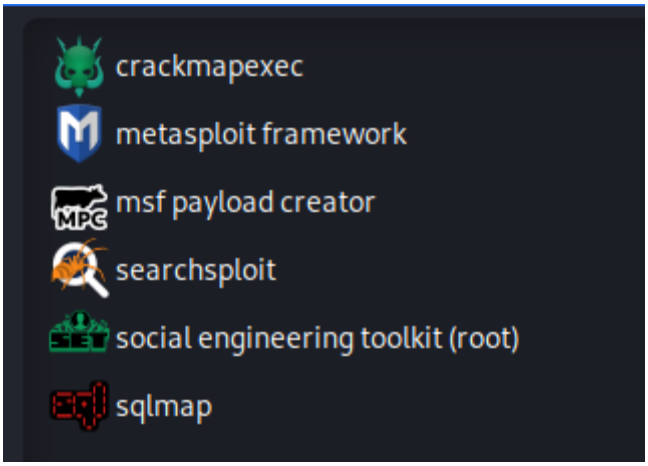
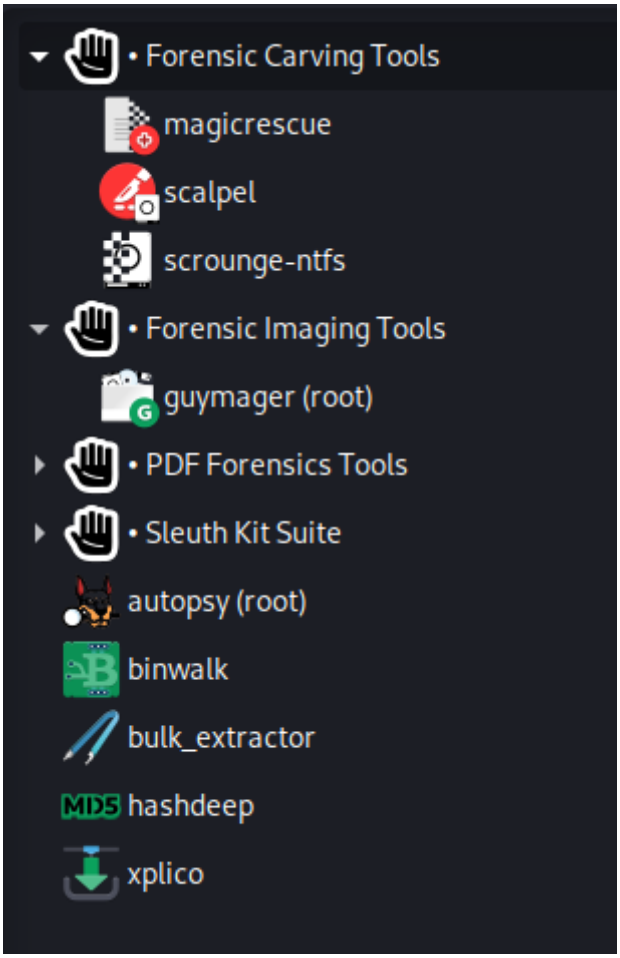
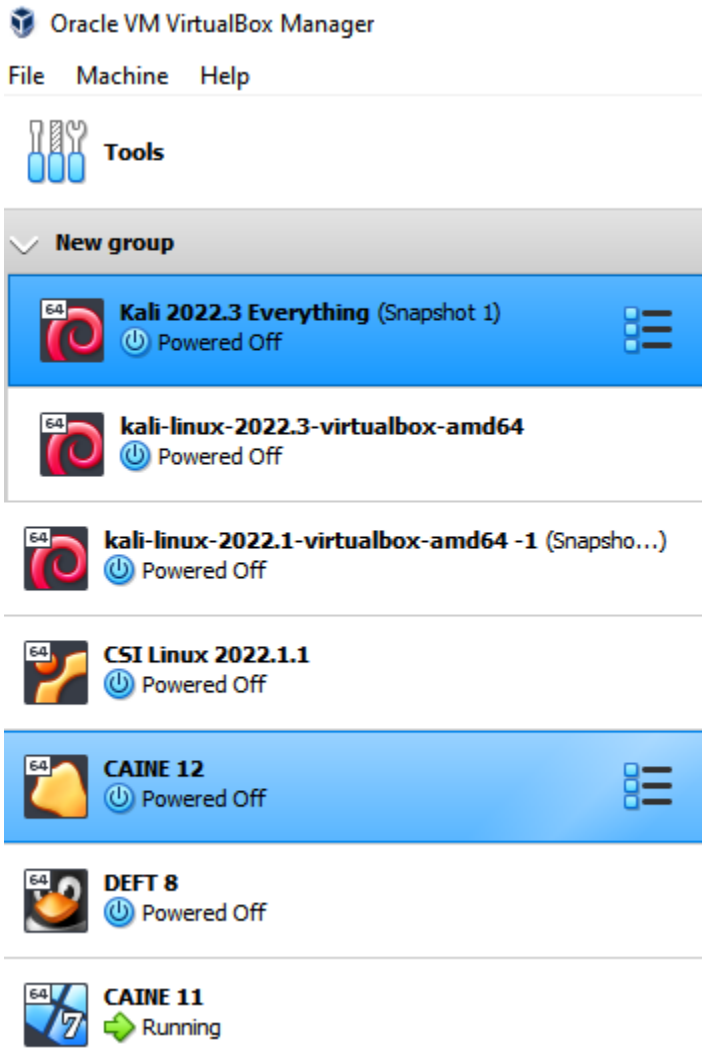
Chapter 1: Red, Blue, and Purple Teaming Fundamentals

