Инструкция для заказчиков по запуску стандартного режима PT Responder (PT Dumper)

1. О PT Responder (PT Dumper) в стандартном режиме

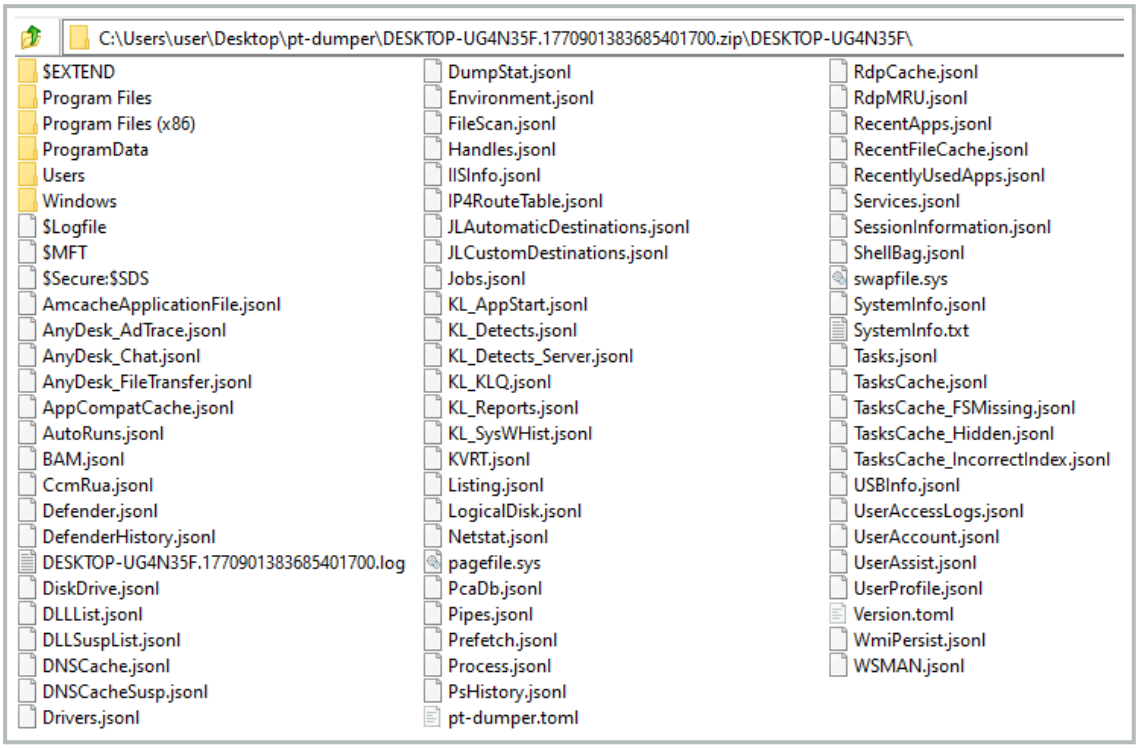
Стандартный режим **PT Responder (PT Dumper)** предназначен для точечного сбора необходимого набора системных данных для их последующего анализа с целью определения признаков компрометации узла на базе различных операционных систем.

В этом режиме **PT Responder (PT Dumper)** выполняет следующие действия:

