumotlar bazasi o'zgarishlarini kuzatadi), Tracking.log (xabarlarni kuzatish uchun, batafsil rejimda IP manzil, vaqt va hatto xabar matnini ham saqlashi mumkin) va Windows Event Viewer orqali ko'rish mumkin bo'lgan diagnostika loglari mavjud. Loglardagi vaqt belgilari va IP manzillarni xabarning sarlavhasi (header)dagi ma'lumotlar bilan solishtirish orqali xabarning yo'lini va haqiqiylikini tekshirish mumkin.

.edb fayli Microsoft Exchange Server tizimining asosiy ma'lumotlar bazasi fayli hisoblanadi va u elektron pochta xabarlari hamda boshqa tegishli ma'lumotlarni saqlash uchun markaziy ombor vazifasini bajaradi. Bu fayllar Microsoft Extensible Storage Engine (ESE) deb nomlanuvchi maxsus ma'lumotlar bazasi texnologiyasi asosida yaratilgan bo'lib, ular asosan Messaging Application Programming Interface (MAPI) formatidagi xabarlarni boshqaradi va saqlaydi. Raqamli kriminalistika yoki tizim diagnostikasi nuqtai nazaridan, .edb fayli tekshiruv jarayonida eng foydali bo'lgan fayllardan biridir; u bilan birga checkpoint fayllari (tranzaksiya loglaridagi oxirgi yozilgan joyni belgilaydi) va .tmp (vaqtinchalik) fayllar ham muhim ahamiyatga ega. Exchange serveridagi elektron pochta ma'lumotlarini, jumladan o'chirilgan xabarlarni tahlil qilish yoki tiklash zarur bo'lganda, Magnet AXIOM, OSForensics, Paraben E-Mail Examiner, AccessData FTK kabi maxsus forensika va ma'lumotlarni tiklash vositalari ko'pincha aynan .edb fayllari bilan ishlashga mo'ljallangan bo'ladi. Ushbu vositalar .edb fayllarining murakkab strukturasi tahlil qilib, undan individual xabarlarni, ularga birlashtirilgan fayllarni va boshqa metama'lumotlarni ajratib olish imkonini beradi.

Tracking.log fayli Microsoft Exchange Server tarkibidagi maxsus log fayllaridan biri bo'lib, uning asosiy maqsadi server orqali o'tadigan elektron pochta xabarlarining harakatini kuzatib borishdir (message tracking). Bu log Exchange serverining tranzaksiya loglaridan (ma'lumotlar bazasi o'zgarishlarini qayd etadi) va Windows Event Viewer orqali

ko'riladigan diagnostika loglaridan (tizim hodisalari va xatoliklarni qayd etadi) alohida yuritiladi. Tracking.log faylining foydali bo'lishi uchun Exchange server administrator tomonidan "Message Tracking" funksiyasini yoqib qo'ygan bo'lishi kerak. Agar bu funksiya yoqilgan bo'lsa va qo'shimcha ravishda "verbose" (batafsil) log yozish opsiyasi ham faollashtirilgan bo'lsa, Tracking.log fayli tergov uchun juda qimmatli ma'lumotlarni saqlashi mumkin. Bunday ma'lumotlarga xususan quyidagilar kiradi: xabarning serverga kelib tushgan yoki undan jo'natilgan aniq sana va vaqti (vaqt belgisi), xabarni jo'natgan yoki qabul qilgan foydalanuvchi yoki tizim, va eng muhimi, xabarni jo'natgan mijoz kompyuterining IP manzili. Batafsil rejimda hatto xabarning mavzusi (subject) yoki qisman matni ham logga yozilishi mumkin. Bu ma'lumotlar shubhali xabarlarining kelib chiqishini aniqlash, ularning server ichida qanday yo'naltirilganini kuzatish va kiberhujumlar yoki ichki siyosat buzilishlarini tekshirishda muhim dalil bo'lib xizmat qiladi.

