УДК 004.9

Володимир Сергійович МАКАРОВ,
старший судовий експерт Харківського науково-дослідного експертно-криміналістичного центру МВС України

МЕТОДИ ДОСЛІДЖЕННЯ JTAG ТА CHIP-OFF У КОМП'ЮТЕРНО-ТЕХНІЧНІЙ ЕКСПЕРТИЗІ

В комп'ютерно-технічній експертизі методи дослідження JTAG ТА CHIP-OFF все більше викликають великий інтерес та необхідність в їх застосуванні, оскільки ці методи дозволяють отримати прямий доступ до даних які можуть перебувати під захистом (наприклад, захист паролем) або даних що містяться в пам'яті пошкоджених пристроїв.

На поточний момент JTAG (Joint Test Action Group) – це промисловий стандарт яким оснащуються практично всі складні цифрові мікросхеми. Фізично він представлений на платі у вигляді точок або коннекторів для підключення спеціального обладнання. Використовується JTAG для прошивки мікросхем з пам'яттю та їх вихідного контролю на виробництві, тестування готових плат, відладочних робіт при проектуванні апаратури та програмного забезпечення.

Тобто JTAG являє собою апаратний інтерфейс для прямого зв'язку робочої станції (персонального комп'ютера) з материнською платою пристрою за допомогою програматорів, наприклад Z3X Easy-Jtag, RIFF Box, Octopus.

Для вилучення даних з пристроїв за допомогою методу JTAG експерт повинен бути забезпечений необхідним програмним та апаратним забезпеченням програматора-JTAG, паяльником або паяльною станцією, припоєм, дротовими з'єднаннями та схемою розміщення на платі мобільного пристрою точок JTAG.

У випадках коли методом JTAG немає можливості скористатись, внаслідок пошкодження плати пристрою, або відсутньою схемою розміщення точок стандарту на платі – є можливість у використанні не менш значимого методу CHIP-OFF.

Якщо розглядати метод CHIP-OFF з точки зору комп'ютерно-технічної експертизи – то це технологія, за якою мікросхема пам'яті вилучається з печатної плати пристрою, проводиться її підготовка для зняття фізичного дампу пам'яті та подальше вилучення цього дампу за допомого програматорів з подальшою обробкою отриманих даних за допомогою спеціального програмного забезпечення.

Наразі існує два види пам'яті NAND – це TSOP и BGA. Основна відмінність мікросхем пам'яті типу TSOP – наявність контактів, що розміщені по контуру мікросхеми та зпаюються з платою. Демонтаж таких мікросхем найпростіший, але потребує великої акуратності. Що до мікросхем типу BGA (Ball Grid Array – масив кульок) – то процес з ними значно важчий. У даному типу мікросхем контакти виконані у вигляді кульок на основі мікросхеми, які припаяні до плати. А ще мікросхеми BGA не мають єдиного стандарту та кожен виробник може розробити та використовувати власний тип мікросхеми зі своїм розміщенням контактів.

Для вилучення даних з пристроїв за допомогою методу CHIP-OFF експерт також повинен бути забезпечений паяльною станцією, припоєм, флюсом, програматорами, що зчитують пам'ять, адаптерами які відповідають топологіям розміщення контактів на мікросхемі, програмним забезпечення для зчитування та обробки даних.

Після зняття фізичного образу даних обох методів, дампи пам'яті обробляються за допомогою програмних продуктів Oxygen Forensics або Cellebrite UFED Physical Analyzer. У випадку вилучення інформації за методом CHIP-OFF, може знадобитись «збірка» дампу, що являє собою виключення службових областей та корекцію стиків сторінок пам'яті. Для цих цілей можна використовувати програмне забезпечення ACE Laboratory.

Важливо зазначити, що для використання методів JTAG та CHIP-OFF, експерт комп'ютерно-технічної експертизи повинен мати розуміння в організації даних на мікросхемах пам'яті, володіти навичками демонтажу та повторного. монтажу компонентів пристрою.

На теперішній час, більшість носіїв інформації які надходять на комп'ютерно-технічну експертизу – це мобільні телефоні та планшетні комп'ютери. До того ж, з кожним днем все більше зростають вимоги до якості та кількості даних що вилучаються з портативних пристроїв. Сьогодні вже недостатньо вилучення лише списку контактів, СМС та журналу дзвінків, а обов'язково стоїть задача у вилученні історії листу-

вання засобами мережі інтернет за допомогою месенджерів, вилучення ГЕО-даних, зображень та відео, відновлення видалених даних. Однак, не всі дані, навіть при наявності їх в мобільному пристрої, можуть бути вилучені. Це пов'язано з апаратними та програмними особливостями зберігання даних в конкретному мобільному пристрої конкретного виробника.

Вже зараз можна сказати, що методи JTAG та CHIP-OFF стають все більш необхідними в сучасній комп'ютерно-технічній експертизі, адже можуть вирішити важливі питання що потребують непростих рішень та вирішення яких звичними методами не виявилося можливим.

Список бібліографічних посилань

1. Cellebrite Advanced JTAG Extraction (CAJE) // Cellebrite. 14.01.2020. URL: https://www.cellebritelearningcenter.com/mod/page/view.php?id=11903 (дата звернення: 28.04.2020).
2. Elder B. Chip-Off and JTAG Analysis. Evidence technology magazine. June 2012. URL: http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=922 (дата звернення: 28.04.2020).
3. Макаров А. Получение данных из мобильных устройств с помощью интерфейса отладки JTAG // Anti-Malware : сайт. 18.04.2017. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Getting_data_from_mobile_devices_using_JTAG_debug_interface (дата звернення: 28.04.2020).

Одержано 30.04.2020