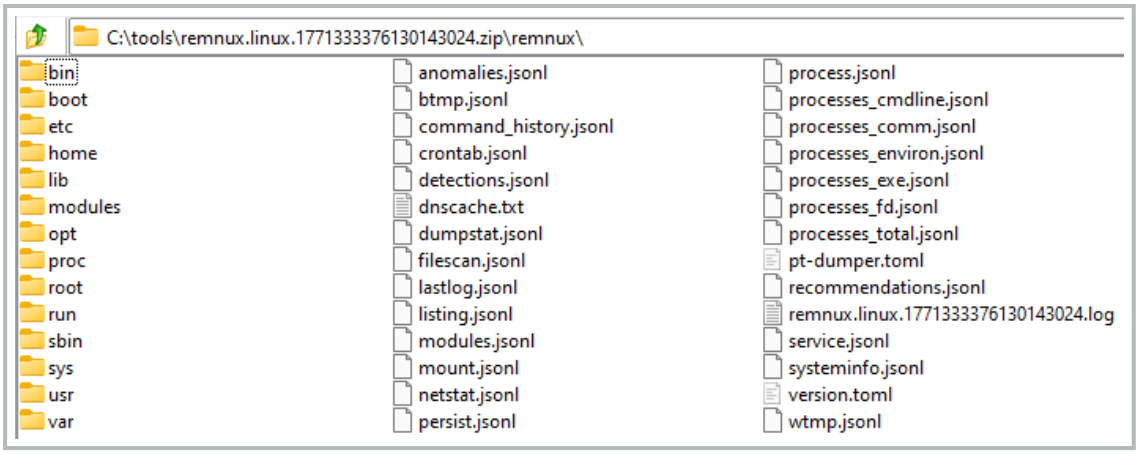
- Запускает расширенный набор live response модулей (Netstat, Dnscache, SystemInfo и т.д.);
- Запускает сигнатурное сканирование областей системного диска с помощью YARA-правил;
- Осуществляет поиск известных индикаторов компрометации (Indicators of Compromise);
- Собирает журналы работы ОС и расширенный перечень криминалистических артефактов.

Данные собираются локально в нативном формате или в формате JSON. Данные хранятся в ZIP-архиве, защищенном паролем.

Пример набора данных, собранных с узла под управлением Windows:



Пример набора данных, собранных с узла под управлением Unix:

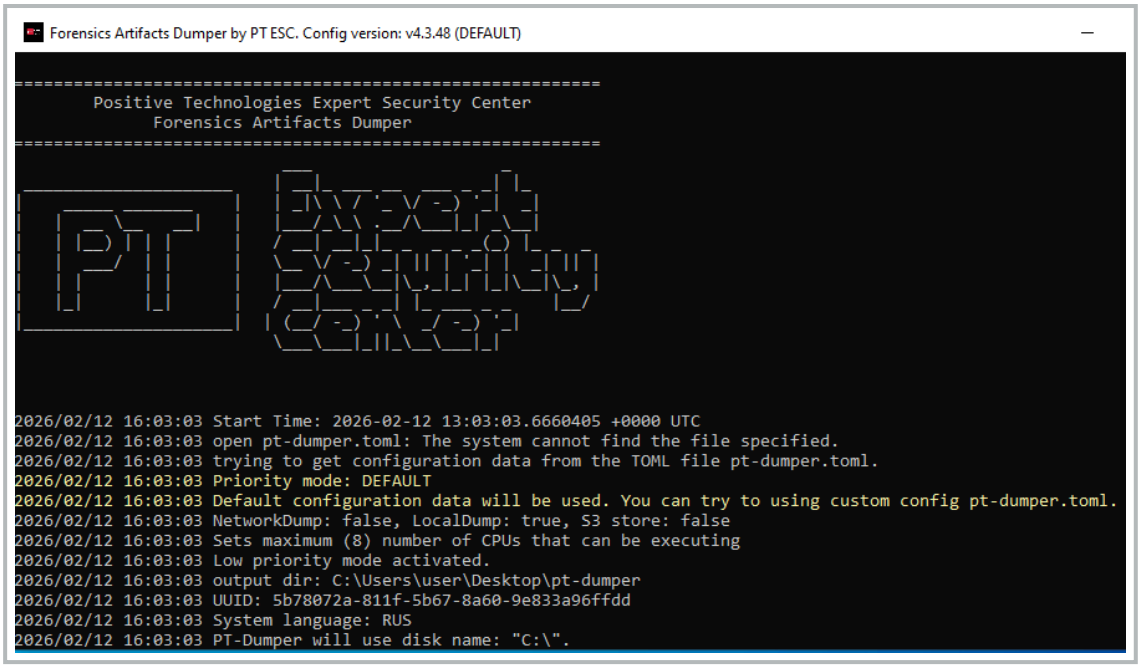


2. Windows

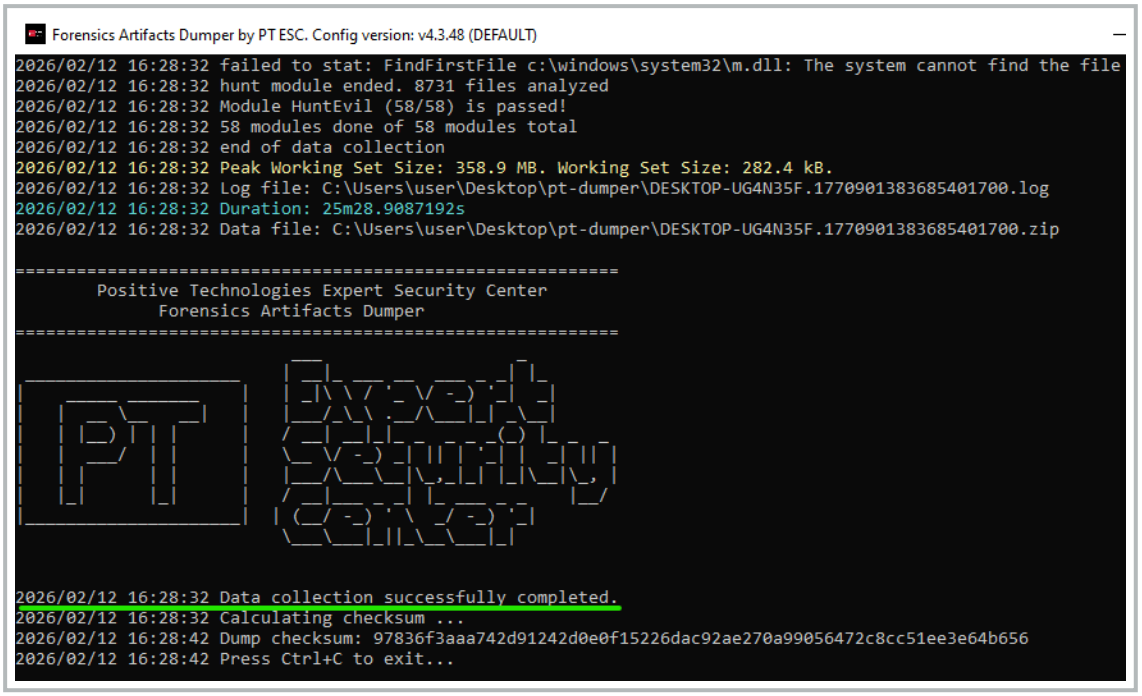
1. В зависимости от архитектуры необходимо выбрать один из следующих исполняемых файлов:
   - `pt-dumper.abcdefg.win64.legacy.exe` – пример исполняемого файла для 64-разрядной версии ОС Windows;
   - `pt-dumper.abcdefg.win32.legacy.exe` – пример исполняемого файла для 32-разрядной версии ОС Windows (данный исполняемый файл возможно запустить и на 64-разрядной версии ОС Windows);
2. Убедитесь, что хост, на котором будет запускаться утилита, удовлетворяет **следующим требованиям**.