UNIX tizimlarida turli xil elektron pochta serverlari ishlatiladi va ular raqamli kriminalistika uchun muhim ma'lumot manbai bo'lishi mumkin. Bu tizimlarda elektron pochta bilan bog'liq loglar odatda /var/log/maillog fayliga yoziladi. Ushbu log fayli SMTP protokoli orqali serverlar o'rtasidagi xat almashinuvini, shuningdek, foydalanuvchilarning o'z pochta qutilariga POP3 yoki IMAP4 protokollari yordamida qachon va qaysi IP manzildan kirganligini qayd etadi. Bu ma'lumotlar, ayniqsa, shubhali elektron pochta xabarining sarlavhasida (header) ko'rsatilgan IP manzil va vaqt belgilari bilan logdagi yozuvlarni solishtirish orqali xabarning kelib chiqishini tekshirishda juda foydalidir. Agar loglar standart joyda, ya'ni /var/log katalogida topilmasa, ularni butun fayl tizimi bo'ylab qidirish uchun find yoki locate .log kabi buyruqlardan foydalanish mumkin. Ba'zida elektron pochta xabarlari markaziy serverda emas, balki foydalanuvchining shaxsiy kompyuteridagi /home/username/mail kabi kataloglarda saqlanishi ham mumkin. Tergov jarayonini soddalashtirish maqsadida, UNIX tizimlarida tergovchiga kerakli fayl va loglarga kirish huquqini berish uchun maxsus foydalanuvchi guruhi yaratilishi va tergovchi shu guruhga a'zo qilinishi mumkin.

Postfix UNIX va unga o'xshash operatsion tizimlarda keng tarqalgan, ishonchli va samarali elektron pochta serveri dasturidir. U ko'pincha Sendmailga zamonaviyroq muqobil sifatida qoraladi. Postfixning asosiy sozlamalari odatda ikkita konfiguratsiya fayli orqali boshqariladi: /etc/postfix/main.cf va /etc/postfix/master.cf. main.cf fayli serverning umumiy parametrlarini, masalan, qaysi domenlarga xizmat ko'rsatishi, tarmoq sozlamalari, xavfsizlik cheklovlari kabilarni belgilaydi. master.cf fayli esa Postfixning ichki jarayonlari (daemonlar) qanday ishga tushirilishi va o'zaro aloqada bo'lishini aniqlaydi. Ushbu konfiguratsiya fayllarini tahlil qilish orqali loglar qayerga yozilishi, xatlar qanday qayta ishlanishi va yo'naltirilishi kabi tergov uchun muhim texnik detallarni bilib olish mumkin. Postfix tomonidan qabul qilingan yoki jo'natish uchun navbatda turgan elektron pochta xabarlari odatda /var/spool/postfix katalogi ichidagi turli quyi kataloglarda fayl ko'rinishida saqlanadi. Postfixning loglari esa, ko'pgina UNIX tizimlaridagi kabi, tizimning markaziy

loglash xizmati (syslog) orqali boshqariladi va odatda /var/log/maillog fayliga yoki syslog konfiguratsiyasida ko'rsatilgan boshqa manzilga yoziladi.

Sendmail UNIX tizimlari uchun eng qadimgi va tarixan keng qo'llanilgan elektron pochta serverlaridan biridir. Ba'zi operatsion tizimlarda, masalan, FreeBSD yoki CentOS'ning eski versiyalarida u sukut bo'yicha o'rnatilgan bo'lishi mumkin. Sendmailning asosiy va juda murakkab konfiguratsiya fayli /etc/mail/sendmail.cf hisoblanadi. Ushbu fayl serverning deyarli barcha ish parametrlarini belgilaydi va uni tahlil qilish orqali log fayllarning joylashuvi va formatini aniqlash mumkin. Bundan tashqari, Sendmail (va boshqa ko'plab UNIX dasturlari) loglarni qayerga yozishni aniqlash uchun tizimning umumiy loglash konfiguratsiya fayli bo'lgan /etc/syslog.conf ga tayanadi. Ushbu faylda qaysi turdagi (facility, masalan, mail) va qanchalik muhimlikdagi (priority level) xabarlar qaysi log faylga (action, masalan, /var/log/maillog) yoki boshqa manzilga (masalan, boshqa serverga) jo'natilishi ko'rsatiladi. Demak, Sendmail loglarining aniq joylashuvini topish uchun ham sendmail.cf, ham syslog.conf fayllarini tekshirish kerak bo'lishi mumkin. Sendmail tomonidan yozilgan loglar ham odatda /var/log/maillog faylida bo'ladi va SMTP protokoli orqali pochta almashinuvi haqida batafsil ma'lumotlarni saqlaydi.

