ОӘЖ 004.056

КОМПЬЮТЕРЛІК ИНЦИДЕНТТІ ТЕРГЕУДЕ DIGITAL FORENSICS FRAMEWORK ҚОЛДАНУ

Мұхамәдиев Мадияр Ғалелұлы
mdrenu@mail.ru
Л.Н.Гумилев атындағы ЕҰУ ақпарттық технологиялар факультетінің
4-ші курс студенті, Нұр-Сұлтан, Қазақстан
Ғылыми жетекші – Сагиндыков Каким Молдабекович

Кез-келген қылмыстық тергеу кезінде "дәлелдемелер жинау" сияқты процесс бар. Алибиді тексеру, саусақ іздерін және кей кезде жеміс іздерін мен қанды анықтау сияқты дәлелдерді жинау кәдімгі криминалистика жиі кездеседі. Жоғарыда аталған дәлелдемелер жиынтығы "аналогтық дәлелдер" ретінде анықталады. Бірақ әлі күнге дейін біздің көзімізге көрінбейтін дерексіз дәлелдер бар екені барлығына белгілі факт, олардың бас бөлігі компьютерлік ортада жасырылған. Мұндай цифрлық сот дәлелдерін жинау "цифрлық дәлелдер" болып табылады.

Қазіргі қоғам ақпараттық қоғам және цифрлық қоғам деп аталатындықтан, бүгінде "цифрлық дәлелдерді" қамтамасыз ету аналогтық дәлелдерді жинау сияқты маңызды болып отыр. Осы сандық дәлелдемелерді зерттеу процесі "цифрлық криминалистика" немесе “Форензика” деп аталады.

Жалпы айтқанда, интернет-технологиялардың дамуымен қылмыстық орта да тез өзгеріп отырады. Оған байланысты қазіргі адамдардың өмірінде сандық криминалистиканың пайда болуы көбірек кездеседі. Бүгін цифрлық сот-медициналық технологиялары, тек тергеу агенттіктерімен шектелмейді. Жалпы мақсаттағы компаниялар мен қаржы компаниялары сияқты жеке секторларда, бұл технологияға деген қажеттілік күннен-күнге артып келеді. Мысалы, сот-медициналық технологияларды сақтандыру кезіндегі алаяқтықтың заңды дәлелдерін жинау және интернет-банкинг арқылы зиянды өтеу, ішкі ақпараттың ағып кетуіне жол бермеу және бухгалтерлік аудит сияқты ішкі қауіпсіздікті күшейту үшін пайдалануға болады.

"Форензика" термині ағылшынның "forensic science" сөзінің қысқартылған түрі, сөзбе — сөз "сот ғылымы", яғни дәлелдемелерді зерттеу туралы ғылым деп аударылады. "Форензика" термині кез-келген криминалистиканы білдірмейді, атап айтқанда оны тек қана компьютерлік криминалистикада қолданады. Оның негізгі саласы - компьютерлік ақпаратқа қол сұғу объектісі ретінде, компьютер қылмыс құралы ретінде, сондай-ақ кез-келген цифрлық дәлелдер ретінде пайда болатын оқиғаларды талдау және тергеу.

Оларға мысал ретінде, веб-серверді бұзу немесе құпия ақпараттың ағуы, құнды деректерді шифрлау және ұқсас мәселелерді жатқызуға болады. Мұндай оқиғалар орын алған кезде, оны бірінші болып жедел әрекет ету топтарының қызметкерлері байқауға тиісті. Бұл жағдайда олардың алдына келесі міндеттер қойылады:

- шабуыл қалай жүзеге асырылғанын түсіну;
- бұзу сценарийін құру;
- шабуыл хронологиясын қалпына келтіру;
- артефактілерді жинау (шабуылдан кейін қалған іздер);
- осындай инциденттер алдағы уақытта қайталанбау үшін, алдын ала қорғау шараларын құрып ұсыну.

Қазіргі кезде өзіндік бренді бар ірі компаниялардың көпшілігі міндетті түрде, бірнеше форензика ісінің шеберлерінен тұратын мамандырылған зертханаларын құрады. Сондай-ақ, форензика көбінесе IT саласынан алыс компаниялардың қызметтерінің бөлігі болып табылады. Мысалы, қаржылық аудитпен айналысатын компаниялар. Шынында да, қаржылық алаяқтықты тергеу кезінде барлық дәлелдердің 100% - ы компьютерлік жүйелерде (ERP, CRM, BI, BPM және т.б.) болуы мүмкін.

Әрине, форензика мамандары юрисприденцияның ажырамас бөлігі болып табылады. Шынында да, компьютерлік қылмыс фактілері бойынша қылмыстық іс қозғау үшін алдымен

Заң нормаларына сәйкес қылмыс фактісін растау және оның құрамын анықтау қажет. Сол сияқты, егер зардап шеккен компания бұзу салдарынан келтірілген залалды өндіріп алу үшін сотқа жүгінсе, онда сараптамасыз болмайды. Криминалистика тәсілдеріне қысқаша сипаттама берейік және сараптау тәсілдерін қарастырайық.

