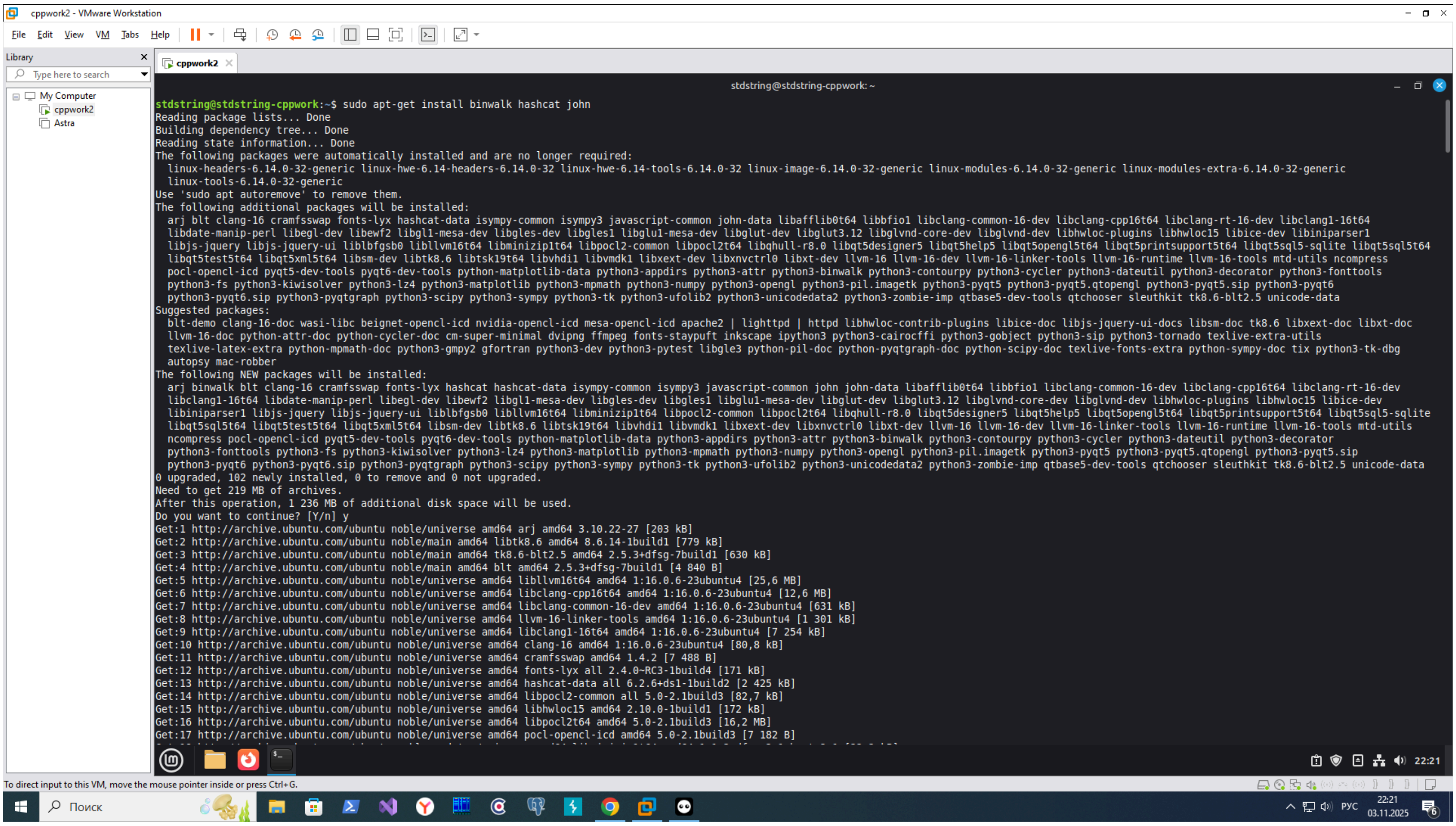
1. Введение.

Цель работы — научиться извлекать файловую систему из прошивки IP-камеры, анализировать ее содержимое и восстанавливать пароли с использованием утилит binwalk и hashcat.

2. Подготовка окружения и извлечение файловой системы.

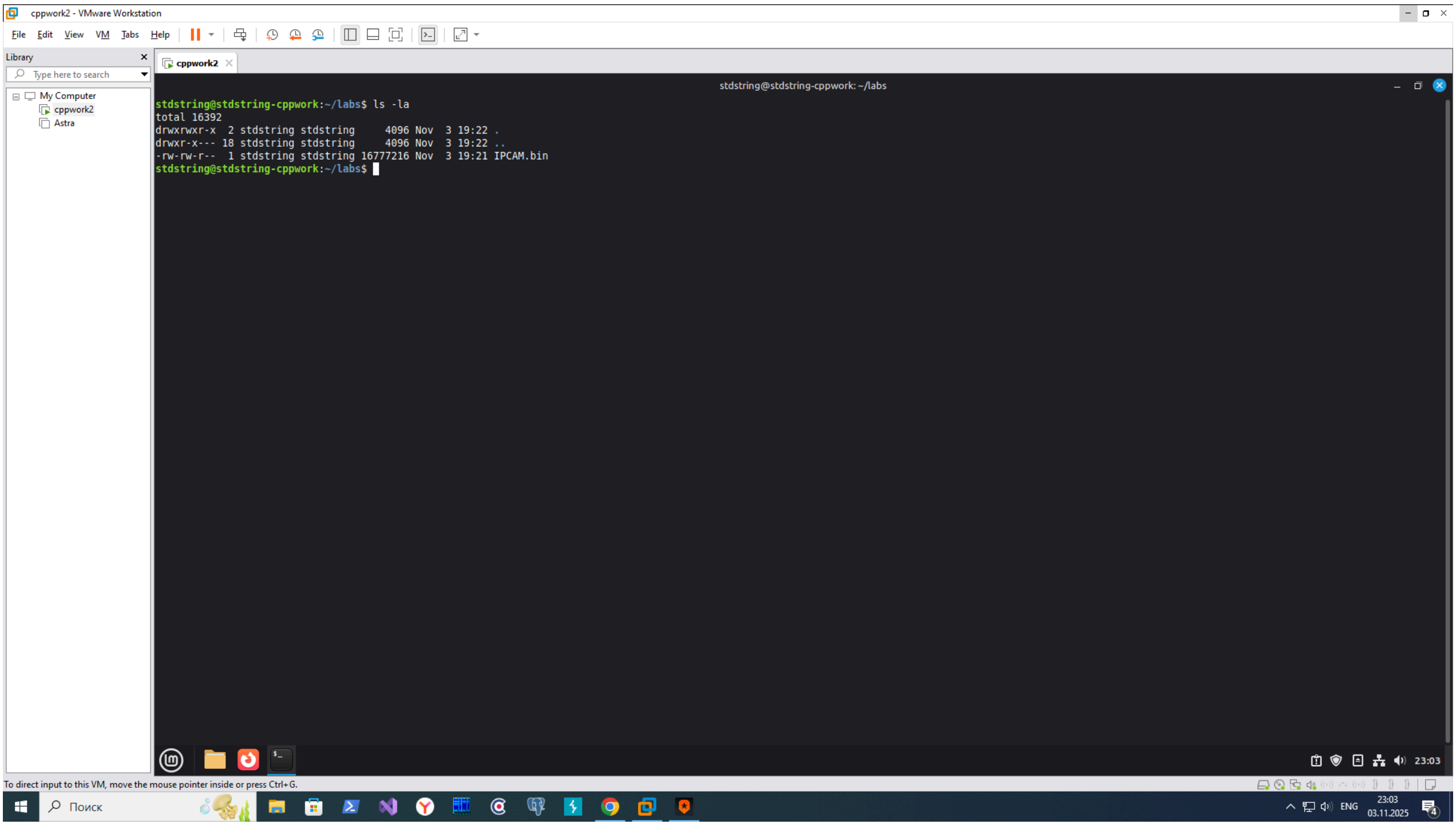
Устанавливаю утилиты binwalk, hashcat, John the Ripper:


cppwork2 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
cppwork2
Astra
cppwork2
stdstring@stdstring-cppwork: ~
22:21
Поиск
РУС
22:21
03.11.2025

```
stdstring@stdstring-cppwork:~$ sudo apt-get install binwalk hashcat john
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-6.14.0-32-generic linux-hwe-6.14-headers-6.14.0-32 linux-hwe-6.14-tools-6.14.0-32 linux-image-6.14.0-32-generic linux-modules-6.14.0-32-generic linux-modules-extra-6.14.0-32-generic
  linux-tools-6.14.0-32-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  arj blt clang-16 cramfsswap fonts-lyx hashcat-data isympy-common isympy3 javascript-common john-data libafflib0t64 libbfio1 libclang-common-16-dev libclang-cpp16t64 libclang-rt-16-dev libclang1-16t64
  libdate-manip-perl libegl-dev libewf2 libgl1-mesa-dev libgles-dev libgles1 libglu1-mesa-dev libglut-dev libglut3.12 libglvnd-core-dev libglvnd-dev libhwloc-plugins libhwloc15 libice-dev libiniparser1
  libjs-jquery libjs-jquery-ui liblbfgsb0 libllvm16t64 libminizip1t64 libpocl2-common libpocl2t64 libqhull-r8.0 libqt5designer5 libqt5help5 libqt5opengl5t64 libqt5printsupport5t64 libqt5sql5-sqlite libqt5sql5t64
  libqt5test5t64 libqt5xml5t64 libsm-dev libtk8.6 libtsk19t64 libvhdi1 libvmdk1 libxext-dev libxnvctrl0 libxt-dev llvm-16 llvm-16-dev llvm-16-linker-tools llvm-16-runtime llvm-16-tools mtd-utils ncompress
  pocl-opencl-icd pyqt5-dev-tools pyqt6-dev-tools python-matplotlib-data python3-appdirs python3-attr python3-binwalk python3-contourpy python3-cycler python3-dateutil python3-decorator python3-fonttools
  python3-fs python3-kiwisolver python3-lz4 python3-matplotlib python3-mpmath python3-numpy python3-opengl python3-pil.imagetk python3-pyqt5 python3-pyqt5.qtopengl python3-pyqt5.sip python3-pyqt6
  python3-pyqt6.sip python3-pyqtgraph python3-scipy python3-sympy python3-tk python3-ufolib2 python3-unicodedata2 python3-zombie-imp qtbase5-dev-tools qtchooser sleuthkit tk8.6-blt2.5 unicode-data
Suggested packages:
  blt-demo clang-16-doc wasi-libc beignet-opencl-icd nvidia-opencl-icd mesa-opencl-icd apache2 | lighttpd | httpd libhwloc-contrib-plugins libice-doc libjs-jquery-ui-docs libsm-doc tk8.6 libxext-doc libxt-doc
  llvm-16-doc python-attr-doc python-cycler-doc cm-super-minimal dvipng ffmpeg fonts-staypuft inkscape ipython3 python3-cairocffi python3-gobject python3-sip python3-tornado texlive-extra-utils
  texlive-latex-extra python-mpmath-doc python3-gmpy2 gfortran python3-dev python3-pytest libgle3 python-pil-doc python-pyqtgraph-doc python-scipy-doc texlive-fonts-extra python-sympy-doc tix python3-tk-dbg
  autopsy mac-robber
The following NEW packages will be installed:
  arj binwalk blt clang-16 cramfsswap fonts-lyx hashcat hashcat-data isympy-common isympy3 javascript-common john john-data libafflib0t64 libbfio1 libclang-common-16-dev libclang-cpp16t64 libclang-rt-16-dev
  libclang1-16t64 libdate-manip-perl libegl-dev libewf2 libgl1-mesa-dev libgles-dev libgles1 libglu1-mesa-dev libglut-dev libglut3.12 libglvnd-core-dev libglvnd-dev libhwloc-plugins libhwloc15 libice-dev
  libiniparser1 libjs-jquery libjs-jquery-ui liblbfgsb0 libllvm16t64 libminizip1t64 libpocl2-common libpocl2t64 libqhull-r8.0 libqt5designer5 libqt5help5 libqt5opengl5t64 libqt5printsupport5t64 libqt5sql5-sqlite
  libqt5sql5t64 libqt5test5t64 libqt5xml5t64 libsm-dev libtk8.6 libtsk19t64 libvhdi1 libvmdk1 libxext-dev libxnvctrl0 libxt-dev llvm-16 llvm-16-dev llvm-16-linker-tools llvm-16-runtime llvm-16-tools mtd-utils
  ncompress pocl-opencl-icd pyqt5-dev-tools pyqt6-dev-tools python-matplotlib-data python3-appdirs python3-attr python3-binwalk python3-contourpy python3-cycler python3-dateutil python3-decorator
  python3-fonttools python3-fs python3-kiwisolver python3-lz4 python3-matplotlib python3-mpmath python3-numpy python3-opengl python3-pil.imagetk python3-pyqt5 python3-pyqt5.qtopengl python3-pyqt5.sip
  python3-pyqt6 python3-pyqt6.sip python3-pyqtgraph python3-scipy python3-sympy python3-tk python3-ufolib2 python3-unicodedata2 python3-zombie-imp qtbase5-dev-tools qtchooser sleuthkit tk8.6-blt2.5 unicode-data
0 upgraded, 102 newly installed, 0 to remove and 0 not upgraded.
Need to get 219 MB of archives.
After this operation, 1 236 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu noble/universe amd64 arj amd64 3.10.22-27 [203 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble/main amd64 libtk8.6 amd64 8.6.14-1build1 [779 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble/main amd64 tk8.6-blt2.5 amd64 2.5.3+dfsg-7build1 [630 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble/main amd64 blt amd64 2.5.3+dfsg-7build1 [4 840 B]
Get:5 http://archive.ubuntu.com/ubuntu noble/universe amd64 libllvm16t64 amd64 1:16.0.6-23ubuntu4 [25,6 MB]
Get:6 http://archive.ubuntu.com/ubuntu noble/universe amd64 libclang-cpp16t64 amd64 1:16.0.6-23ubuntu4 [12,6 MB]
Get:7 http://archive.ubuntu.com/ubuntu noble/universe amd64 libclang-common-16-dev amd64 1:16.0.6-23ubuntu4 [631 kB]
Get:8 http://archive.ubuntu.com/ubuntu noble/universe amd64 llvm-16-linker-tools amd64 1:16.0.6-23ubuntu4 [1 301 kB]
Get:9 http://archive.ubuntu.com/ubuntu noble/universe amd64 libclang1-16t64 amd64 1:16.0.6-23ubuntu4 [7 254 kB]
Get:10 http://archive.ubuntu.com/ubuntu noble/universe amd64 clang-16 amd64 1:16.0.6-23ubuntu4 [80,8 kB]
Get:11 http://archive.ubuntu.com/ubuntu noble/universe amd64 cramfsswap amd64 1.4.2 [7 488 B]
Get:12 http://archive.ubuntu.com/ubuntu noble/universe amd64 fonts-lyx all 2.4.0~RC3-1build4 [171 kB]
Get:13 http://archive.ubuntu.com/ubuntu noble/universe amd64 hashcat-data all 6.2.6+ds1-1build2 [2 425 kB]
Get:14 http://archive.ubuntu.com/ubuntu noble/universe amd64 libpocl2-common all 5.0-2.1build3 [82,7 kB]
Get:15 http://archive.ubuntu.com/ubuntu noble/universe amd64 libhwloc15 amd64 2.10.0-1build1 [172 kB]
Get:16 http://archive.ubuntu.com/ubuntu noble/universe amd64 libpocl2t64 amd64 5.0-2.1build3 [16,2 MB]
Get:17 http://archive.ubuntu.com/ubuntu noble/universe amd64 pocl-opencl-icd amd64 5.0-2.1build3 [7 182 B]
```