Microsoft Exchange Server asosan korporativ mijozlarga mo'ljallangan, Microsoft tomonidan ishlab chiqilgan kuchli elektron pochta va hamkorlik platformasidir. U shunchaki pochta serveri emas, balki kalendarlar, kontaktlar va vazifalarni boshqarish imkoniyatini ham beradi. Exchange Microsoft Extensible Storage Engine (ESE) deb ataladigan maxsus ma'lumotlar bazasi texnologiyasidan foydalanadi. Elektron pochta xabarlari va boshqa ma'lumotlar .edb kengaytmali ma'lumotlar bazasi fayllarida saqlanadi. Tizimning barqaror ishlashi va ma'lumotlar yo'qolishining oldini olish uchun Exchange barcha o'zgarishlarni (tranzaksiyalarni) maxsus tranzaksiya log fayllariga ketma-ket yozib boradi. Ma'lumotlar bazasiga muvaffaqiyatli yozilgan so'nggi tranzaksiyani qayd etib turuvchi checkpoint fayllari esa tizimda nosozlik yuz berganda ma'lumotlarni tezda tiklashga yordam beradi. Ba'zi vaqtinchalik operatsiyalar uchun .tmp fayllari ham ishlatilishi mumkin. Exchange server ham o'z faoliyati haqida loglar yuritadi. Tranzaksiya loglarining holatini tekshirish uchun Windows PowerShell'da GetTransactionLogStats.ps1 -Gather buyrug'ini ishlatish mumkin. Eng muhim loglardan biri bu Tracking.log faylidir. Agar administrator tomonidan xabarlarni kuzatish (Message Tracking) funksiyasi yoqilgan bo'lsa, bu log fayli orqali xabarlarning server ichidagi harakatini kuzatish mumkin. Agar "batafsil" (verbose) log yozish rejimi yoqilgan bo'lsa, Tracking.log da xabar jo'natilgan vaqt, jo'natuvchining IP manzili va hatto xabarning mavzusi yoki qisman matni kabi tergov uchun juda qimmatli ma'lumotlar ham saqlanishi mumkin. Bundan tashqari, Exchange tizimida yuzaga keladigan turli hodisalar va xatoliklar haqida diagnostik loglar ham yuritiladi. Ushbu loglarni Windows tizimidagi standart Event Viewer (Voqealar jurnali) dasturi orqali ko'rish mumkin. Har bir log yozuvi o'zining noyob identifikatoriga (Event ID) va muhimlik darajasiga (Severity Level) ega bo'ladi. Bu diagnostik loglar, ayniqsa, serverga qilingan hujumlarni, ruxsatsiz kirish urinishlarini yoki ma'lumotlar o'zgartirilganligini aniqlashda juda muhim rol o'ynaydi.

