Şəbəkə Mühiti üçün Kiberkriminalistik Həllər və Alətlərin Müqayisəli Analizi

[1]Elsevər Şiraliyev, [2]Emin Eyvazov, [3]Qədir Mikayılzadə
[1,2,3] Azərbaycan Texniki Universiteti, Bakı, Azərbaycan
[1]*esireliyev4@gmail.com*, [2]*emineyvazov271@gmail.com*, [3]*qadir.mikayilzada@gmail.com*

***Xülasə*— Müasir kibertəhlükələrin geniş vüsət aldığı bir şəraitdə şəbəkə trafikinin monitorinqi, rəqəmsal sübutların toplanması və analiz edilməsi kibertəhlükəsizlik sahəsində mühüm rol oynayır. Tədqiqat işində kiberkriminalistika prosesində istifadə olunan əsas alətlər və həllər, onların funksional imkanları və tətbiq sahələri müqayisəli analiz edilmişdir. Problemin ümumi qoyuluşu verilmiş şəbəkə mühitində rəqəmsal kriminalistika proseslərinin mərhələləri və təhlükəsizlik insidentlərinin araşdırılması üçün istifadə olunan metodlar araşdırılmışdır. Rəqəmsal sübutların etibarlılığı və şəbəkə təhlükəsizliyinin təmin olunmasında düzgün alət seçiminin xüsusi əhəmiyyət daşıdığı müəyyən edilmişdir.**

Açar sözlər*— *kiberkriminalistika; şəbəkə mühiti; təhlükəsizlik analizi; insident cavablandırma; paket analizi.

I. GİRİŞ

Müasir dövrdə informasiya texnologiyalarının sürətli inkişafı və korporativ şəbəkə infrastrukturlarının mürəkkəbləşməsi kibertəhlükələrin həm sayının, həm də modifikasiya dərəcəsinin əhəmiyyətli dərəcədə artmasına səbəb olmuşdur. Xüsusilə hibrid mühitlərdə və çoxsəviyyəli arxitekturalarda baş verən hücumlar – inkişaf etmiş davamlı təhdidlər (APT), paylanmış xidmətin inkarı (DDoS), mürəkkəb fidyə proqramları (ransomware) və məqsədyönlü icazəsiz giriş cəhdləri təşkilatların informasiya təhlükəsizliyinə qlobal səviyyədə ciddi təhdid yaradır. Bu kontekstdə rəqəmsal kiberkriminalistika (digital forensics) sahəsi təkcə hücumdan sonrakı reaktiv tədbir kimi deyil, eyni zamanda kibertəhlükəsizlik ekosisteminin ayrılmaz, davamlı komponenti kimi çıxış edir [1]. Kiberkriminalistika rəqəmsal mühitdə baş verən hadisələrin elmi metodologiyalara əsaslanan araşdırılması, hücum vektorlarının müəyyən edilməsi, sübutların toplanması və təhlil edilməsi proseslərini əhatə edir [2].

Xüsusilə şəbəkə mühitində kiberkriminalistik tədqiqatlar daha mürəkkəb xarakter daşıyır. Bunun əsas səbəbi rəqəmsal sübutların uçuculuq (volatility) səviyyəsinin yüksək olması, məlumatların dinamik şəkildə ötürülməsi və şifrələnmiş trafik həcminin artmasıdır [3]. İnsidentlərə reaksiya (DFIR) çərçivəsində rəqəmsal izlərin toplanması zamanı məlumatların tamlığının (integrity) qorunması və qəbul edilmiş beynəlxalq standartlara (məsələn, NIST və SANS prinsiplərinə) uyğun olaraq "Sübutların İzlənməsi Zənciri"nin (Chain of Custody) təmin edilməsi hüquqi və texniki baxımdan kritik əhəmiyyət kəsb edir [4, 5].