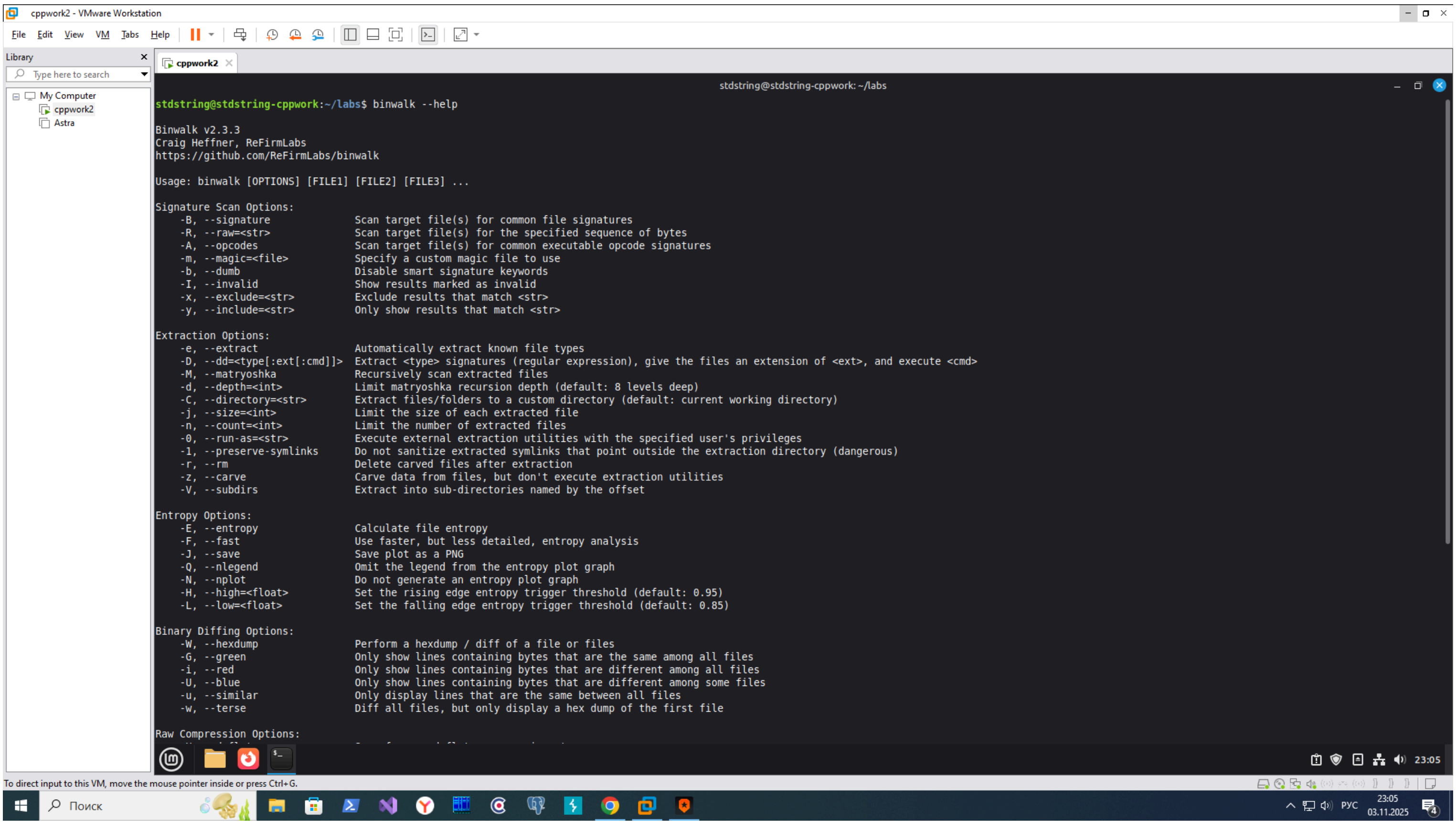
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Проверяю, что в текущем каталоге расположен образ прошивки:



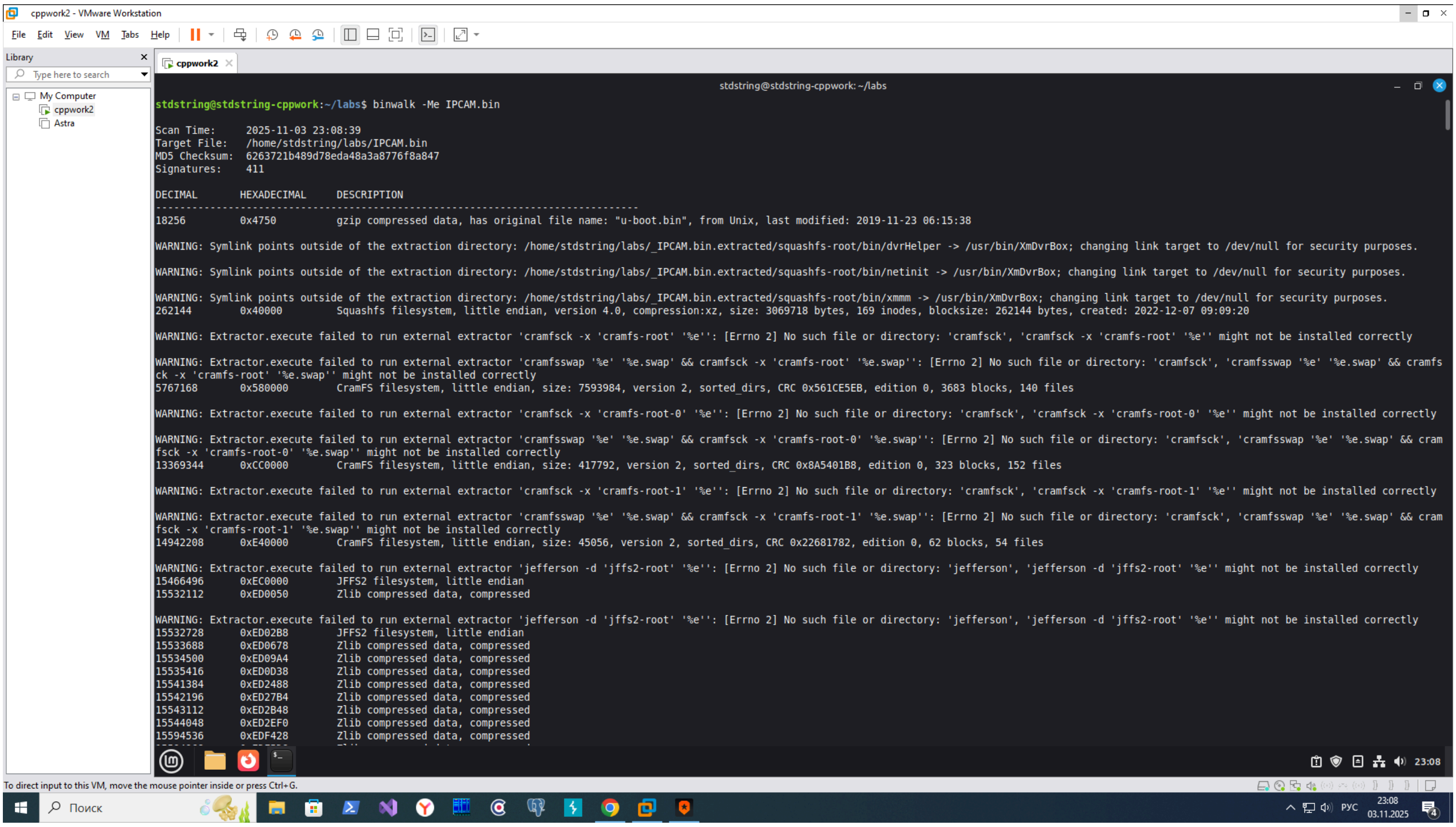
```
stdstring@stdstring-cppwork:~/labs$ ls -la
total 16392
drwxrwxr-x  2 stdstring stdstring     4096 Nov  3 19:22 .
drwxr-x--- 18 stdstring stdstring     4096 Nov  3 19:22 ..
-rw-rw-r--  1 stdstring stdstring 16777216 Nov  3 19:21 IPCAM.bin
stdstring@stdstring-cppwork:~/labs$ 
```

Изучаю помощь для утилиты binwalk:

