Дигитална форензика е процес на идентификација, складирање, испитување и анализа на дигитал ни докази со користење на
научно прифатен и валиден процес и конечно презентирање на тие докази

Принцип на Локард
◦ во физичкиот свет, секогаш кога сторителите ќе влезат или ќе го напуштат местото на злосторств ото,
тие ќе остават нешто зад себе и ќе земат нешто со себе.

Дигиталната форензичка анализа се дели на четири подфази, кои исто така претставуваат четири принципи на успешен
процес.
Идентификација,
Зачувување,
Анализа и
Известување

Главниот елемент во дигиталната форензичка анализа е дигиталниот уред

Цел на форензичката анализа
◦ да се валидираат дигиталните докази, со цел да се потврди или отфрли основната хипотеза.

Генерално постојат два пристапи кон анализа:
- Анализа во живо
- Анализа по настанот

Слоеви на апстракција на податоци
Физички слој
◦ Податоци во изворен облик
◦ Проблем: потежок за работа

Логички слој
◦ Податоци во поедноставен облик
◦ Проблем: можност за грешки

Временска анализа
- се користат докази за следење настани, да се утврдат локациите, насоката или времето и времет раењето на дејствијата.

- Релациона анализа - се проверува каде некој предмет е во однос на другите објекти и како тие ме ѓусебно комуницираат или се однесуваат.

- Функционална анализа - се гледа начинот на кој работи нешто или како се користело.

Основниот процес на форензичката анализа е.
1. Прибирање и преглед на податоците
2. Формирање на хипотеза
3. Евалуација на хипотезата
4. Заклучок и извештај

С-скалата (Скала на сигурност) обезбедува метод за сигурност при повикување на дигитални доказ и и
квалификување на заклучоците.
Некои форензичари користат помалку формален систем за степени на веројатност:
- (1) скоро дефинитивно,
- (2) највероjатно,
- (3) веројатно,
- (4) многу веројатно
- (5) евентуално.

стратегија за вршење на форензичка анализа со три нивоа:
◦ (1) triage forensic inspection,
◦ (2) survey forensic examination,
◦ (3) in-depth forensic analysis

Стеганографија
- Криење на податоци во други документи

Електронско откривање или „E-discovery“ е размена на податоци помеѓу страните во граѓанска или кривична парница.

Треба да се одлучи дали податоците ги исполнуваат следниве три критериуми т.е. дали информац иите се
◦ релевантни,
◦ непривилегирани и
◦ разумно достапни

Постојат пет локации за дигитално складирање што се типичен фокус еоткривање:
◦ Workstation environment (вклучувајќи стари, тековни и домашни компјутери, лаптопи)
◦ Personal Digital Assistants (мобилни телефони)
◦ Removable media (CD, DVD, USB)
◦ Server environment (датотеки, е-пошта, база на податоци)
◦ Backup environment (архиви, бекап)

Основните компоненти на сеопфатната и темелна истрага за идентификување на потенцијално ре левантното податоци се:
информативните интервјуа и
барањата за документација

Главните цели во фазата на обработка на податоците се:
трансформација на податоци
◦ во читлив формат за да може правник да ги разгледа податоците за релевантност и привилегија
намалување на податоците
◦ преку филтрирање за типови на датотеки, дупликати, датум и клучни зборови

Двете главни задачи во истрагата за упад на системи се:
проценка на опсегот (Scope Assessment)
реконструкција на криминалот (Crime Reconstruction)

Некои од почестите почетни набудувања се:
◦ Antivirus
◦ IDS
◦ “Blacklist” правила
◦ Информации надвор од инцидентот

На Интернет на Нештата се гледа како на:
◦ Огромен број паметни, поврзани „нешта“ (еден вид на глобална мрежа во облак)

Едни од побитните технологии се:
◦ Вештачката Интелигенција,
◦ Уреди за Идентификација со Радио Фреквенција (Radio Frequency Identification Devices),
◦ мобилни уреди и
◦ платформи за користење на облак (Cloud Platforms).

Предизвиците кои доаѓаат со Интернет на Нештата може да се разгледуваат од два аспекти:
◦ Аспект на Приватност (Privacy Aspect)
◦ Аспект на Безбедност (Security Aspect)

Според Saini et al, сајбер криминалот генерално може да се подели во 4 категории:
◦ Податочен Криминал
◦ Мрежен Криминал
◦ Криминал на Пристап
◦ Содржински Криминал

Според истражувањето во трудот на Zawoad et al. Дигиталната форензика е процес кој се состои о д 4 основни чекори:
◦ Идентификација
◦ Колекција
◦ Организација
◦ Презентација

Дигиталната Форензика во Интернет на Нештата се дели на 3 дела:
◦ Форензика на Уред
◦ Форензика на Мрежа
◦ Форензика на Облак

Препорачаниот модел се состои од два клучни дела:
◦ Модел на 1,2,3 Зони (1,2,3 Zones Model)
◦ Модел на Следно Најдобро Нешто (Next Best Thing Triage Model)

Процесот на форензичка истрага со споменатиот модел се одвива во 4 фази:
◦ Фаза на Подготовка
◦ Фаза на Собирање на Податоци
◦ Истрага
◦ Извештај и Складирање

Трите модели на сервиси на cloud computing се категоризирани како IaaS, PaaS и SaaS.

Четирите модели за распоредување на облак компјутери се: јавен облак, приватен облак, хибриде н облак и облак на заедницата