PT DUMPER ДЛЯ WINDOWS								
ОС	МИНИМАЛЬНЫЕ				РЕКОМЕНДУЕМЫЕ			
	ОЗУ	ДИСК	CPU	ЧАСТОТА	ОЗУ	ДИСК	CPU	ЧАСТОТА
Windows 7	1 ГБ	20 ГБ	1	1 ГГЦ	2 ГБ	32 ГБ	2	1 ГГЦ
Windows XP	256 МБ	10 ГБ	1	233 МГЦ	512 МБ	20 ГБ	2	300 МГЦ
Windows 10	2 ГБ	32 ГБ	2	2 ГГЦ	4 ГБ	64 ГБ	4	2 ГГЦ
Windows 8	2 ГБ	20 ГБ	2	1 ГГЦ	4 ГБ	64 ГБ	2	2 ГГЦ
Windows 11	4 ГБ	64 ГБ	2	2 ГГЦ	8 ГБ	128 ГБ	4	2.5 ГГЦ
Windows Server 2003	128 МБ	1.25 ГБ	1	133 МГЦ	256 МБ	2 ГБ	1	550 МГЦ
Windows Server 2025	2 ГБ	32 ГБ	1	1.4 ГГЦ	4 ГБ	64 ГБ	2	2 ГГЦ

3. Выбрать один из двух вариантов запуска **PT Responder (PT Dumper)**:
   - Запуск через контекстное меню (пример запуска через контекстное меню можно посмотреть **по ссылке**):
     - Нажать на исполняемый файл правой кнопкой мыши;
     - Выбрать "Запуск от имени администратора";
   - Запуск через консоль (пример запуска через консоль можно посмотреть **по ссылке**):
     - Запустить консоль с **правами локального администратора**;
     - Запустить исполняемый файл, введя его полный путь в консоли: `<путь_к_каталогу_с_исполняемым_файлом>\pt-dumper.abcdefg.win64.legacy.exe`;
     - Нажать `Enter`.
4. После запуска в консоли Windows начнётся вывод сообщений, информирующих о старте выполнения утилиты, как показано на изображении:



5. Необходимо дождаться завершения выполнения утилиты. О завершении будет свидетельствовать появление сообщения **"Data collection successfully completed."**, как показано на изображении (отмечено зелёным цветом):

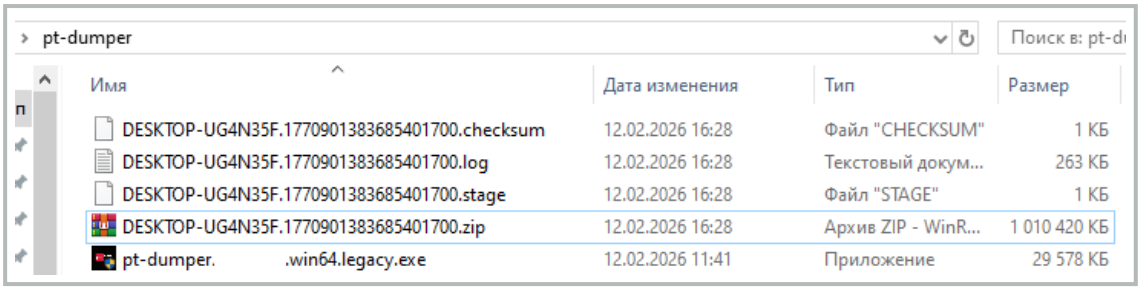


6. В результате работы утилиты формируются:

- архив с собранными данными (`.zip`) с именем в формате `<HOST>.<временная_метка_в_формате_Unix_TimeStamp>.zip` ,
- файл журнала работы утилиты **PT Responder (PT Dumper)** (`.log`),
- файл с контрольной суммой SHA256 результирующего архива (`.checksum`),
- файл с прогрессом выполнения модулей (`.stage`) **PT Responder (PT Dumper)** в следующем формате:

```
{
"TimeLine":"XXXX-XX-XXTXX:XX:XX.XXXXXXZ",
"Name":"<name_module>",
"Stage":"58/58"
}
```

7. Упомянутые файлы сохраняются в директорию, содержащую исполняемый файл **PT Responder (PT Dumper)**, как показано на изображении:



Четыре файла необходимо передать сотрудникам **PT ESC** по отдельности; упаковка этих файлов в дополнительный архив **не требуется**. Если необходимо передать более 5 архивов с данными, перед отправкой их следует упаковать **в один общий архив с именем, содержащим только латинские буквы**. Для передачи рекомендуется использовать утилиту **pt-cloud** (клиент предоставляется сотрудниками **PT ESC**).