Şəbəkə trafikinin dərin paket analizi (DPI), genişləndirilmiş log məlumatlarının (məsələn, uç nöqtələrindən və şəbəkə avadanlıqlarından gələn telemetriyanın) mərkəzləşdirilmiş sistemlərdə korrelyasiyası və anomaliyaların aşkarlanması müasir təhlükəsizlik əməliyyatlarının əsas elementləridir [6]. Qabaqcıl kibermüdafiə təkcə reaktiv log analizi ilə məhdudlaşmır; eyni zamanda Kiber Təhdid Kəşfiyyatı (CTI) məlumatlarına əsaslanan proaktiv təhdid ovu (Threat Hunting) strategiyalarını tələb edir. Bu məqsədlə istifadə olunan mürəkkəb proqram alətləri və arxitektura həllərinin hər biri fərqli analitik qabiliyyətlərə, resurs istehlakına və inteqrasiya imkanlarına malikdir.

Bu qədər müxtəlif funksional imkanlara malik həllərin mövcudluğu kiberkriminalistik araşdırmaların optimallaşdırılmasını zəruri edir. Təqdim olunan məqalənin əsas məqsədi şəbəkə mühitində istifadə olunan spesifik kiberkriminalistik alətlərin müqayisəli analizini aparmaq, onların arxitekturaya inteqrasiya imkanlarını, üstün və zəif tərəflərini [7] müəyyənləşdirməkdir. Alınan nəticələr müxtəlif hücum ssenarilərində bu alətlərin effektivliyini qiymətləndirməyə və mürəkkəb korporativ şəbəkə infrastrukturunda insidentlərin araşdırılması prosesini optimallaşdırmaq üçün elmi əsaslandırılmış metodoloji tövsiyələr verməyə xidmət edəcəkdir.

II. ŞƏBƏKƏ MÜHİTİNDƏ KİBERKRİMİNALİSTİKA PROSESLƏRİ

Kiberkriminalistika prosesi standartlaşdırılmış və məntiqi ardıcıllıqla bir-birini izləyən bir neçə mərhələdən ibarətdir. Mürəkkəb korporativ şəbəkə infrastrukturunda bu mərhələlərin hər biri fərdi uç nöqtələrindən (endpoints) fərqli olaraq, hibrid və mərkəzləşdirilmiş yanaşma tələb edir. Ümumi qəbul edilmiş metodologiyalara əsasən, bu proses dörd əsas fazaya bölünür: məlumatların toplanması (Collection), qorunması, analizi və hesabatlılıq.

İlkin və ən kritik mərhələ identifikasiya və məlumatların toplanmasıdır. Şəbəkə mühitində rəqəmsal məlumatların böyük əksəriyyəti uçucu (volatile) xarakter daşıdığından, bu mərhələnin çevik icrası mütləqdir. Bu fazada tam şəbəkə trafikinin tutulması (Full Packet Capture - PCAP), şəbəkə avadanlıqlarından və mərkəzləşdirilmiş log idarəetmə (SIEM) sistemlərindən gələn telemetriya qeydləri xüsusi proqram təminatları vasitəsilə əldə edilir. Məlumatların düzgün, süzgəcdən keçirilmədən və tam şəkildə toplanması sonrakı korrelyasiya və analiz mərhələsinin dəqiqliyinə birbaşa təsir edən təməl faktordur [3].

Növbəti mərhələ əldə edilmiş məlumatların qorunması və

DOI: 10.25045/forensic.gov.2026.42

bütövlüyünün təmin edilməsidir (Preservation). Toplanmış rəqəmsal sübutların modifikasiya edilməsinin və ya zədələnməsinin qarşısını almaq üçün təcrid olunmuş saxlama mühitləri yaradılmalıdır. Bu məqsədlə sübutların orijinal vəziyyətini təsdiqləmək üçün qabaqcıl kriptoqrafik heşləmə alqoritmlərindən (məsələn, SHA-256) istifadə olunur. Məhz bu mərhələdə əldə edilmiş məlumatların hüquqi müstəvidə keçərliliyini təmin etmək üçün "Sübutların İzlənməsi Zənciri" (Chain of Custody) prosesi sənədləşdirilməli və ardıcıl olaraq izlənilməlidir [4].