Magnet AXIOM kompyuterlar, mobil qurilmalar va bulut tizimlaridan dalillarni olish hamda tahlil qilish uchun mo'ljallangan keng qamrovli dasturiy ta'minot vositasidir. U elektron pochta tergovlarida ham qo'llaniladi va umumiy ma'lumotlarni tiklash uchun tavsiya etilgan vositalar qatoriga kiradi. AXIOM ikkita asosiy moduldan iborat: tergov ma'lumotlarini kiritish va dalillarni (masalan, disk obrazlarini) yuklash uchun mo'ljallangan Process moduli hamda yuklangan dalillarni tahlil qilish va ko'rib chiqish uchun ishlatiladigan Examine moduli. Matnda elektron pochta ma'lumotlarini AXIOM yordamida tiklash bo'yicha amaliyot ham ko'rsatilgan: AXIOM Process ishga tushirilib, yangi "Case" (ish) yaratiladi (InChap11 nomi bilan), dalil manbai sifatida kompyuter tanlanib, Jim Shu001.vhd disk obrazi yuklanadi, qidiruv turlari tanlanib, tahlil jarayoni boshlanadi (bu jarayon bir necha soat davom etishi mumkinligi aytilgan). Tahlil tugagach, AXIOM Examine ishga tushiriladi va unda "EMAIL" bo'limidan kerakli elektron pochta xabarlarini topiladi. Bu vosita nafaqat mavjud, balki o'chirilgan xabarlarini ham qayta tiklashga yordam berishi mumkin va .edb yoki log fayllari kabi dalillarni topishda qo'l keladi.

Autopsy raqamli forensika uchun mo'ljallangan, ochiq kodli va bepul dasturiy vositadir. U kompyuterlardagi ma'lumotlarni, jumladan elektron pochta fayllarini tiklash va tahlil qilish uchun ishlatiladi. Matnda Autopsy umumiy ma'lumotlarni tiklash va elektron pochta tergovlarida qo'llaniladigan asosiy forensik vositalardan biri sifatida Magnet AXIOM va OSForensics bilan bir qatorda sanab o'tilgan. U turli xil fayl tizimlarini tahlil qilish, o'chirilgan fayllarni tiklash, kalit so'zlar bo'yicha qidirish va topilgan dalillarni tartiblash kabi imkoniyatlarni taqdim etadi, bu esa uni elektron pochta bilan bog'liq tergovlarda foydali vositaga aylantiradi. Garchi matnda uning ishlashi AXIOM kabi batafsil yoritilmagan bo'lsa-da, u forensika hamjamiyatida keng qo'llaniladigan muhim vosita sifatida qayd etilgan.

MXToolBox asosan elektron pochta bilan bog'liq texnik masalalarni hal qilish va tahlil qilish uchun mo'ljallangan onlayn vositalar to'plamidir. Matnda u aynan elektron pochta sarlavhalarini (email headers) dekodlash, tahlil qilish va kuzatish uchun ishlatiladigan vosita sifatida keltirilgan. Elektron pochta sarlavhasi xabarining jo'natilish marshruti, ishtirok etgan serverlar, IP manzillar va vaqt belgilari kabi ko'plab texnik ma'lumotlarni o'z ichiga oladi, ammo bu ma'lumotlar ko'pincha murakkab formatda bo'ladi. MXToolBox kabi vositalar ushbu sarlavhalarni "ochib berish" va tushunarli formatda taqdim etishga yordam beradi. Matndagi Magnet AXIOM bilan ishlash jarayonida ham aynan shu vositadan foydalanish ko'rsatilgan: AXIOM Examine orqali topilgan elektron pochta xabarining sarlavhasi nusxalanib, MXToolBox veb-saytidagi (<https://mxtoolbox.com/EmailHeaders.aspx>) maxsus "E-mail Header Analyzer" maydoniga joylashtiriladi va "Analyze Header" tugmasi bosiladi. Natijada, sarlavhadagi texnik ma'lumotlar tahlil qilinib, xabarining kelib chiqishi va yo'li haqida qo'shimcha ma'lumot olish mumkin bo'ladi.