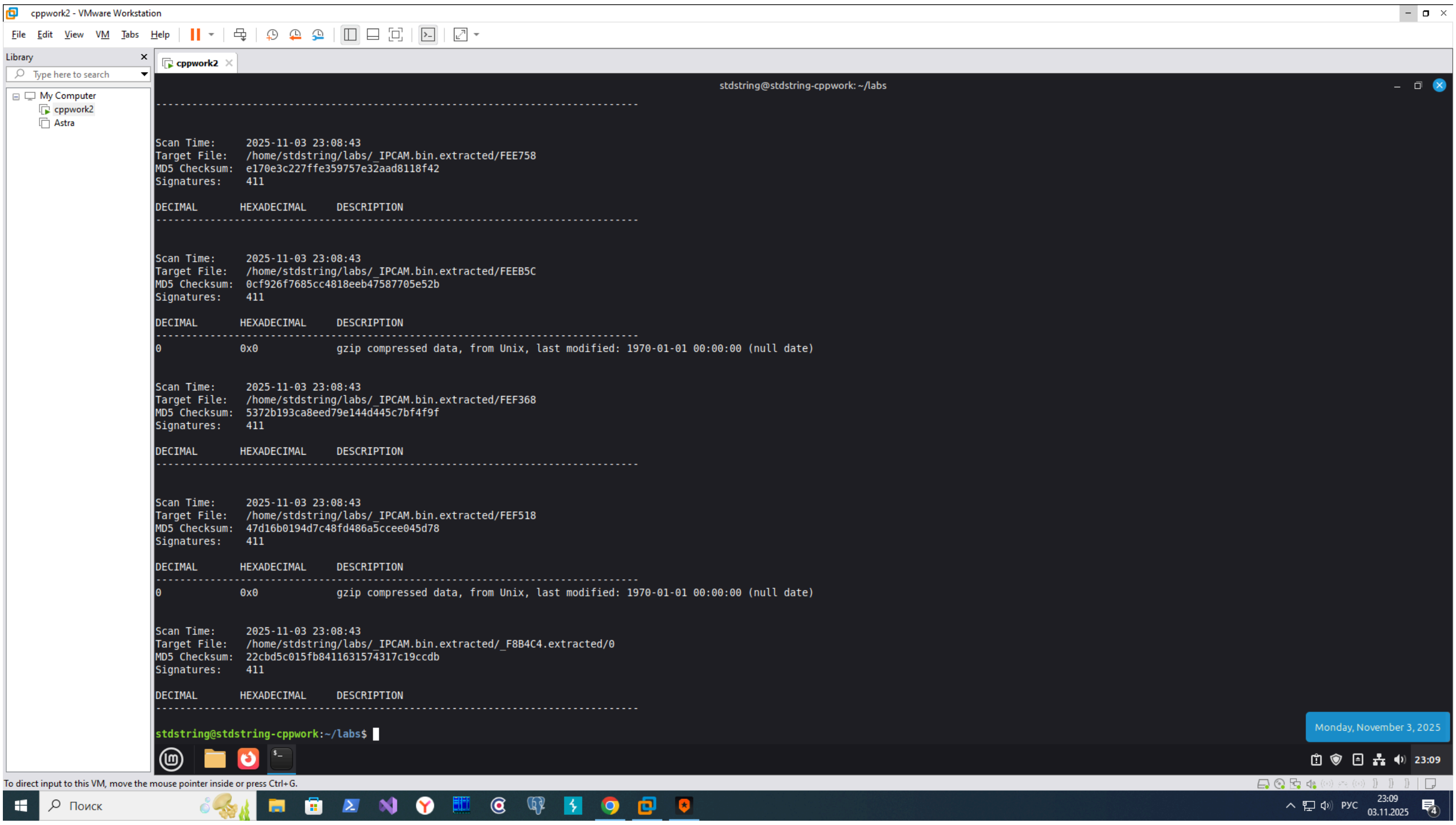


```
stdstring@stdstring-cppwork:~/labs$ binwalk --help

Binwalk v2.3.3
Craig Heffner, ReFirmLabs
https://github.com/ReFirmLabs/binwalk

Usage: binwalk [OPTIONS] [FILE1] [FILE2] [FILE3] ...

Signature Scan Options:
    -B, --signature             Scan target file(s) for common file signatures
    -R, --raw=<str>             Scan target file(s) for the specified sequence of bytes
    -A, --opcodes               Scan target file(s) for common executable opcode signatures
    -m, --magic=<file>          Specify a custom magic file to use
    -b, --dumb                  Disable smart signature keywords
    -I, --invalid               Show results marked as invalid
    -x, --exclude=<str>         Exclude results that match <str>
    -y, --include=<str>         Only show results that match <str>

Extraction Options:
    -e, --extract               Automatically extract known file types
    -D, --dd=<type[:ext[:cmd]]> Extract <type> signatures (regular expression), give the files an extension of <ext>, and execute <cmd>
    -M, --matryoshka            Recursively scan extracted files
    -d, --depth=<int>           Limit matryoshka recursion depth (default: 8 levels deep)
    -C, --directory=<str>       Extract files/folders to a custom directory (default: current working directory)
    -j, --size=<int>            Limit the size of each extracted file
    -n, --count=<int>           Limit the number of extracted files
    -0, --run-as=<str>          Execute external extraction utilities with the specified user's privileges
    -1, --preserve-symlinks     Do not sanitize extracted symlinks that point outside the extraction directory (dangerous)
    -r, --rm                    Delete carved files after extraction
    -z, --carve                 Carve data from files, but don't execute extraction utilities
    -V, --subdirs               Extract into sub-directories named by the offset

Entropy Options:
    -E, --entropy               Calculate file entropy
    -F, --fast                  Use faster, but less detailed, entropy analysis
    -J, --save                  Save plot as a PNG
    -Q, --nlegend               Omit the legend from the entropy plot graph
    -N, --nplot                 Do not generate an entropy plot graph
    -H, --high=<float>          Set the rising edge entropy trigger threshold (default: 0.95)
    -L, --low=<float>           Set the falling edge entropy trigger threshold (default: 0.85)

Binary Diffing Options:
    -W, --hexdump               Perform a hexdump / diff of a file or files
    -G, --green                 Only show lines containing bytes that are the same among all files
    -i, --red                   Only show lines containing bytes that are different among all files
    -U, --blue                  Only show lines containing bytes that are different among some files
    -u, --similar               Only display lines that are the same between all files
    -w, --terse                 Diff all files, but only display a hex dump of the first file

Raw Compression Options:
```

Использую утилиту binwalk для извлечения файловой системы из образа прошивки:


cppwork2 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
cppwork2
Astra
stdstring@stdstring-cppwork: ~/labs
23:08
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Поиск
РУС
23:08
03.11.2025

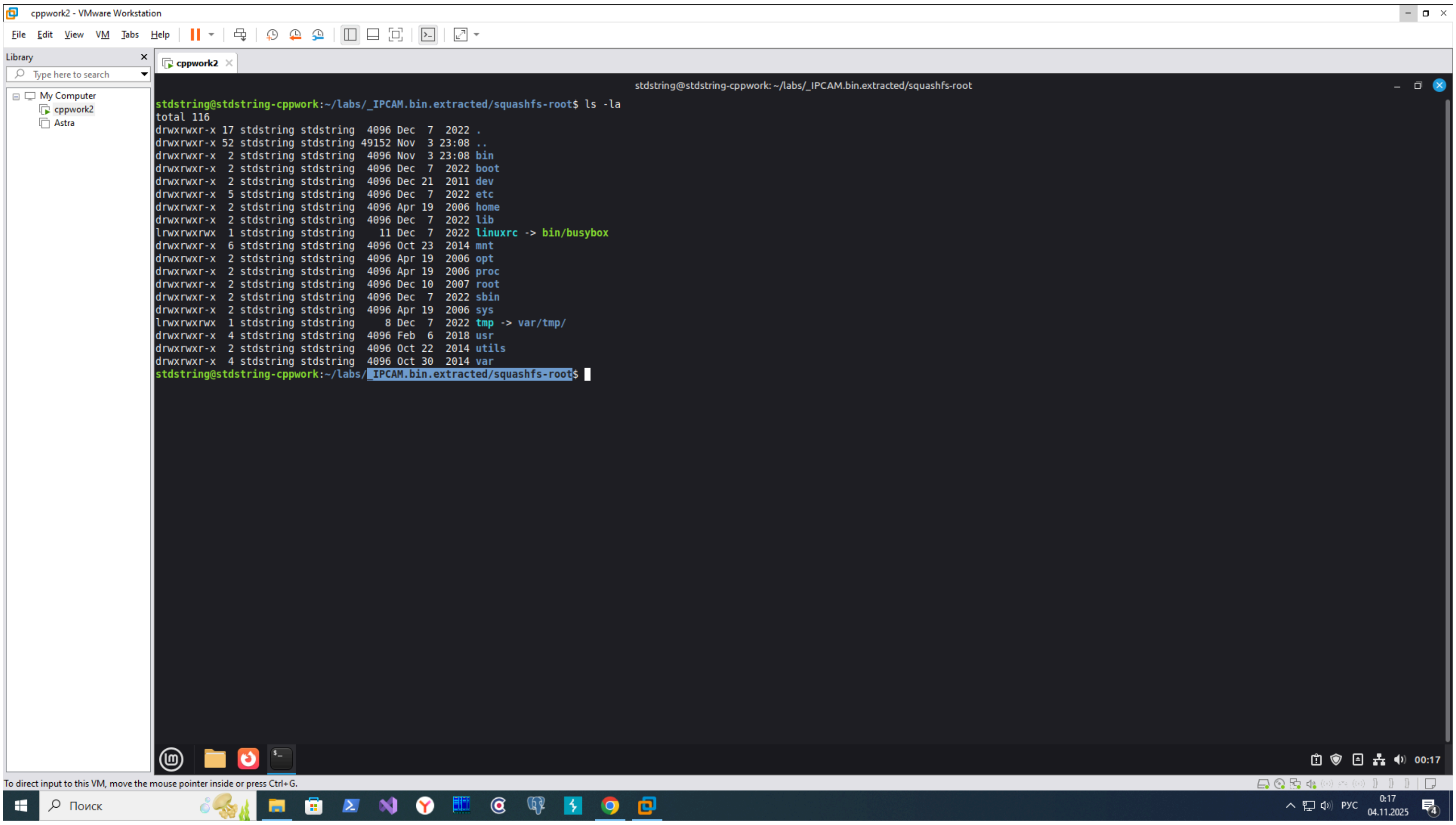
```
stdstring@stdstring-cppwork:~/labs$ binwalk -Me IPCAM.bin

Scan Time:     2025-11-03 23:08:39
Target File:   /home/stdstring/labs/IPCAM.bin
MD5 Checksum:  6263721b489d78eda48a3a8776f8a847
Signatures:    411

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
18256         0x4750          gzip compressed data, has original file name: "u-boot.bin", from Unix, last modified: 2019-11-23 06:15:38

WARNING: Symlink points outside of the extraction directory: /home/stdstring/labs/_IPCAM.bin.extracted/squashfs-root/bin/dvrHelper -> /usr/bin/XmDvrBox; changing link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /home/stdstring/labs/_IPCAM.bin.extracted/squashfs-root/bin/netinit -> /usr/bin/XmDvrBox; changing link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /home/stdstring/labs/_IPCAM.bin.extracted/squashfs-root/bin/xmmm -> /usr/bin/XmDvrBox; changing link target to /dev/null for security purposes.
262144        0x40000         Squashfs filesystem, little endian, version 4.0, compression:xz, size: 3069718 bytes, 169 inodes, blocksize: 262144 bytes, created: 2022-12-07 09:09:20

WARNING: Extractor.execute failed to run external extractor 'cramfsck -x 'cramfs-root' '%e'': [Errno 2] No such file or directory: 'cramfsck', 'cramfsck -x 'cramfs-root' '%e'' might not be installed correctly

WARNING: Extractor.execute failed to run external extractor 'cramfsswap '%e' '%e.swap' && cramfsck -x 'cramfs-root' '%e.swap'': [Errno 2] No such file or directory: 'cramfsck', 'cramfsswap '%e' '%e.swap' && cramfs
ck -x 'cramfs-root' '%e.swap'' might not be installed correctly
5767168       0x580000        CramFS filesystem, little endian, size: 7593984, version 2, sorted_dirs, CRC 0x561CE5EB, edition 0, 3683 blocks, 140 files

WARNING: Extractor.execute failed to run external extractor 'cramfsck -x 'cramfs-root-0' '%e'': [Errno 2] No such file or directory: 'cramfsck', 'cramfsck -x 'cramfs-root-0' '%e'' might not be installed correctly

WARNING: Extractor.execute failed to run external extractor 'cramfsswap '%e' '%e.swap' && cramfsck -x 'cramfs-root-0' '%e.swap'': [Errno 2] No such file or directory: 'cramfsck', 'cramfsswap '%e' '%e.swap' && cram
fsck -x 'cramfs-root-0' '%e.swap'' might not be installed correctly
13369344      0xCC0000        CramFS filesystem, little endian, size: 417792, version 2, sorted_dirs, CRC 0x8A5401B8, edition 0, 323 blocks, 152 files

WARNING: Extractor.execute failed to run external extractor 'cramfsck -x 'cramfs-root-1' '%e'': [Errno 2] No such file or directory: 'cramfsck', 'cramfsck -x 'cramfs-root-1' '%e'' might not be installed correctly

WARNING: Extractor.execute failed to run external extractor 'cramfsswap '%e' '%e.swap' && cramfsck -x 'cramfs-root-1' '%e.swap'': [Errno 2] No such file or directory: 'cramfsck', 'cramfsswap '%e' '%e.swap' && cram
fsck -x 'cramfs-root-1' '%e.swap'' might not be installed correctly
14942208      0xE40000        CramFS filesystem, little endian, size: 45056, version 2, sorted_dirs, CRC 0x22681782, edition 0, 62 blocks, 54 files

WARNING: Extractor.execute failed to run external extractor 'jefferson -d 'jffs2-root' '%e'': [Errno 2] No such file or directory: 'jefferson', 'jefferson -d 'jffs2-root' '%e'' might not be installed correctly
15466496      0xEC0000        JFFS2 filesystem, little endian
15532112      0xED0050        Zlib compressed data, compressed

WARNING: Extractor.execute failed to run external extractor 'jefferson -d 'jffs2-root' '%e'': [Errno 2] No such file or directory: 'jefferson', 'jefferson -d 'jffs2-root' '%e'' might not be installed correctly
15532728      0xED02B8        JFFS2 filesystem, little endian
15533688      0xED0678        Zlib compressed data, compressed
15534500      0xED09A4        Zlib compressed data, compressed
15535416      0xED0D38        Zlib compressed data, compressed
15541384      0xED2488        Zlib compressed data, compressed
15542196      0xED27B4        Zlib compressed data, compressed
15543112      0xED2B48        Zlib compressed data, compressed
15544048      0xED2EF0        Zlib compressed data, compressed
15594536      0xEDF428        Zlib compressed data, compressed
```


