

**Домашнее задание № 25**

***Forensics, Incident response***

***part 2***

1. **Изучить основные виды HTTP methods and requests**
2. **Установить volatility на ubuntu**

* Установить набор программных инструментов для криминалистического анализа данных [Volatility](https://github.com/volatilityfoundation/volatility3)

1. **Установить avml либо Lime**

* Снять дамп ram (оперативной памяти) linux с помощью [AVML](https://github.com/microsoft/avml)
* Узнать точно профиль вашей linux системы uname -a
* С помощью набора инструментов [Volatility передав точный imageinfo](https://docs.google.com/document/d/1v7u6HVrae1R4fCCs1SNAGryjy5tmJCPDKq2Hyhqd9Fo/edit?usp=sharing) (профиль из которого вы сняли дамп) открыть дамп оперативной памяти, скрин вывода прикрепить

Ссылки на дополнительные ресурсы

* [HTTP methods, headers, responses](https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods)
* [ELK подробный обзор видео](https://www.youtube.com/watch?v=syjTFmLY2T4)
* [Volatility 3: The volatile memory extraction framework](https://github.com/volatilityfoundation/volatility3)
* [AVML утилита для снятия дампа оперативной памяти RAM](https://github.com/microsoft/avml)
* [**Примеры работы с VOLATILITY**](https://docs.google.com/document/d/1v7u6HVrae1R4fCCs1SNAGryjy5tmJCPDKq2Hyhqd9Fo/edit?usp=sharing)