Дигитална форензика и анализа трагова у сајбер безбедности

Гране, процес и примене

Стефан Павловић

Математички факултет универзитета у Београду

14. јануар 2026.

Увод

- Појава са развојем личних рачунара
- Посебан значај у 21. веку због велике брзине развоја технологије
- Примена код органа реда и компанија - Органи реда је примењују у класичним истрагама док компаније је могу применити у интерним истрагама инцидената
- Прихватање дигиталних доказа на суду - У дигиталној форензици постоје специјалне процедуре које се прате да би ти дигатлни докази били прихваћени на суду

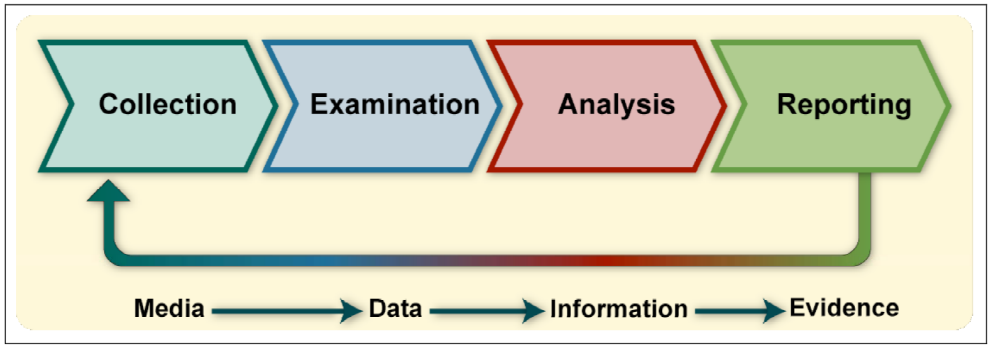
Историја дигиталне форензике

- Рани облици сајбер криминала су били много једноставнији, али и не знатно истраживани
- Недостатак алата и ресурса - разлог због којег се није придавало много значаја случајевима високотехнолошког криминала
- Развој касних деведесетих и раних двехиљадитих - технологија постаје аспект свакодневног живота
- Све то захтева увођење стандарда и школовање истражитеља

Гране дигиталне форензике

- Рачунарска форензика
- Форензика база података
- Мрежна форензика
- Меморијска форензика
- Разне друге

Процес дигиталне форензичке истраге (NIST)



1. Прикупљање података
2. Преглед
3. Анализа
4. Писање извештаја

Форензичко прикупљање података

- Клонирање дискова без измене оригинала
- То се ради јер је врло важно очувати интегритет доказа

Преглед и анализа података

- Анализа лог датотека и комуникације - Може открити много тога
- Обнова обрисаних података - Важно ако неко покуша да сакрије податке (доказе)
- Дешифровање података и анализа метаподатака - Теже, али може открити много тога
- Повезивање трагова у целину

Анализа трагова у сајбер-безбедности

- Индикатори компромитовања (IOC)
- Сумњиве IP адресе и саобраћај - Може открити много о покушају неког напада (нпр. IP адреса која је већ извршила неки напад у прошлости)
- Реконструкција сајбер инцидента - Важно за писање извештаја о инциденту
- Превенција будућих напада

Примена у високотехнолошком криминалу

- Истраге хаковања и ransomware напада - Све већи проблем са обзиром на то да нам се већина живота одвија у дигиталном свету
- Финансијске и криптовалутне преваре
- DFIR у корпоративном окружењу
- Dark web истраге - Важне с обзиром на то да се на dark weby одвијају нелегалне транзакције и друге нелегалне активности

Примена у осталим кривичним делима

- Убиства, напади, крађе, преваре
- Анализа телефона, GPS-а и порука
- Нови тип доказа при класичним кривичним делима
- Пример: BTK серијски убица - једно од првих убистава решених употребом дигиталне форензике

Закључак

- Кључна улога у савременим истрагама
- Повезује технологију и право
- Будућност: IoT и вештачка интелигенција

Хвала на пажњи ☺☺☺