8. Если в процессе работы утилиты возникают ошибки, необходимо определить их суть, используя справочную таблицу. Таблица содержит описание возможных ошибок и способы их устранения. При невозможности самостоятельного решения следует обратиться к сотрудникам **PT ESC**, приложив скриншот окна консоли с сообщением об ошибке

ПРОБЛЕМА	РЕШЕНИЕ
PT Responder (PT Dumper) неожиданно завершает работу, окно консоли автоматически закрывается	1. Запустить консоль с правами локального администратора; 2. Запустить исполняемый файл, введя его полный путь в консоли: `<путь_к_каталогу_с_исполняемым_файлом>/pt-dumper.abcdefg.win64.legacy.exe` ; 3. Нажать `Enter` ; 4. Сделать скриншот окна или скопировать текст из консоли с сообщением об ошибке. Обратиться к сотрудникам **PT ESC** для решения проблемы.
Архив с данными не создается	Убедитесь, что используется корректный исполняемый файл, соответствующий вашей разрядности архитектуры системы (x86 или x64). При обнаружении несоответствия выполнение утилиты будет прервано, а в лог-файл будет записано соответствующее сообщение об ошибке.

3. Unix

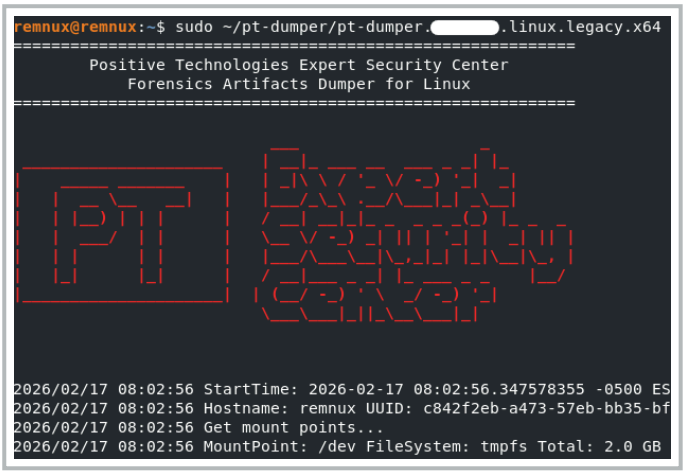
1. В зависимости от архитектуры необходимо выбрать один из следующих исполняемых файлов (в качестве примера будет приведена ОС Linux):
   - `pt-dumper.abcdefg.linux.legacy.x64` – пример исполняемого файла для 64-разрядной версии ОС Linux;
   - `pt-dumper.abcdefg.linux.legacy.x86` – пример исполняемого файла для 32-разрядной версии ОС Linux (данный исполняемый файл возможно запустить и на 64-разрядной версии ОС Linux);
2. Убедитесь, что хост, на котором будет запускаться утилита, удовлетворяет **следующим требованиям**.