Üçüncü faza olan analiz mərhələsi (Analysis) prosesin ən mürəkkəb və intellektual resurs tələb edən hissəsidir. Bu mərhələdə toplanmış və bütövlüyü təsdiqlənmiş məlumatlar detallı şəkildə araşdırılır, şübhəli fəaliyyətlər və komprometasiya indikatorları (IoC) müəyyən edilir. Şəbəkə mühitində bu proses dərin paket analizi (DPI), fərqli cihazlardan gələn logların kəsişdirilməsi (korrelyasiyası) və hücumçuların taktika, texnika və prosedurlarının (TTP) deşifrə edilməsi ilə həyata keçirilir [5]. Analiz nəticəsində kibertəhdidin vektoru, hücumun mənbəyi və infrastruktura vurulan zərərin miqyası dəqiq şəkildə modelləşdirilir [6].

Sonuncu mərhələ hesabatın hazırlanması və təqdimatıdır (Reporting). Bu mərhələdə tədqiqat ərzində əldə olunan bütün nəticələr, tapıntılar və tətbiq edilən metodologiyalar sistemləşdirilir. Hazırlanan kiberkriminalistik hesabat həm rəhbərlik üçün aydın anlaşılan strukturda, həm də mühəndislər və hüquq-mühafizə orqanları üçün texniki və hüquqi baxımdan tam əsaslandırılmış olmalıdır.

Yekun olaraq, bu mərhələlərin hər birinin vahid beynəlxalq standartlara uyğun həyata keçirilməsi kiberinsidentlərin effektiv araşdırılması, gələcək təhdidlərin proaktiv şəkildə qarşısının alınması və mürəkkəb şəbəkə infrastrukturlarında təhlükəsizlik əməliyyatlarının optimallaşdırılması üçün həlledici əhəmiyyət kəsb edir.

III. KİBERKRİMİNALSTİK ALƏTLƏR

Müasir çoxsəviyyəli və hibrid şəbəkə mühitlərində kiberinsidentlərin miqyası və mürəkkəbliyi araşdırma prosesində istifadə olunan kiberkriminalistik alətlərin funksional diversifikasiyasını zəruri edir. Hər bir alət insidentlərə reaksiya (DFIR) tsiklinin müəyyən mərhələsində spesifik tapşırıqların (şəbəkə telemetriyasının yığılması, log korrelyasiyası, yaddaş və disk analizi) yerinə yetirilməsi üçün arxitektur baxımdan optimallaşdırılmışdır. Korporativ mühitlərdə bu alətlər əsasən iki böyük sinfə ayrılır: Şəbəkə kriminalistikası (Network Forensics) və Uç nöqtəsi/Disk kriminalistikası (Endpoint/Disk Forensics). Aşağıda kiberkriminalistik tədqiqatlarda həlledici rola malik olan fundamental alətlərin texniki və metodoloji xüsusiyyətləri təhlil edilmişdir.

Şəbəkə Kriminalistikası Həlləri: Wireshark və Snort

Şəbəkə kriminalistikasının təməl daşlarından biri hesab olunan Wireshark, şəbəkə trafikinin Dərin Paket Analizi (Deep Packet Inspection - DPI) üçün qlobal standart kimi qəbul edilmiş [8] açıq mənbəli (open-source) protokolyöndümlü analizatordur. Wireshark OSI (Open Systems Interconnection) modelinin bütün səviyyələrində mikrosekund dəqiqliyi ilə paketləri tutur, qeydə alır (PCAP formatında) və vizuallaşdırır. Onun ən böyük elmi və praktiki üstünlüyü minlərlə müxtəlif şəbəkə protokolunu deşifrə (dissect) edə bilmə qabiliyyəti və qabaqcıl süzgəc (filtering) mexanizmidir. Bununla belə, alətin arxitekturası məlumatların avtomatlaşdırılmış korrelyasiyası üçün deyil, sırf xam məlumatların (raw data) əl ilə (manual) analizi üçün nəzərdə tutulmuşdur. Bu amil, Wireshark-ın kifayət qədər mürəkkəb interfeysi ilə birləşdikdə, ilkin çeşidləmə (triage) mərhələsində böyük həcmli məlumatların analizi zamanı istifadəçinin koqnitiv yükünü artırır və yüksək ixtisaslı kiber-təhlilçi tələb edir.