cppwork2 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
cppwork2
Astra
stdstring@stdstring-cppwork: ~/labs
Monday, November 3, 2025
23:09
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Поиск
РУС
23:09
03.11.2025

```
--------------------------------------------------------------------------------


Scan Time:     2025-11-03 23:08:43
Target File:   /home/stdstring/labs/_IPCAM.bin.extracted/FEE758
MD5 Checksum:  e170e3c227ffe359757e32aad8118f42
Signatures:    411

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------


Scan Time:     2025-11-03 23:08:43
Target File:   /home/stdstring/labs/_IPCAM.bin.extracted/FEEB5C
MD5 Checksum:  0cf926f7685cc4818eeb47587705e52b
Signatures:    411

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             gzip compressed data, from Unix, last modified: 1970-01-01 00:00:00 (null date)


Scan Time:     2025-11-03 23:08:43
Target File:   /home/stdstring/labs/_IPCAM.bin.extracted/FEF368
MD5 Checksum:  5372b193ca8eed79e144d445c7bf4f9f
Signatures:    411

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------


Scan Time:     2025-11-03 23:08:43
Target File:   /home/stdstring/labs/_IPCAM.bin.extracted/FEF518
MD5 Checksum:  47d16b0194d7c48fd486a5ccee045d78
Signatures:    411

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             gzip compressed data, from Unix, last modified: 1970-01-01 00:00:00 (null date)


Scan Time:     2025-11-03 23:08:43
Target File:   /home/stdstring/labs/_IPCAM.bin.extracted/_F8B4C4.extracted/0
MD5 Checksum:  22cbd5c015fb8411631574317c19ccdb
Signatures:    411

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------

stdstring@stdstring-cppwork:~/labs$ 
```

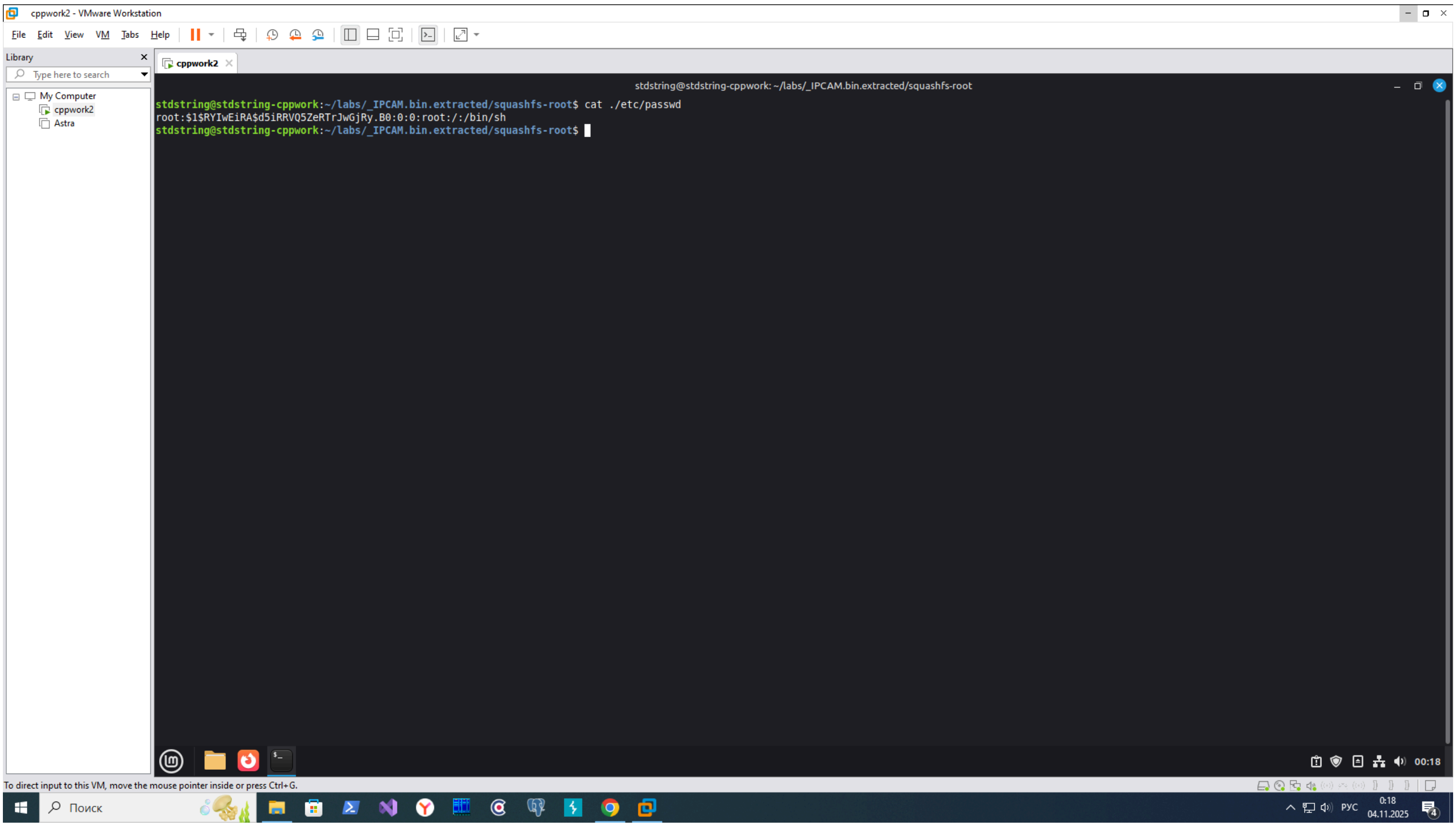
3, 4. Анализ содержимого файловой системы, восстановление паролей.

Перехожу в директорию _IPCAM.bin.extracted/squashfs-root. Вывожу ее содержимое:


cppwork2 - VMware Workstation
stdstring@stdstring-cppwork: ~/labs/_IPCAM.bin.extracted/squashfs-root
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
stdstring@stdstring-cppwork:~/labs/_IPCAM.bin.extracted/squashfs-root$ ls -la
total 116
drwxrwxr-x 17 stdstring stdstring  4096 Dec  7  2022 .
drwxrwxr-x 52 stdstring stdstring 49152 Nov  3 23:08 ..
drwxrwxr-x  2 stdstring stdstring  4096 Nov  3 23:08 bin
drwxrwxr-x  2 stdstring stdstring  4096 Dec  7  2022 boot
drwxrwxr-x  2 stdstring stdstring  4096 Dec 21  2011 dev
drwxrwxr-x  5 stdstring stdstring  4096 Dec  7  2022 etc
drwxrwxr-x  2 stdstring stdstring  4096 Apr 19  2006 home
drwxrwxr-x  2 stdstring stdstring  4096 Dec  7  2022 lib
lrwxrwxrwx  1 stdstring stdstring    11 Dec  7  2022 linuxrc -> bin/busybox
drwxrwxr-x  6 stdstring stdstring  4096 Oct 23  2014 mnt
drwxrwxr-x  2 stdstring stdstring  4096 Apr 19  2006 opt
drwxrwxr-x  2 stdstring stdstring  4096 Apr 19  2006 proc
drwxrwxr-x  2 stdstring stdstring  4096 Dec 10  2007 root
drwxrwxr-x  2 stdstring stdstring  4096 Dec  7  2022 sbin
drwxrwxr-x  2 stdstring stdstring  4096 Apr 19  2006 sys
lrwxrwxrwx  1 stdstring stdstring     8 Dec  7  2022 tmp -> var/tmp/
drwxrwxr-x  4 stdstring stdstring  4096 Feb  6  2018 usr
drwxrwxr-x  2 stdstring stdstring  4096 Oct 22  2014 utils
drwxrwxr-x  4 stdstring stdstring  4096 Oct 30  2014 var
stdstring@stdstring-cppwork:~/labs/_IPCAM.bin.extracted/squashfs-root$
```

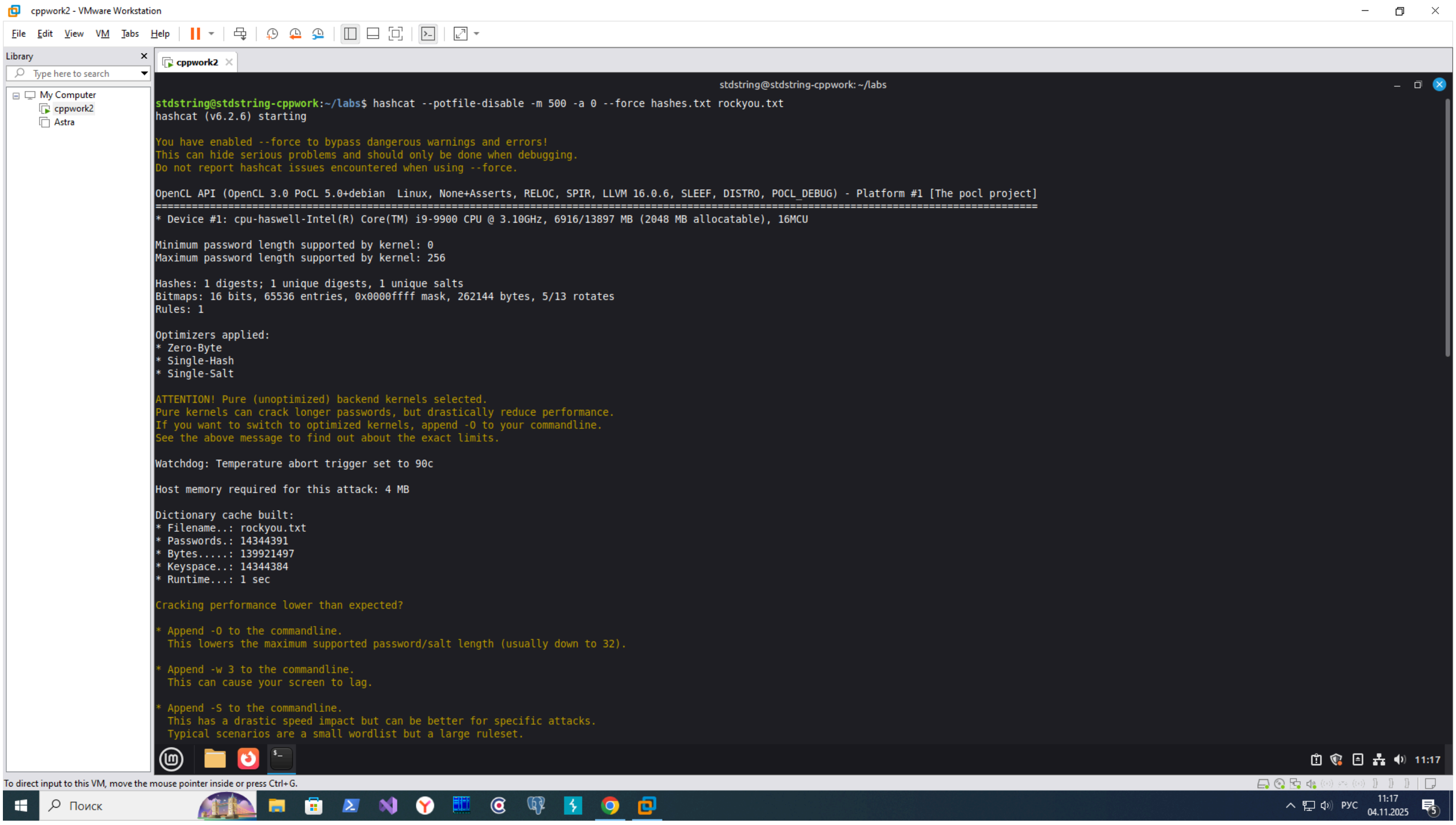
Вывожу содержимое файла ./etc/passwd:


cppwork2 - VMware Workstation
stdstring@stdstring-cppwork: ~/labs/_IPCAM.bin.extracted/squashfs-root
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

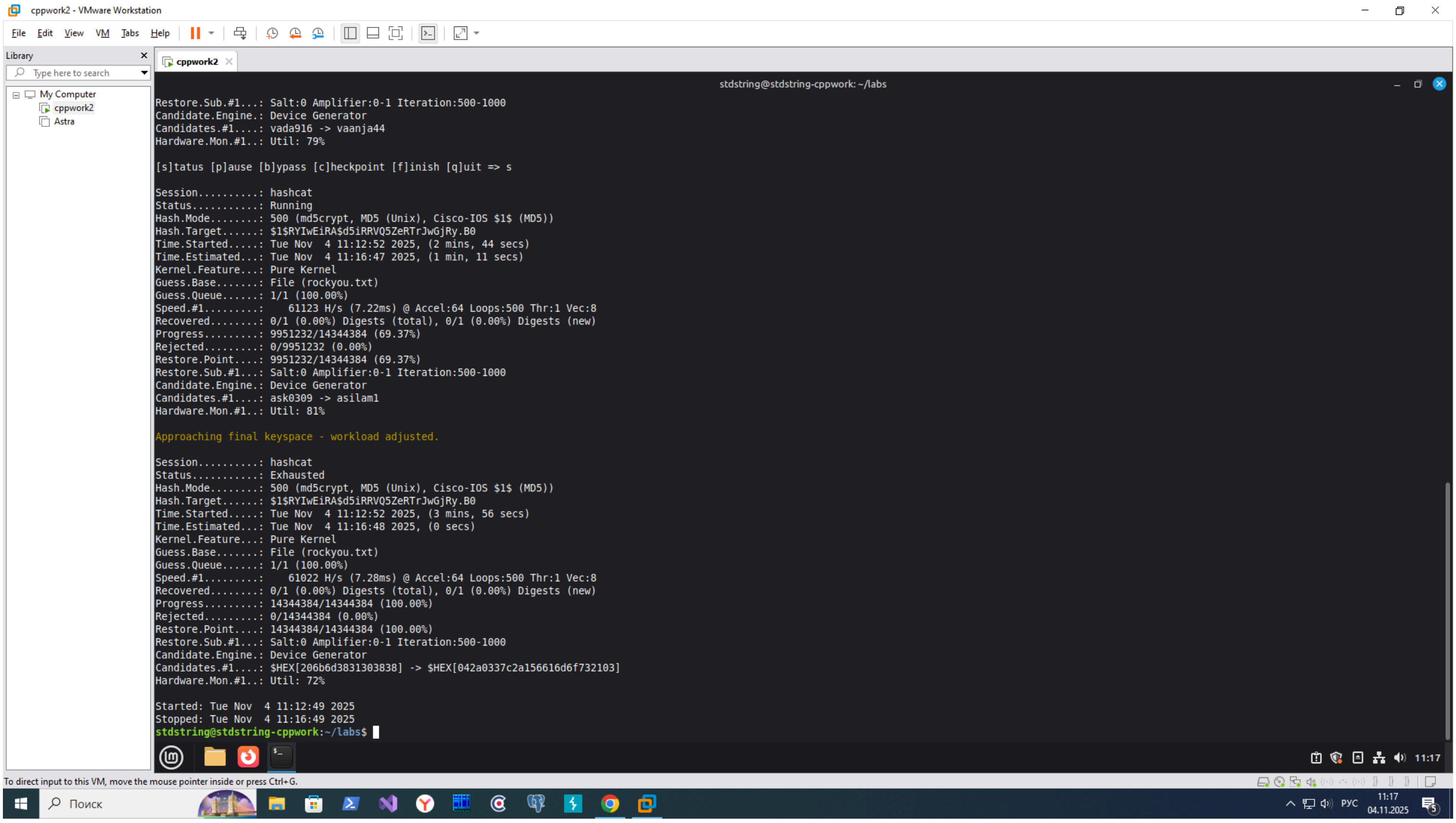
```
stdstring@stdstring-cppwork:~/labs/_IPCAM.bin.extracted/squashfs-root$ cat ./etc/passwd
root:$1$RYIwEiRA$d5iRRVQ5ZeRTrJwGjRy.B0:0:0:root:/:/bin/sh
stdstring@stdstring-cppwork:~/labs/_IPCAM.bin.extracted/squashfs-root$
```

Видно, что определен пользователь root, MD5 хеш пароля которого равен $1$RYIwEiRA$d5iRRVQ5ZeRTrJwGjRy.B0

Сохраняю MD5 хеш пароля в файл hashes.txt.
Попробую взломать его с помощью обычного словаря rockyou.
Запускаю hashcat:

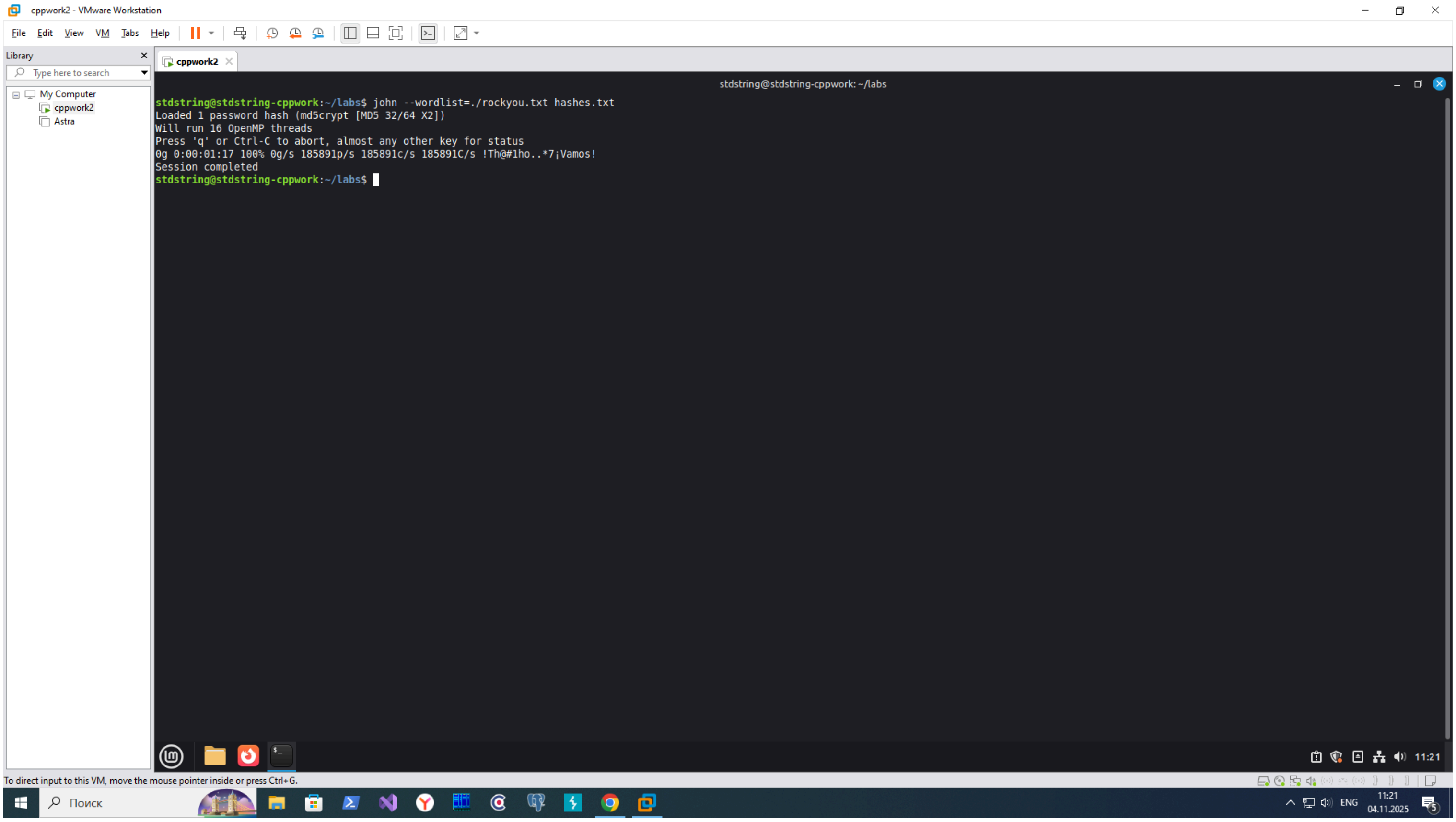

cppwork2 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
cppwork2
Astra
cppwork2
stdstring@stdstring-cppwork: ~/labs
11:17
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Поиск
РУС
11:17
04.11.2025

```
stdstring@stdstring-cppwork:~/labs$ hashcat --potfile-disable -m 500 -a 0 --force hashes.txt rockyou.txt
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==================================================================================================================================================
* Device #1: cpu-haswell-Intel(R) Core(TM) i9-9900 CPU @ 3.10GHz, 6916/13897 MB (2048 MB allocatable), 16MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 4 MB

Dictionary cache built:
* Filename..: rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 1 sec

Cracking performance lower than expected?

* Append -O to the commandline.
  This lowers the maximum supported password/salt length (usually down to 32).

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.
```


cppwork2 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
cppwork2
Astra
cppwork2
stdstring@stdstring-cppwork: ~/labs
11:17
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Поиск
РУС
11:17
04.11.2025

```
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:500-1000
Candidate.Engine.: Device Generator
Candidates.#1....: vada916 -> vaanja44
Hardware.Mon.#1..: Util: 79%

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit => s

Session..........: hashcat
Status...........: Running
Hash.Mode........: 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5))
Hash.Target......: $1$RYIwEiRA$d5iRRVQ5ZeRTrJwGjRy.B0
Time.Started.....: Tue Nov  4 11:12:52 2025, (2 mins, 44 secs)
Time.Estimated...: Tue Nov  4 11:16:47 2025, (1 min, 11 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    61123 H/s (7.22ms) @ Accel:64 Loops:500 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 9951232/14344384 (69.37%)
Rejected.........: 0/9951232 (0.00%)
Restore.Point....: 9951232/14344384 (69.37%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:500-1000
Candidate.Engine.: Device Generator
Candidates.#1....: ask0309 -> asilam1
Hardware.Mon.#1..: Util: 81%

Approaching final keyspace - workload adjusted.

Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5))
Hash.Target......: $1$RYIwEiRA$d5iRRVQ5ZeRTrJwGjRy.B0
Time.Started.....: Tue Nov  4 11:12:52 2025, (3 mins, 56 secs)
Time.Estimated...: Tue Nov  4 11:16:48 2025, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    61022 H/s (7.28ms) @ Accel:64 Loops:500 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 14344384/14344384 (100.00%)
Rejected.........: 0/14344384 (0.00%)
Restore.Point....: 14344384/14344384 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:500-1000
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b6d3831303838] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Util: 72%

Started: Tue Nov  4 11:12:49 2025
Stopped: Tue Nov  4 11:16:49 2025
stdstring@stdstring-cppwork:~/labs$
```

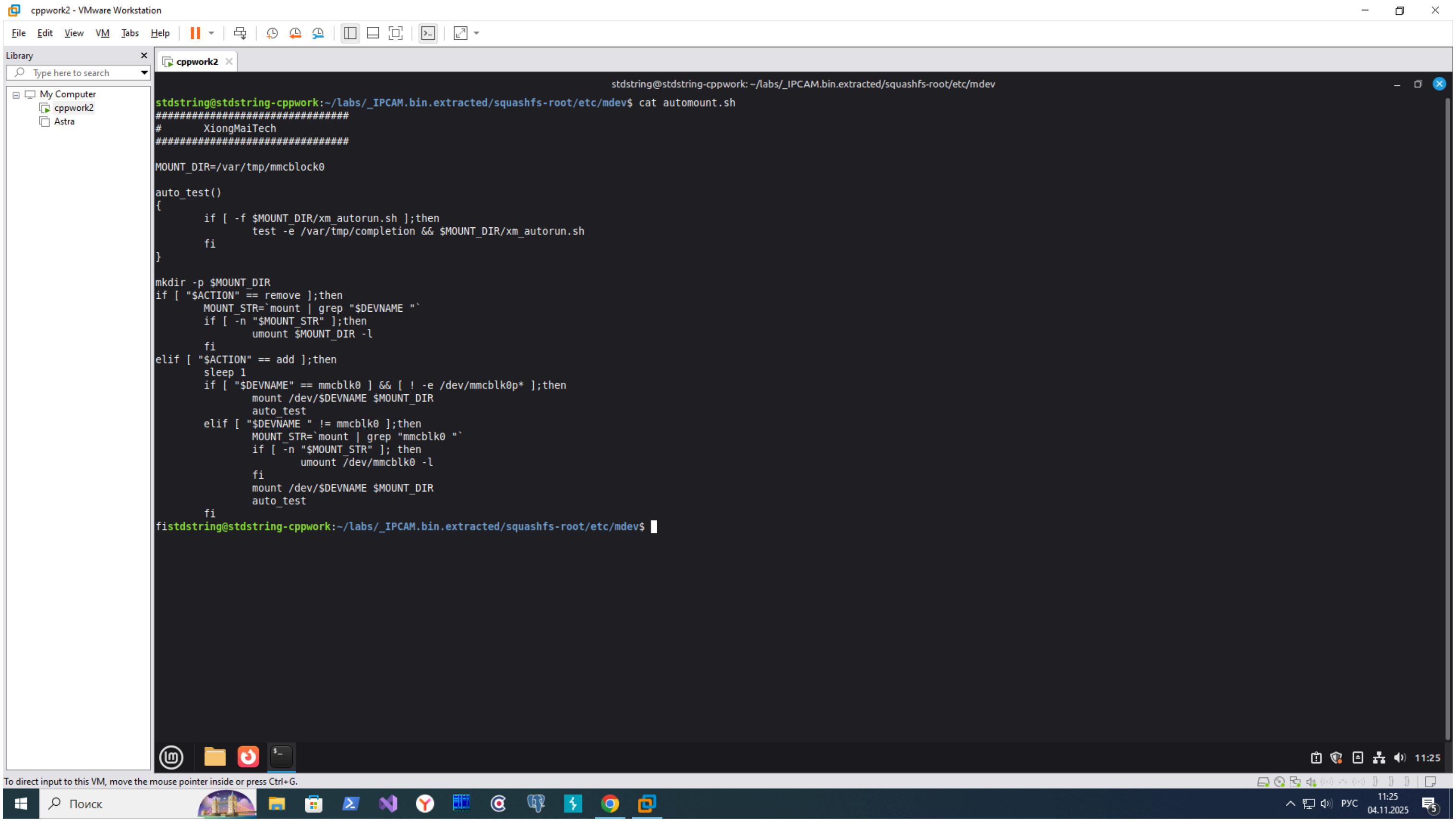
Видно, что результата нет - пароль мы взломать не смогли с помощью hashcat
Запускаю John the Ripper:



cppwork2 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
cppwork2
Astra
cppwork2
stdstring@stdstring-cppwork: ~/labs
11:21
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Поиск
ENG
11:21
04.11.2025

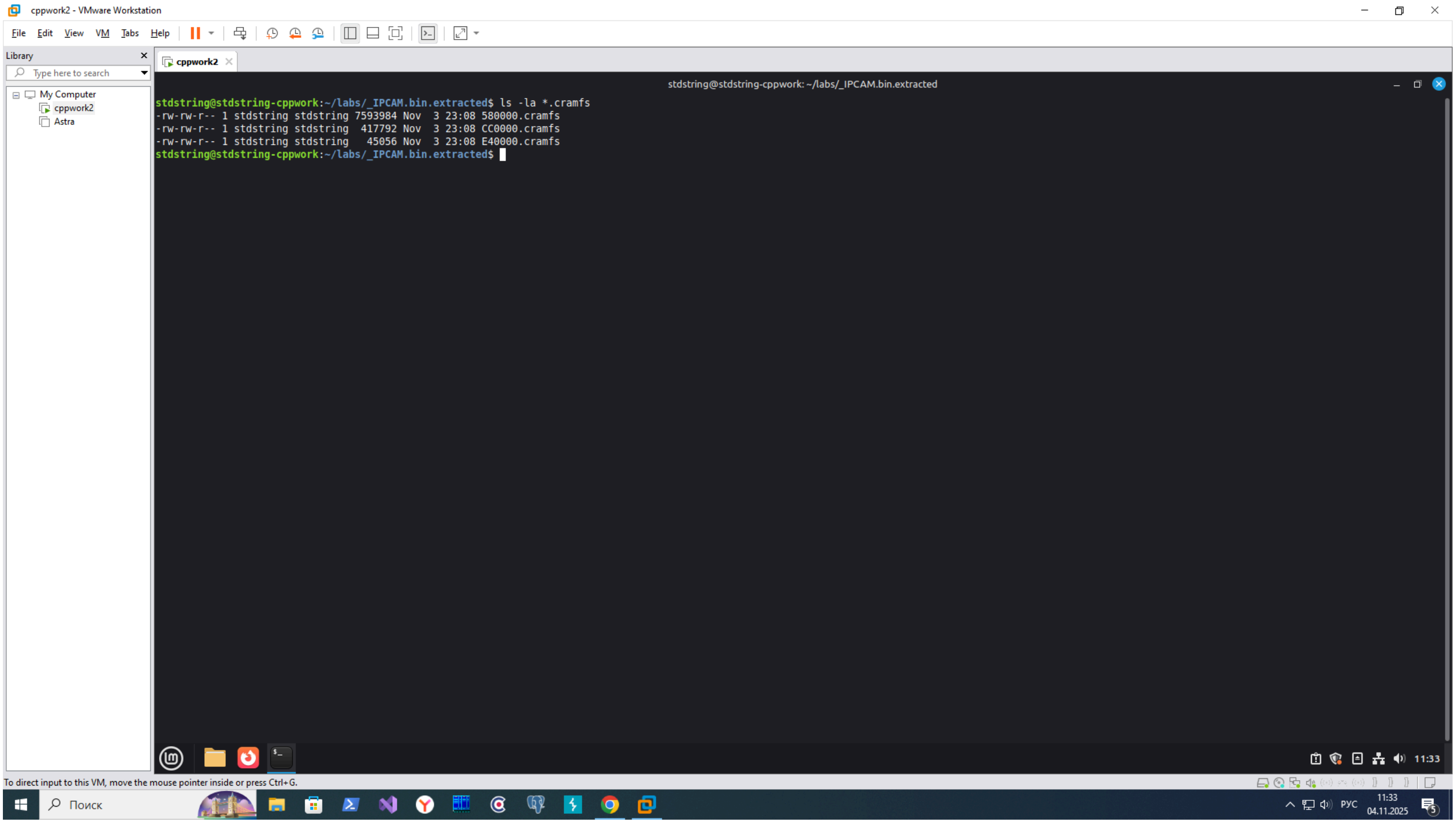
```
stdstring@stdstring-cppwork:~/labs$ john --wordlist=./rockyou.txt hashes.txt
Loaded 1 password hash (md5crypt [MD5 32/64 X2])
Will run 16 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:01:17 100% 0g/s 185891p/s 185891c/s 185891C/s !Th@#1ho..*7¡Vamos!
Session completed
stdstring@stdstring-cppwork:~/labs$
```

Видно, что результата нет - пароль мы взломать не смогли с помощью John the Ripper
Попробуем найти дополнительную информацию в файловой системе.
Во-первых, файл _IPCAM.bin.extracted/squashfs-root/etc/mdev/automount.sh содержит имя вендора - XiongMaiTech:



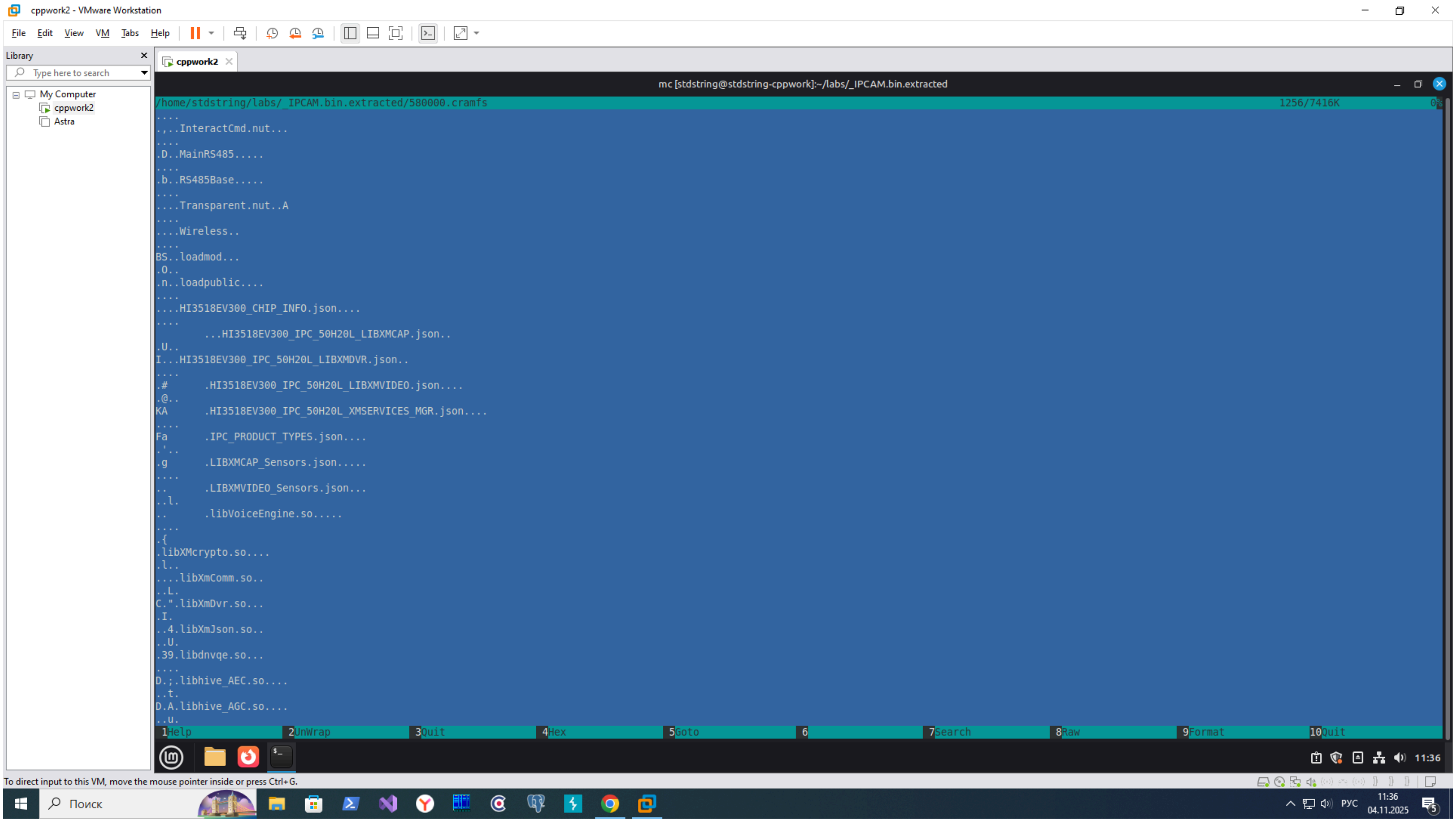
```
stdstring@stdstring-cppwork:~/labs/_IPCAM.bin.extracted/squashfs-root/etc/mdev$ cat automount.sh
################################
#       XiongMaiTech
################################