PT DUMPER ДЛЯ UNIX								
ОС	МИНИМАЛЬНЫЕ				РЕКОМЕНДУЕМЫЕ			
	ОЗУ	ДИСК	CPU	ЧАСТОТА	ОЗУ	ДИСК	CPU	ЧАСТОТА
MacOS High Sierra 10.13	2 ГБ	32 ГБ	2	2 ГГЦ	4 ГБ	64 ГБ	2	2.2 ГГЦ
MacOS Taho 26	8 ГБ	64 ГБ	8	3.2 ГГЦ	16 ГБ	128 ГБ	8	3.2 ГГЦ
Ubuntu 14	1 ГБ	10 ГБ	1	700 МГЦ	2 ГБ	20 ГБ	2	2 ГГЦ
Ubuntu 24	4 ГБ	32 ГБ	2	2 ГГЦ	8 ГБ	64 ГБ	4	2.5 ГГЦ
Debian 8	256 МБ	16 ГБ	1	1 ГГЦ	512 МБ	32 ГБ	2	1 ГГЦ
Debian 12	512 МБ	16 ГБ	1	1 ГГЦ	1 ГБ	32 ГБ	2	1 ГГЦ
Fedora 21	1 ГБ	16 ГБ	1	1 ГГЦ	2 ГБ	32 ГБ	2	2 ГГЦ
Fedora 43	2 ГБ	32 ГБ	2	2 ГГЦ	4 ГБ	64 ГБ	4	2 ГГЦ
CentOS 6	1 ГБ	10 ГБ	1	1 ГГЦ	2 ГБ	20 ГБ	2	2 ГГЦ
CentOS Stream 10	1 ГБ	10 ГБ	1	2 ГГЦ	4 ГБ	20 ГБ	2	2 ГГЦ
Astra Linux	1 ГБ	4 ГБ	1	1 ГГЦ	4 ГБ	16 ГБ	2	2 ГГЦ
Red Hat Enterprise Linux 6	1 ГБ	10 ГБ	1	700 МГЦ	2 ГБ	20 ГБ	2	2 ГГЦ
Red Hat Enterprise Linux 9	2 ГБ	32 ГБ	2	2 ГГЦ	4 ГБ	64 ГБ	4	2 ГГЦ
Oracle Linux 6	1 ГБ	10 ГБ	1	700 МГЦ	2 ГБ	20 ГБ	2	2 ГГЦ
Oracle Linux 8	2 ГБ	32 ГБ	2	2 ГГЦ	4 ГБ	64 ГБ	4	2 ГГЦ

   Формирование архива с данными может быть прекращено досрочно в случае, если уже собранный объём достигнет предельного значения `sizeLimitDump`, заданного в конфигурационном файле (по умолчанию – 25 ГБ).
3. Открыть терминал;
4. Необходимо файл утилиты сделать исполняемым с помощью команды: `chmod +x /<путь_к_каталогу_с_исполняемым_файлом>/pt-dumper.abcdefg.linux.legacy.x64`.

```
remnux@remnux:~$ chmod +x ~/pt-dumper/pt-dumper.[redacted].linux.legacy.x64
```

5. Запустить исполняемый файл с **правами суперпользователя root** с помощью команды: `sudo /<путь_к_каталогу_с_исполняемым_файлом>/pt-dumper.abcdefg.linux.legacy.x64` (пример запуска можно посмотреть по ссылке).
6. После запуска в терминале начнётся вывод сообщений, информирующих о старте выполнения утилиты, как показано на изображении:

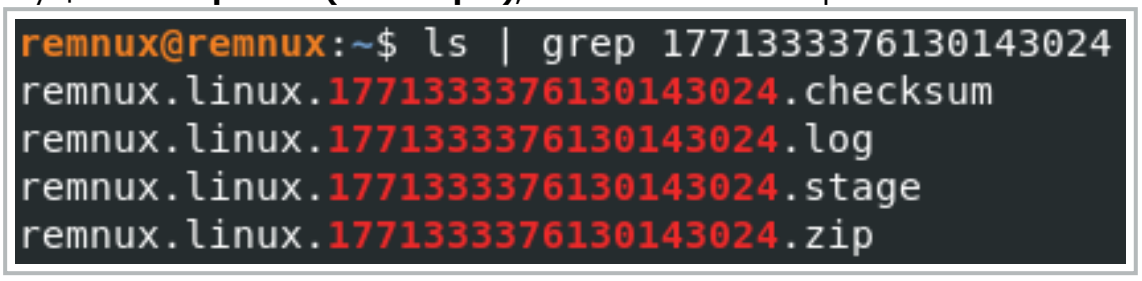


7. Необходимо дождаться завершения выполнения утилиты. О завершении будет свидетельствовать появление сообщения **"Collection completed"**, как показано на изображении (отмечено зелёным цветом):