Şəbəkə mühitində kiberkriminalistik araşdırmaları qidalandıran digər kritik komponent isə Snort sistemidir. Əsasən Şəbəkəyə Müdaxilənin Aşkarlanması və Qarşısının Alınması Sistemi (NIDS/NIPS) olaraq təsnif edilən Snort, mürəkkəb imza əsaslı (signature-based) təhlil mexanizmindən istifadə edərək şəbəkədəki anomaliyaları [6, 9] və şübhəli fəaliyyətləri real-vaxt rejimində identifikasiya edir. Kiberkriminalistika kontekstində Snort fəal sübut toplayıcısı rolunu oynayır; o, zərərli trafik modellərini (məsələn, port skanlama, bufer daşmaları və qurd hücumları) aşkar etdikdə, bu barədə detallı log qeydləri generasiya edir. Lakin Snort-un effektivliyi bilavasitə mütəxəssis tərəfindən yaradılan və daim yenilənən konfiqurasiya qaydalar toplusundan (ruleset) asılıdır. Yanlış pozitivlərin (false positives) sayını minimuma endirmək və spesifik korporativ arxitekturaya uyğunlaşdırmaq üçün alət daimi tənzimləmə (tuning) tələb edir.

Rəqəmsal Sübutların Analizi Platformaları: Autopsy və FTK

Hücumun hədəf aldığı sistemlərdə (uç nöqtələrində və ya serverlərdə) post-mortem (hadisədən sonra) araşdırmaların aparılması üçün istifadə olunan alətlər fərqli yanaşma nümayiş etdirir. Autopsy, The Sleuth Kit (TSK) əsasında işləyən rəqəmsal kriminalistika platformasıdır. Açıq mənbəli və modul arxitekturaya malik olan bu alət istifadəçi dostu qrafik interfeysi ilə fərqlənir. Autopsy vasitəsilə tədqiqatçılar müxtəlif fayl sistemlərinin (NTFS, FAT, ext4 və s.) analizi, silinmiş məlumatların bərpası (data carving), xronoloji analiz (timeline analysis) və məlum zərərli faylların kriptoqrafik heşlərinə görə (məsələn, NSRL bazası əsasında) süzülməsi proseslərini effektiv şəkildə həyata keçirə bilirlər [10]. Bu xüsusiyyətlər onu standart DFIR (Digital Forensics and Incident Response) prosesləri üçün əvəzedilməz edir.

Bununla belə, çox böyük həcmli (terabaytlarla ölçülən) korporativ məlumatların emalı zamanı kommersiya alətlərinin performansı qabarıq şəkildə önə çıxır. Bu kontekstdə AccessData tərəfindən inkişaf etdirilən Forensic Toolkit (FTK) sənaye standartı [8, 11] hesab olunur. FTK-nın əsas üstünlüyü onun verilənlər bazasına əsaslanan (database-driven) arxitekturasıdır. Bu o deməkdir ki, məlumatlar alətə yükləndiyi zaman əvvəlcədən indeksləşdirilir; nəticədə analitiklərin axtarış və sorğu əməliyyatları inanılmaz dərəcədə sürətlənir. Alət həmçinin yaddaş (RAM) analizi, zərərli kodların aşkarlanması və mürəkkəb parolların sındırılması (PRTK inteqrasiyası) kimi genişləndirilmiş imkanlara malikdir. Lakin, kommersiya aləti olaraq FTK-nın lisenziya xərclərinin yüksək olması və işləməsi üçün böyük həcmdə aparat resursları (CPU, RAM, sürətli disk altsistemləri) tələb etməsi onun əsas məhdudiyyətlərindən sayılır.

IV. Alətlərin Funksional və Arxitektur Müqayisəsi

Mürəkkəb korporativ şəbəkə infrastrukturunda kiberkriminalistik araşdırmaların optimallaşdırılması və insidentlərə reaksiyanın effektivliyinin artırılması bilavasitə tətbiq edilən analitik alətlərin düzgün və məqsədyönlü seçilməsindən asılıdır. Tədqiqata cəlb olunan müxtəlif proqram həlləri fərqli əməliyyat mühitlərində özünəməxsus arxitektur xüsusiyyətlər, resurs istehlakı dinamikası və məlumat emalı metodologiyaları nümayiş etdirir. Bu baxımdan, kiberinsidentin xarakterindən, sübutların həcmindən və mühitin arxitekturasından asılı olaraq tədqiqatçılar üçün ən optimal alət seçimini elmi cəhətdən əsaslandırmaq zərurəti yaranır. Bu zərurəti qarşılamaq və texnologiyaların tətbiq ssenarilərini dəqiqləşdirmək məqsədilə yuxarıda təhlil edilən şəbəkə və uc nöqtəsi (endpoint) kriminalistikası alətlərinin çoxmeyarlı funksional parametrləri sistemləşdirilərək Cədvəl I-də təqdim edilmişdir. Tətbiq edilən bu müqayisəli yanaşma kiberkriminalistik tədqiqat prosesinin həm texniki, həm də əməliyyat baxımından səmərəliliyini obyektiv qiymətləndirməyə imkan verir.