MOUNT_DIR=/var/tmp/mmcblock0

auto_test()
{
        if [ -f $MOUNT_DIR/xm_autorun.sh ];then
                test -e /var/tmp/completion && $MOUNT_DIR/xm_autorun.sh
        fi
}

mkdir -p $MOUNT_DIR
if [ "$ACTION" == remove ];then
        MOUNT_STR=`mount | grep "$DEVNAME "`
        if [ -n "$MOUNT_STR" ];then
                umount $MOUNT_DIR -l
        fi
elif [ "$ACTION" == add ];then
        sleep 1
        if [ "$DEVNAME" == mmcblk0 ] && [ ! -e /dev/mmcblk0p* ];then
                mount /dev/$DEVNAME $MOUNT_DIR
                auto_test
        elif [ "$DEVNAME " != mmcblk0 ];then
                MOUNT_STR=`mount | grep "mmcblk0 "`
                if [ -n "$MOUNT_STR" ]; then
                        umount /dev/mmcblk0 -l
                fi
                mount /dev/$DEVNAME $MOUNT_DIR
                auto_test
        fi
fistdstring@stdstring-cppwork:~/labs/_IPCAM.bin.extracted/squashfs-root/etc/mdev$
```

Во-вторых, в директории _IPCAM.bin.extracted содержится несколько cramfs (Compressed ROM file system) файлов:



```
stdstring@stdstring-cppwork:~/labs/_IPCAM.bin.extracted$ ls -la *.cramfs
-rw-rw-r-- 1 stdstring stdstring 7593984 Nov  3 23:08 580000.cramfs
-rw-rw-r-- 1 stdstring stdstring  417792 Nov  3 23:08 CC0000.cramfs
-rw-rw-r-- 1 stdstring stdstring   45056 Nov  3 23:08 E40000.cramfs
stdstring@stdstring-cppwork:~/labs/_IPCAM.bin.extracted$
```

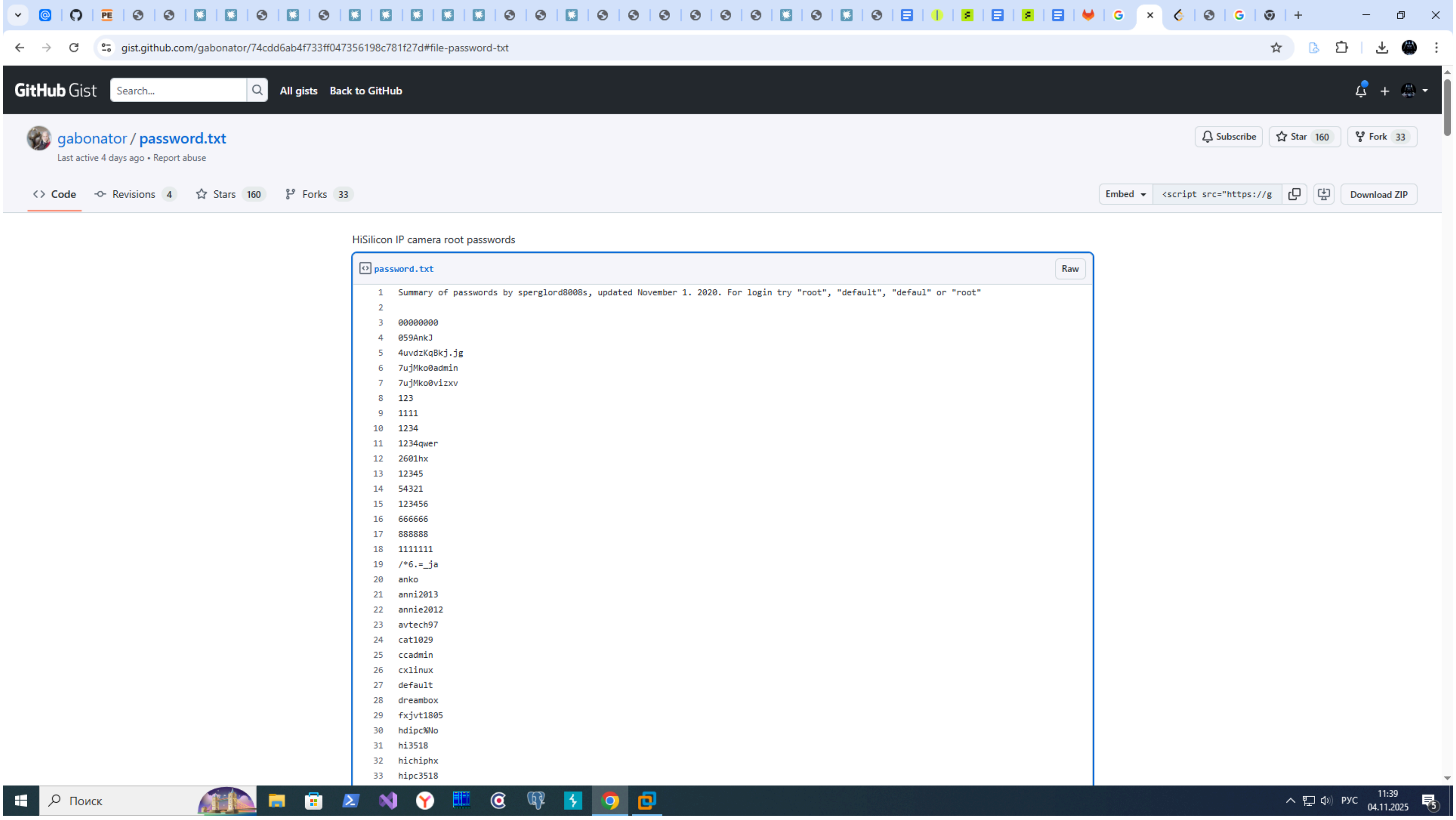
Смотрим содержимое файла 580000.cramfs в средстве для просмотра midnight commander (можно, конечно, посмотреть и с помощью cat/less):


cppwork2 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
cppwork2
Astra
cppwork2
mc [stdstring@stdstring-cppwork]:~/labs/_IPCAM.bin.extracted
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Поиск
РУС
11:36
04.11.2025

```
/home/stdstring/labs/_IPCAM.bin.extracted/580000.cramfs                                    1256/7416K   0%
....
.,..InteractCmd.nut...
....
.D..MainRS485.....
....
.b..RS485Base.....
....
....Transparent.nut..A
....
....Wireless..
....
BS..loadmod...
.O..
.n..loadpublic....
....
....HI3518EV300_CHIP_INFO.json....
....
        ...HI3518EV300_IPC_50H20L_LIBXMCAP.json..
.U..
I...HI3518EV300_IPC_50H20L_LIBXMDVR.json..
....
.#      .HI3518EV300_IPC_50H20L_LIBXMVIDEO.json....
.@..
KA      .HI3518EV300_IPC_50H20L_XMSERVICES_MGR.json....
....
Fa      .IPC_PRODUCT_TYPES.json....
.'..
.g      .LIBXMCAP_Sensors.json.....
....
..      .LIBXMVIDEO_Sensors.json...
..l.
..      .libVoiceEngine.so.....
....
.{
.libXMcrypto.so....
.l..
....libXmComm.so..
..L.
C.".libXmDvr.so...
.I.
..4.libXmJson.so..
..U.
.39.libdnvqe.so...
....
D.;.libhive_AEC.so....
..t.
D.A.libhive_AGC.so....
..u.
 1Help    2UnWrap   3Quit    4Hex    5Goto    6    7Search   8Raw    9Format   10Quit
```

В нем видно очень интересную строку - HI3518EV300_CHIP_INFO.json. Похоже, что HI3518EV300 - это название чипа. Если вбить это название в поисковике, то он предложит следующее имя для камеры: hisilicon hi3518ev300.

Ищу в поисковике словарь с паролями для камеры: hisilicon hi3518ev300 - нахожу следующий словарь:



gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d#file-password-txt

gabonator / password.txt

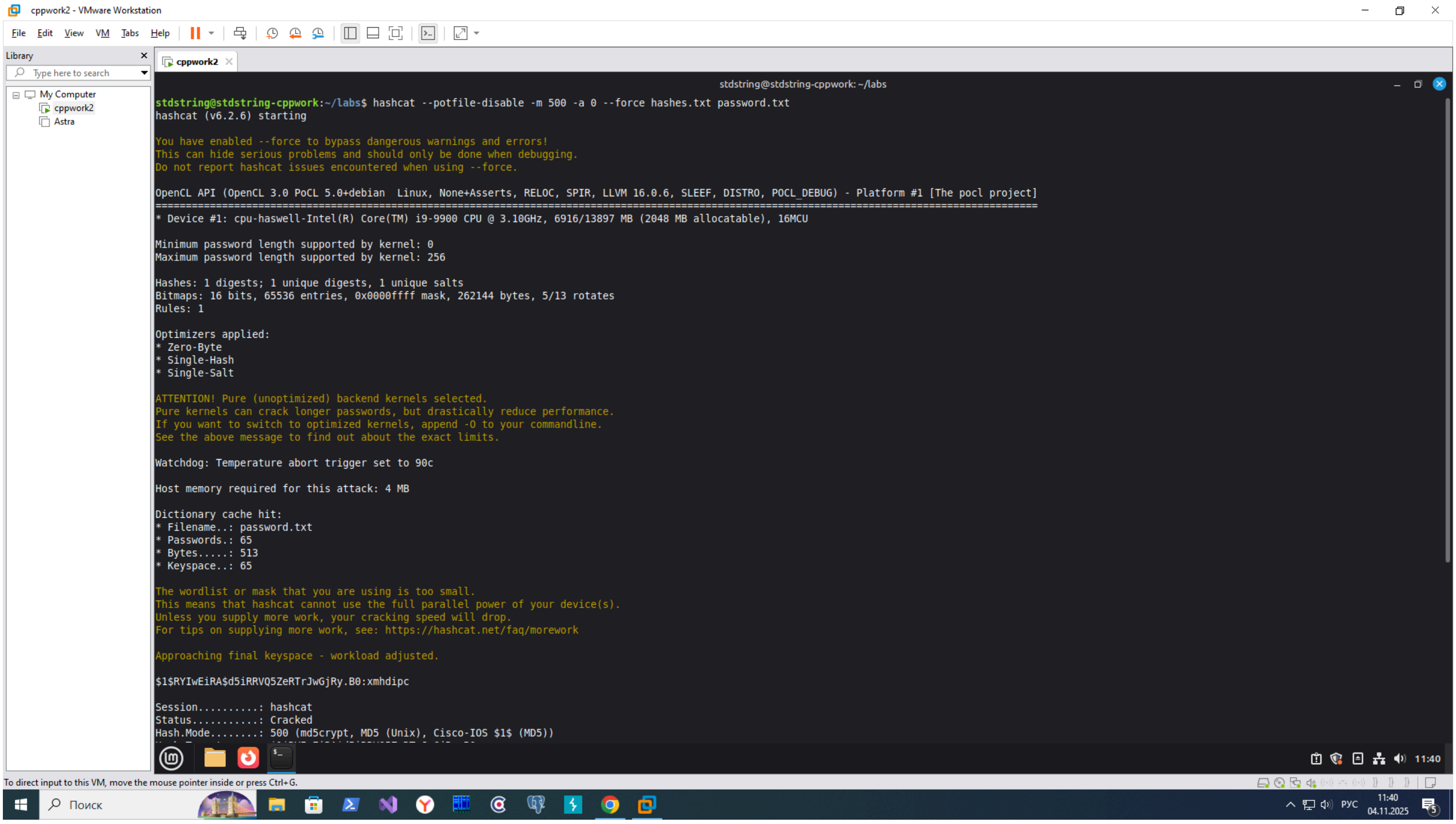
Last active 4 days ago • Report abuse

HiSilicon IP camera root passwords

password.txt

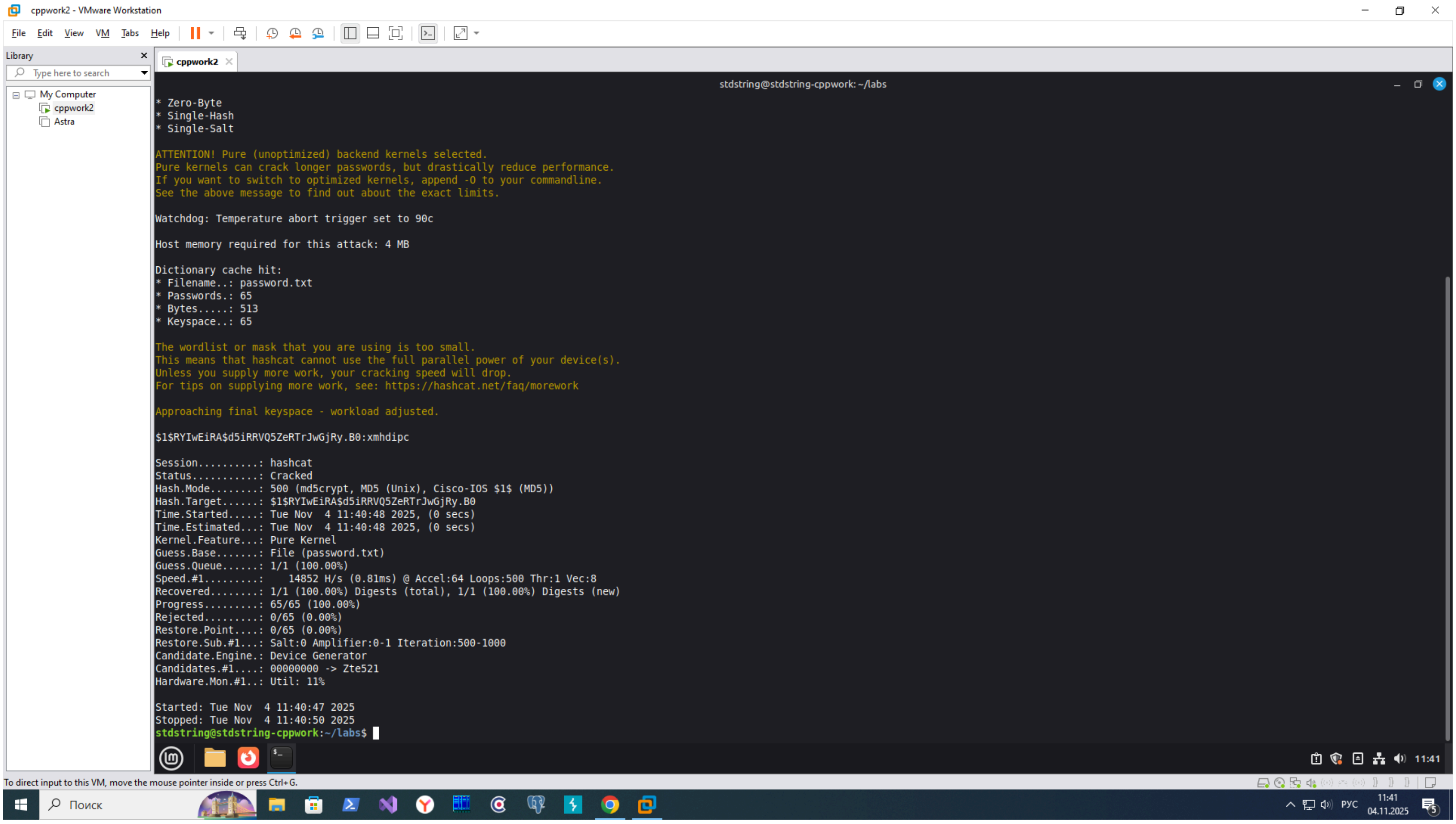
```
Summary of passwords by sperglord8008s, updated November 1. 2020. For login try "root", "default", "defaul" or "root"