XULOSA

Elektron pochta serverlari, xususan UNIX (Postfix, Sendmail kabi vakillari bilan) va Microsoft Exchange kabi platformalar, raqamli aloqaning markaziy bo'g'ini bo'lishi bilan birga, kiberjinoyatlar tergovida asosiy ma'lumot manbai hisoblanadi. Serverlar tomonidan

yuritiladigan log fayllar (masalan, UNIX tizimlaridagi /var/log/maillog, Microsoft Exchange'dagi Tracking.log va diagnostika loglari) xabarlar almashinuvi, foydalanuvchi faoliyati, tizimga kirishlar, IP manzillar va aniq vaqt belgilari kabi tergov uchun o'ta qimmatli dalillarni saqlaydi. Ayniqsa, Microsoft Exchange serverining .edb ma'lumotlar bazasi fayllari elektron pochta xabarlarining o'zini va ular bilan bog'liq boshqa muhim ma'lumotlarni o'z ichiga oladi va maxsus forensika vositalari yordamida tahlil qilinishi mumkin.

Tergov samaradorligi uchun har bir server turining o'ziga xos jihatlari, jumladan, ularning konfiguratsiya fayllarini (masalan, /etc/syslog.conf, /etc/postfix/main.cf, /etc/mail/sendmail.cf), loglash mexanizmlarini (oddiy fayllar, tranzaksiya loglari, ESE, Message Tracking) va ma'lumot saqlash joylarini (/var/spool/postfix, .edb fayllari) tushunish muhim ahamiyat kasb etadi. Shu bilan birga, aylanuvchi loglar (circular logging) yoki provayderlar tomonidan belgilangan qisqa saqlash muddatlari kabi omillar tufayli dalillarning yo'qolishi ehtimolini ham hisobga olish zarur. Shu bois, elektron pochta serverlari forensikasi nafaqat chuqur texnik bilimlarni, balki vaziyatni to'g'ri baholash, o'z vaqtida harakat qilish va tegishli vositalardan samarali foydalanishni talab etadigan murakkab jarayondir. Ushbu murakkab tizimlardan ma'lumotlarni ajratib olish, o'chirilgan xabarlarni tiklash va chuqur tahlil qilishda Magnet AXIOM (keng qamrovli tahlil imkoniyatlari va amaliy ish oqimi misoli bilan), Autopsy (bepul va ochiq kodli muqobil sifatida) hamda MXToolBox (elektron pochta sarlavhalarini tahlil qilish uchun) kabi maxsus forensika vositalarining o'rni beqiyosdir. Matnda ko'rsatilganidek, bu vositalar ko'pincha birgalikda ishlatilib (masalan, AXIOM'dan olingan sarlavhani MXToolBox'da tahlil qilish), tergov samaradorligini oshiradi. Demak, zamonaviy elektron pochta forensikasi serverlarning ishlashini chuqur tushunishni va ushbu maxsus tahlil vositalaridan mohirona foydalanishni birlashtirgan kompleks yondashuvni talab qiladi.

ADABIYOTLAR:

1. Nakhimov, V. I. (2008). Raqamli kriminalistika: nazariy asoslari va amaliyot. Moskva: Yuridik nashriyoti.
2. Shapero, R. M. (2010). Digital Forensics and Cyber Crime: A Roadmap for Future Directions. Springer Science & Business Media.
3. Kaspersky, E. (2015). Phishing and Cybercrime: Defending Against Online Attacks. Kaspersky Labs.
4. Jones, J., & Smith, P. (2017). Cybersecurity: Understanding Phishing and Pharming Attacks. Journal of Cybersecurity, 14(3), 56-67.
5. Alvarez, F., & Ramirez, M. (2019). Forensic Linguistics: Theory and Practice in Criminal Investigations. Cambridge University Press.
6. Gasser, U., & O'Reilly, L. (2020). Cloud Services and Security: Risks and Safeguards. Wiley-Blackwell.

7. Clark, P., & Thornton, R. (2016). 419 Scams: Understanding and Preventing Financial Fraud. Financial Times.
8. Kumari, M., & Patel, S. (2018). Pharming and Its Impact on Internet Security. International Journal of Computer Applications, 45(8), 123-134.