CƏDVƏL I. Şəbəkə və Uc Nöqtəsi Kriminalistikası Alətlərinin Çoxmeyarlı Funksional Parametrləri

Alət	Kateqoriy/ Model	Əsas hədəf/ Funksiya	Məlumat arxitekturası	Texnoloji yanaşma
Wire-shark	Şəbəkə analizi (DPI)	Paket səviyyəli dərin analiz (PCAP)	Siyahı əsaslı xam məlumat (raw data) faylları	Xüsusi süzgəclər, əl ilə protokol təhlili, yüksək öyrənmə əyrisi
Snort	Şəbəkə təhlükəsiz-liyi (NIDS/ NIPS)	Real-vaxt təhdid aşkarlanmas ı və loglama	Qayda əsaslı mətn faylları, bazaya ixrac	İmza əsaslı monitorinq, daimi tənzimləmə tələbi
Autopsy	Disk/Uç nöqtəsi kriminalis-tikası	Fayl bərpası, sistem analizi və xronoloji araşdırma	TSK mühərrikli daxili SQLite bazası	Qrafik istifadəçi interfeysi (GUI), vizual analiz, orta resurs tələbi
FTK	Kompleks kriminalis-tika, kommersi-ya	Böyük həcmli məlumatları n indeksləşdir ilməsi, RAM analizi	Oracle/Postgre SQL verilənlər bazası arxitekturası	Avtomatlaşdı rılmış emal, çox yüksək aparat (CPU/RAM) tələbi

Tədqiqat işi çərçivəsində aparılan hərtərəfli təhlillər göstərir ki, mürəkkəb və çoxsəviyyəli korporativ şəbəkə infrastrukturlarında kiberkriminalistik araşdırmaların optimallaşdırılması birbaşa olaraq istifadə edilən analitik alətlərin məqsədyönlü seçimi və onların arxitektur inteqrasiyası ilə bağlıdır. Fərqli funksional təyinatlara malik bu alətlərin effektivliyi təcrid olunmuş şəkildə deyil, kiberinsidentin xarakterinə və mühitin miqyasına uyğunlaşdırılmış xüsusi tətbiq ssenariləri çərçivəsində qiymətləndirilməlidir. Aparılan müqayisəli analiz təsdiq edir ki, açıq mənbəli (open-source) kiberkriminalistik ekosistemlər ilkin triaj mərhələsində yüksək çeviklik, şəffaf modul arxitektura və maliyyə səmərəliliyi təqdim etsə də, terabaytlarla ölçülən rəqəmsal sübutların emalı və genişmiqyaslı insidentlərə reaksiya (DFIR) proseslərində kommersiya platformalarının təmin etdiyi mərkəzləşdirilmiş verilənlər bazası arxitekturası və yüksək hesablama performansı əvəzedilməzdir.

Bundan əlavə, vurğulamaq lazımdır ki, ənənəvi qayda (imza) əsaslı və əl ilə aparılan analiz metodları müasir şəbəkələrdə yaranan nəhəng həcmli (Big Data) telemetriya məlumatlarının təhlilində qeyri-kafi qalmağa başlayır. Bu tendensiya kiberkriminalistika proseslərində Süni İntellekt (AI) və Maşın Öyrənməsi (ML) alqoritmləri ilə gücləndirilmiş avtomatlaşdırılmış həllərin tətbiqini zəruri edir. Süni intellekt əsaslı qabaqcıl analitik yanaşmalar böyük verilənlər bazasında davranış anomaliyalarının (UEBA) və gizli komprometasiya indikatorlarının (IoC) sürətli korrelyasiyasını təmin edərək analitiklərin koqnitiv yükünü yüngülləşdirir və insan faktorundan irəli gələn xətaları minimuma endirir. Gələcək perspektivdə kiberkriminalistika paradiqmasının tamamilə SOAR (Təhlükəsizlik Orkestrasiyası, Avtomatlaşdırma və Reaksiya) inteqrasiyalı, avtomatlaşdırılmış ekosistemlərə doğru təkamül edəcəyi proqnozlaşdırılır.