Статикалық талдаудың міндеттері-қатты дискінің немесе жедел жадтың қоқысының кескінін жасау (көшіру), жойылған файлдарды, жүйелік каталогтардағы қалыптан тыс файлдардың қалдықтарын анықтау және қалпына келтіру, веб-шолғыштың серфинг тарихын, жүйелік журналдарды (авторизация оқиғалары, файлдар мен каталогтарға кіру аудиті және т.б.) жинау, жадта жұмыс істейтін процестер мен ашық желі қосылыстарының тізімін алу.

Динамикалық талдау, не болып жатқанын толық көрсету үшін әртүрлі жағдайларда іске қосылған жүйенің снапшоталарын кесуді қолданады. Мысалы, малвар белгілі бір әрекеттерден кейін өзінің коды мен инфекция белгілерін жоюға бейім. Егер осы уақытқа дейін бұзылған жүйенің снапшоты алынып тасталса, онда бұл малвардың жәбірленушінің компьютерінде не істегені туралы мәліметтер алуға нақты мүмкіндік бар. Тиісінше, скриншоттар, Желіге қосылу журналдары, Берілетін трафик, оқиғаға дейін және одан кейінгі ОЖ файлдық жүйесінің жағдайын салыстыру электрондық куәліктердің тігісі бола алады.

DFF (Digital Forensics Framework) - бұл жеке API-нің үстіне салынған ашық кодты криминалистикалық компьютерлік платформа. DFF құрылғысы бүгінгі күнге дейін қолданылыста болған ескірген цифрлық криминалистикалық фреймворктарды ауыстыруға арналған. Қарапайым пайдалану және автоматтандыру үшін жасалған DFF-тің интерфейсі қолданушыны сандық тергеудің негізгі қадамдары арқылы жүргізеді. Сондықтан оны цифрлық тергеулерді тез және оңай жүргізу және оқиғаларға жауап беру үшін мамандар да, жай ғана студенттер де қолдана алады. DFF дискіні және жылдам өзгеретін жадты жылдам талдауға, компьютерлер мен смартфондарды терең зерттеуге қабілетті. DFF дәлелдерді қорғау және медианың тұтастығын сақтау үшін блокты жазу технологиясын қолданады. Қуатты интеграцияланған іздеу қозғалтқышы құжаттар, медиа және пошта жәшіктеріндегі артефактілерді тез табуға мүмкіндік береді.

DFF-тің мүмкіндіктері:

1. Дәлелдемелерді сақтау
- Логикалық блоктарды жазу
- Шикі форматтарды талдау
- Encase EWF файл пішімімен үйлесімділік
- Aff файл пішімімен үйлесімділік
- Криптографиялық хэш есептеу

2. Деректерді жылдам қысқарту және сұрыптау
- Файл қолтаңбаларын анықтау
- Жетілдірілген сүзу және іздеу қозғалтқышы

3. Томдар мен файлдық жүйені қайта құру
- бөлімдерді анықтау және орнату
- виртуалды диск пішімі VMDK
- FAT 12/16/32 (Thumbdrive)
- ADS және қысу қолдауы (Microsoft Windows) бар NTFS
- HFS HFS + hfsx файлдық жүйелері (OS X және iphone)
- Ext2/3 / 4 файлдық жүйелер (GNU / Linux және Android)

4. Мультимедиялық талдау
- Галереяны қарау
- EXIF метадеректерін таңдау

5. Windows ОЖ-ны талдау

- Регистрді талдау
- Microsoft Outlook PST пошта жәшіктері
- Preferch-ті талдау
- LNK файлдардың талдаушысы

6. Жадты талдау

- Volatility фреймворкімен біріктіруі
- Процесстер ағашының графикалық қайта құруы (pstree және psxview қоспасы)
- Процестер туралы ақпарат (қосылымдар, procdump)
- Күдікті деп белгіленген rwx беттерімен VAD қатынасы

7. Құжаттарды талдау

- Ерекшеленген көрушілер (PDF, мәтін, Вэб форматында)
- Кеңсе құжаттарының метадеректерін, мәтінді және кірістірілген суреттерді бөлектеу

Қолданылған әдебиеттер

1. Мессье P. Network Forensics 1st Editio, 2017. – 360 б.
2. Тамма Р. , Боммизетти С. , Махалик Х. Practical Mobile Forensics, 2014. – 400 б.
3. Саммонс Д. The Basics of Digital Forensics:The Primer for Getting Started in Digital Forensics, 2011. – 177 б.
4. Федотов Н.Н. Форензика-компьютерная криминалистика-М .: Юридический мир, 2007.-360 б.
5. Харлан Карви. Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 8, 2014 – 346 б.
6. Сапронов К. , Шаабан А. Practical Windows Forensics Paperback, 2016 – 324 б.
7. Джеймс М. , Кейси Э. Malware Forensics Field Guide for Windows Systems, 2010 – 560 б.
8. DFF (Digital Forensics Framework – цифровой криминалистический фреймворк). https://kali.tools/?p=1227