8. В результате работы утилиты формируются:
   - архив с собранными данными (`.zip`) с именем в формате `<HOST>.linux.<временная_метка_в_формате_Unix_TimeStamp>.zip` ,
   - файл журнала работы утилиты **PT Responder (PT Dumper)** (`.log`),
   - файл с контрольной суммой SHA256 результирующего архива (`.checksum`),
   - файл с прогрессом выполнения модулей (`.stage`) **PT Responder (PT Dumper)** в следующем формате:

```
{
"TimeLine":"XXXX-XX-XXTXX:XX:XX.XXXXXXZ",
"Name":"<name_module>",
"Stage":"15/15"
}
```

9. Упомянутые файлы сохраняются в текущую директорию терминала, из которой был запущен **PT Responder (PT Dumper)**, как показано на изображении:



Четыре файла необходимо передать сотрудникам **PT ESC** по отдельности; упаковка этих файлов в дополнительный архив **не требуется**. Если необходимо передать более 5 архивов с данными, перед отправкой их следует упаковать **в один общий архив с именем, содержащим только латинские буквы**. Для передачи рекомендуется использовать утилиту **pt-cloud** (клиент предоставляется сотрудниками **PT ESC**).

10. Если в процессе работы утилиты возникают ошибки, необходимо определить их суть, используя справочную таблицу. Таблица содержит описание возможных ошибок и способы их устранения. При невозможности самостоятельного решения следует обратиться к сотрудникам **PT ESC**, приложив скриншот окна терминала с сообщением об ошибке

ПРОБЛЕМА	РЕШЕНИЕ
Долгая работа **PT Responder (PT Dumper)** при локальном запуске	Сначала необходимо остановить выполнение утилиты и сделать скриншот окна терминала (или скопировать текст из терминала). Далее возможны два варианта решения проблемы:

ПРОБЛЕМА	РЕШЕНИЕ
	1.1 Отправить сотрудникам **PT ESC** сделанный скриншот или текст из терминала; 1.2 Выгрузить на диск конфигурационный файл режима `local` с помощью ключа `-dropconfig=local`; 1.3 Отправить его сотрудникам **PT ESC** для редактирования и исключения файловых путей; 1.4 Запустить **PT Responder (PT Dumper)** с новым конфигурационным файлом, полученным от сотрудников **PT ESC**; 2. Запустить **PT Responder (PT Dumper)** с ключом `-exceptpath`, где после знака "=" через запятую перечислить пути для исключения из сканирования (например, `-exceptpath="/home,/var"`).
Долгая работа **PT Responder (PT Dumper)** при локальном запуске	Запустить стабильную версию запущенного ранее режима с помощью ключа `-mode=localstable`. Если указанное решение не помогло, то необходимо выгрузить на диск конфигурационный файл режима `local` с помощью ключа `-dropconfig=local` и отправить его сотрудникам **PT ESC** для редактирования.
Модуль **PT Responder (PT Dumper)** отрабатывает с ошибкой при локальном запуске	Необходимо отправить сотрудникам **PT ESC** информацию об ошибке (скриншот или текст из терминала) для дальнейшего устранения.
Архив с данными не создается	Убедитесь, что используется корректный исполняемый файл, соответствующий разрядности архитектуры системы (x86 или x64). При несоответствии утилита не запустится.