Nəticə

Yekun qənaət ondan ibarətdir ki, mürəkkəb hücum vektorlarının (məsələn, inkişaf etmiş davamlı təhdidlər - APT) dəf edilməsi və dərindən araşdırılması üçün heç bir fərdi alət universal həll hesab edilə bilməz. Ən optimal və həlledici nəticə yalnız müxtəlif kiberkriminalistik alətlərin hibrid (kombinasiyalı) şəkildə istifadəsi – yəni şəbəkə telemetriyasının (NIDS/DPI) loglarının uç nöqtəsi (Endpoint) disklərindən əldə edilən xronoloji məlumatlarla kəsişdirilməsi ilə əldə edilə bilər. Bu sinergetik yanaşma həm rəqəmsal sübutların hüquqi bütövlüyünü ("Chain of Custody") təmin edir, həm də gələcək kibertəhdidlərin proaktiv şəkildə qarşısının alınması üçün insidentlərin daha yüksək dəqiqliklə modelləşdirilməsinə imkan yaradır.

ƏDƏBİYYAT

[1] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," NIST Special Publication 800-86, National Institute of Standards and Technology, 2006.

[2] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press, 2011.

[3] A. Ghazvini and Z. Shukur, "Awareness of Volatile Data Preservation in Network Forensics," Procedia Technology, vol. 11, pp. 334–340, 2013.

[4] SANS Institute, "Forensic Analysis of Network Traffic and Threat Hunting Methodologies," SANS Reading Room, 2023. https://www.sans.org/reading-room/

[5] U.S. Department of Justice, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," Cybercrime Lab, OLE, 2020.

[6] R. Bace and P. Mell, "Intrusion Detection Systems," NIST Special Publication 800-31, 2001.

[7] H. Al-Dawsari and M. Al-Qurishi, "A Comparative Analysis of Digital Forensics Tools for Corporate Network Environments," IEEE Access, vol. 9, pp. 1125–1138, 2021.

[8] A. Orebaugh, G. Ramirez, and J. Beale, Wireshark & Ethereal Network Protocol Analyzer Toolkit. Syngress, 2006.

[9] M. Roesch, "Snort: Lightweight Intrusion Detection for Networks," in Proceedings of the 13th USENIX Conference on System Administration (LISA '99), 1999, pp. 229–238.

[10] B. Carrier, File System Forensic Analysis. Addison-Wesley Professional, 2005.

[11] M. H. Ligh, A. Case, J. Levy, and A. Walters, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. John Wiley & Sons, 2014.

Comparative Analysis of Cyber Forensic Solutions and Tools for Network Environments

Elsevar Shiraliyev[1], Emin Eyvazov[2], Gadir Mikayilzada[3]
[1,2,3]Azerbaijan Technical University, Baku, Azerbaijan
[1]*esireliyev4@gmail.com*, [2]*emineyvazov271@gmail.com*,
[3]*qadir.mikayilzada@gmail.com*

Abstract - A comparative analysis of cyber forensic solutions and tools in the network environment was conducted. With the increase in modern cyber threats, monitoring network traffic, collecting and analyzing digital evidence plays an important role in cybersecurity. In this work, the main tools and solutions used in the cyber forensics process, their functional capabilities, performance and application areas were comparatively analyzed. The general statement of the problem was given, the stages of digital forensic processes in the network environment and the methods used to investigate security incidents were studied. Based on the conducted research, the effectiveness of various cyber forensic tools was assessed and their applicability in different network scenarios was compared. As a result, it was determined that the right choice of tool is of critical importance in ensuring the reliability of digital evidence and network security.

Keywords - cyber forensics; network environment;, digital forensics; security analysis; incident response; packet analysis.