00000000
059AnkJ
4uvdzKqBkj.jg
7ujMko0admin
7ujMko0vizxv
123
1111
1234
1234qwer
2601hx
12345
54321
123456
666666
888888
1111111
/*6.=_ja
anko
anni2013
annie2012
avtech97
cat1029
ccadmin
cxlinux
default
dreambox
fxjvt1805
hdipc%No
hi3518
hichiphx
hipc3518
```

Скачиваю его, убираю первые 2 строки. Попробую подобрать пароль с его помощью. Запускаю hashcat:



```
stdstring@stdstring-cppwork:~/labs$ hashcat --potfile-disable -m 500 -a 0 --force hashes.txt password.txt
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====================================================================================================================================================
* Device #1: cpu-haswell-Intel(R) Core(TM) i9-9900 CPU @ 3.10GHz, 6916/13897 MB (2048 MB allocatable), 16MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 4 MB

Dictionary cache hit:
* Filename..: password.txt
* Passwords.: 65
* Bytes.....: 513
* Keyspace..: 65

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

$1$RYIwEiRA$d5iRRVQ5ZeRTrJwGjRy.B0:xmhdipc

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5))
```

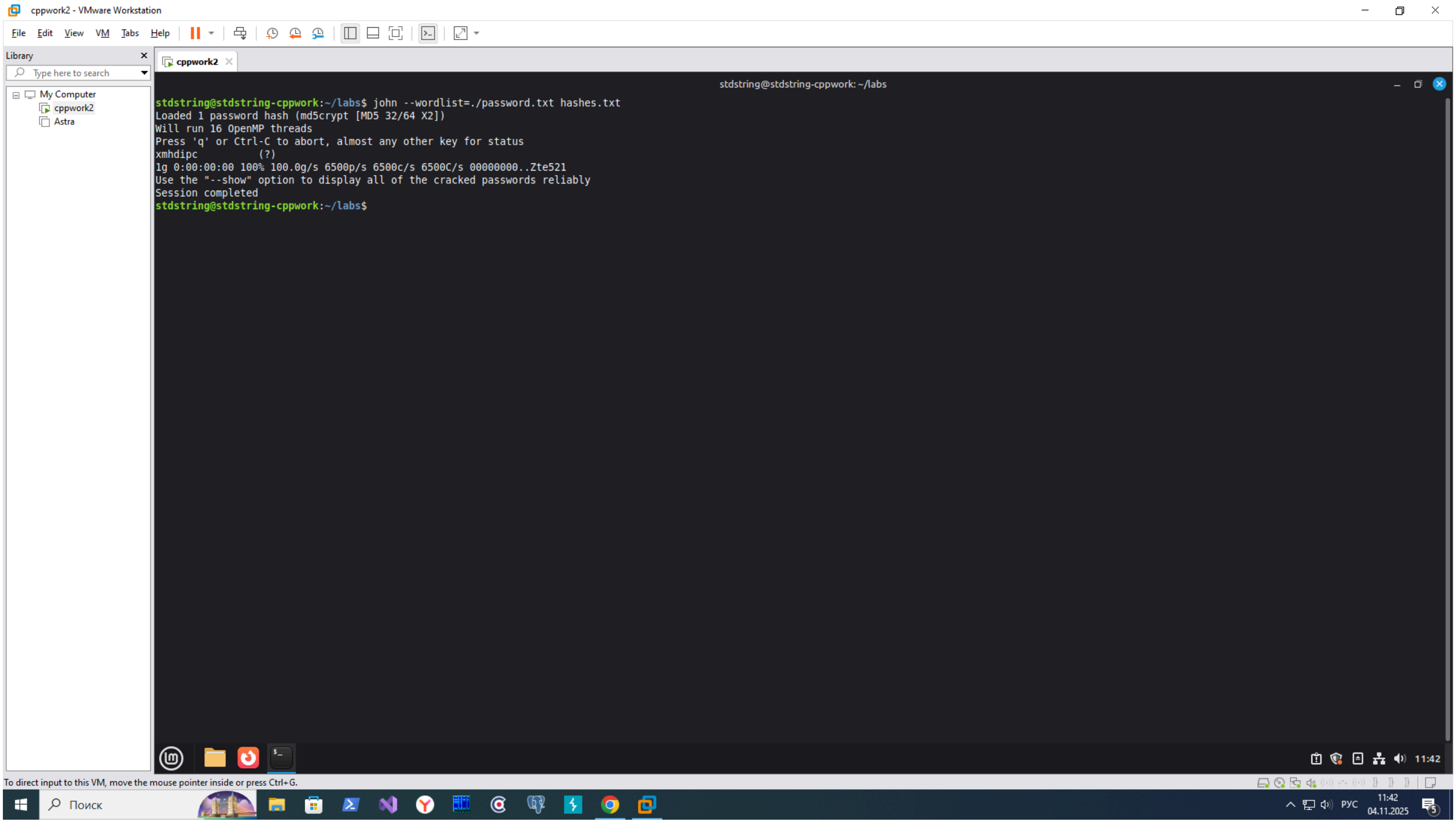
cppwork2 - VMware Workstation
File
Edit
View
VM
Tabs
Help
Library
My Computer
cppwork2
Astra
stdstring@stdstring-cppwork: ~/labs
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


cppwork2 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
cppwork2
Astra
cppwork2
stdstring@stdstring-cppwork: ~/labs
11:41
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Поиск
РУС
11:41
04.11.2025

```
* Zero-Byte
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 4 MB

Dictionary cache hit:
* Filename..: password.txt
* Passwords.: 65
* Bytes.....: 513
* Keyspace..: 65

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

$1$RYIwEiRA$d5iRRVQ5ZeRTrJwGjRy.B0:xmhdipc

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5))
Hash.Target......: $1$RYIwEiRA$d5iRRVQ5ZeRTrJwGjRy.B0
Time.Started.....: Tue Nov  4 11:40:48 2025, (0 secs)
Time.Estimated...: Tue Nov  4 11:40:48 2025, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (password.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    14852 H/s (0.81ms) @ Accel:64 Loops:500 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 65/65 (100.00%)
Rejected.........: 0/65 (0.00%)
Restore.Point....: 0/65 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:500-1000
Candidate.Engine.: Device Generator
Candidates.#1....: 00000000 -> Zte521
Hardware.Mon.#1..: Util: 11%

Started: Tue Nov  4 11:40:47 2025
Stopped: Tue Nov  4 11:40:50 2025
stdstring@stdstring-cppwork:~/labs$ 
```

Видно, что hashcat смог подобрать пароль по этому словарю - это xmhdipc.

Запускаю John the Ripper:


cppwork2 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
cppwork2
Astra
cppwork2
stdstring@stdstring-cppwork: ~/labs
11:42
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Поиск
РУС
11:42
04.11.2025

```
stdstring@stdstring-cppwork:~/labs$ john --wordlist=./password.txt hashes.txt
Loaded 1 password hash (md5crypt [MD5 32/64 X2])
Will run 16 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
xmhdipc          (?)
1g 0:00:00:00 100% 100.0g/s 6500p/s 6500c/s 6500C/s 00000000..Zte521
Use the "--show" option to display all of the cracked passwords reliably
Session completed
stdstring@stdstring-cppwork:~/labs$
```

Видно, что John the Ripper смог подобрать пароль по этому словарю - это xmhdipc.

5. Выводы.

- Без знания дополнительной информации об устройстве очень трудно восстановить пароль по стандартному словарю, т.к. его там может и не быть.
- Если есть информация об устройстве и пароль остался стандартным, то его восстановление очень простое, т.к. в интернете можно найти словари паролей для подбора перебором.
- Поэтому рекомендация к защите устройства только одна - использовать сложные, длинные, не стандартные пароли; всегда менять заводские пароли на свои. По возможности не пользоваться MD5 хеш-функцией, которая является устаревшей (по ней можно подобрать пароль за приемлемое время даже не пользуясь словарями паролей).