4. Запуск PT Responder (PT Dumper) для Linux в качестве сервиса

1. Необходимо файл утилиты сделать исполняемым с помощью команды: `chmod +x /<путь_к_каталогу_с_исполняемым_файлом>/pt-dumper.abcdefg.linux.legacy.x64`.

```
remnux@remnux:~$ chmod +x ~/pt-dumper/pt-dumper.[redacted].linux.legacy.x64
```

2. Создать файл `pt-dumper.service` в каталоге с исполняемым файлом утилиты одним из предложенных способов:
   - воспользоваться ключом утилиты `-dropservice`, запустив следующую команду: `/<путь_к_каталогу_с_исполняемым_файлом>/pt-dumper.abcdefg.linux.legacy.x64 -dropservice`, который выгрузит файл сервиса на диск рядом с исполняемым файлом утилиты;
   - создать вручную и поместить туда следующий текст:

```
[Unit]
Description=PT Responder (PT Dumper), collecting data for PT

[Service]
Type=oneshot
ExecStart=/<путь_к_каталогу_с_исполняемым_файлом>/pt-
dumper.abcdefg.linux.legacy.x64 -outpath="/<output_path>"
MemoryLimit=2048M
CPUQuota=50%
OOMScoreAdjust=-1000

[Install]
WantedBy=multi-user.target
```

Примечание: Параметры, выделенные красным, нужно заменить на свои значения, а именно:

- `/<путь_к_каталогу_с_исполняемым_файлом>/pt-dumper.abcdefg.linux.legacy.x64` – путь к исполняемому файлу **PT Responder (PT Dumper)**,
- `/<output_path>` – директория для записи результатов.

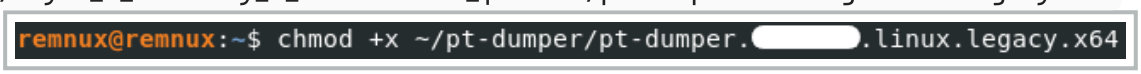
3. Запустить исполняемый файл с **правами суперпользователя root** с помощью команды: `sudo /<путь_к_каталогу_с_исполняемым_файлом>/pt-dumper.abcdefg.linux.legacy.x64`. После запуска файл `pt-dumper.service` будет автоматически перемещен в каталог `/etc/systemd/system`.
4. Проверить состояние работы сервиса можно с помощью команды: `/<путь_к_каталогу_с_исполняемым_файлом>/pt-dumper.abcdefg.linux.legacy.x64 -status-service`.

5. Запуск PT Responder (PT Dumper) для Unix с примонтированного раздела

Существует возможность запуска утилиты, не оставляя следов запуска на файловой системе исследуемого узла. При таком запуске данные, хранящиеся в оперативной памяти, не будут анализироваться при сборе дампа. В частности, будут отключены модули сбора сведений о системе (`systeminfo`), запущенных процессах (`process`), точках монтирования (`mount`), состоянии сетевых соединений (`netstat`), DNS-кэше (`dnscache`), а также проверка соблюдения рекомендаций по усилению защиты ОС на базе Linux (`recommendations`).

Для осуществления такого запуска следует выполнить следующие шаги:

1. Необходимо файл утилиты сделать исполняемым с помощью команды: `chmod +x /<путь_к_каталогу_с_исполняемым_файлом>/pt-dumper.abcdefg.linux.legacy.x64`.



2. **(Опционально)** Запустить узел и загрузить на нем другую операционную систему с использованием **Live CD**. Убедиться, что системный раздел примонтирован в режиме "только для чтения";
3. Запустить **PT Responder (PT Dumper)** с аргументами `root` и `outpath`, которые используются для указания логического диска, к которому примонтирован

системный раздел операционной системы исследуемого узла, и директории, в которую будут сохраняться результаты, соответственно:

```
/<путь_к_каталогу_с_исполняемым_файлом>/pt-dumper.abcdefg.linux.legacy.x64 -root="/mnt/mountpoint" -outpath="/mnt/<outpath_path>"
```

Примечание: При указании директории для записи результатов не следует указывать директорию, расположенную на файловой системе операционной системы, которая загружена с использованием **Live CD**.