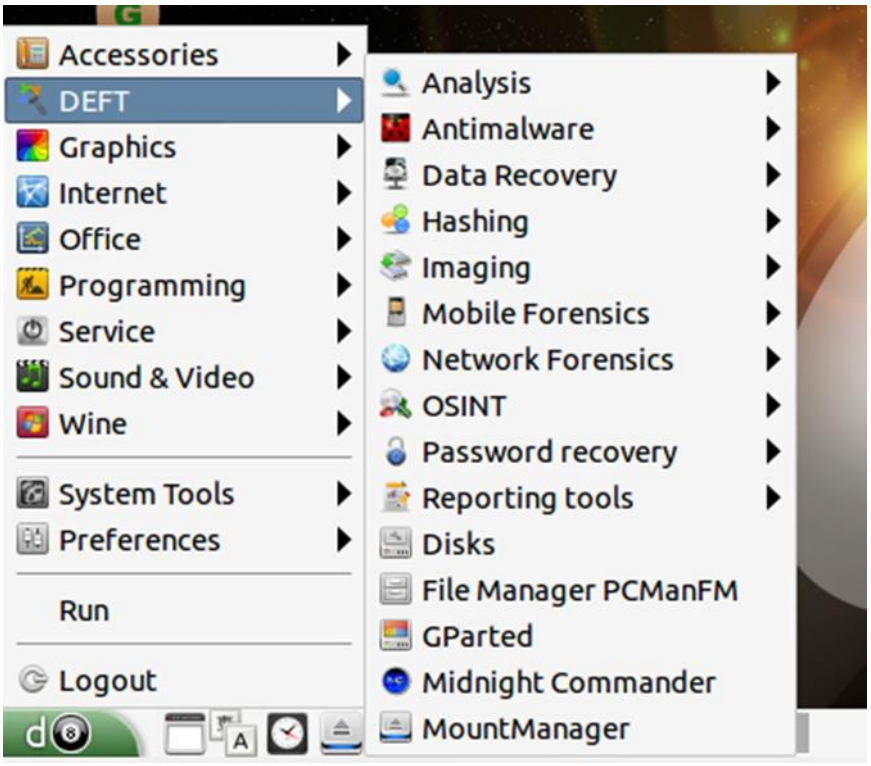

crackmapexec
metasploit framework
msf payload creator
searchsploit
social engineering toolkit (root)
sqlmap

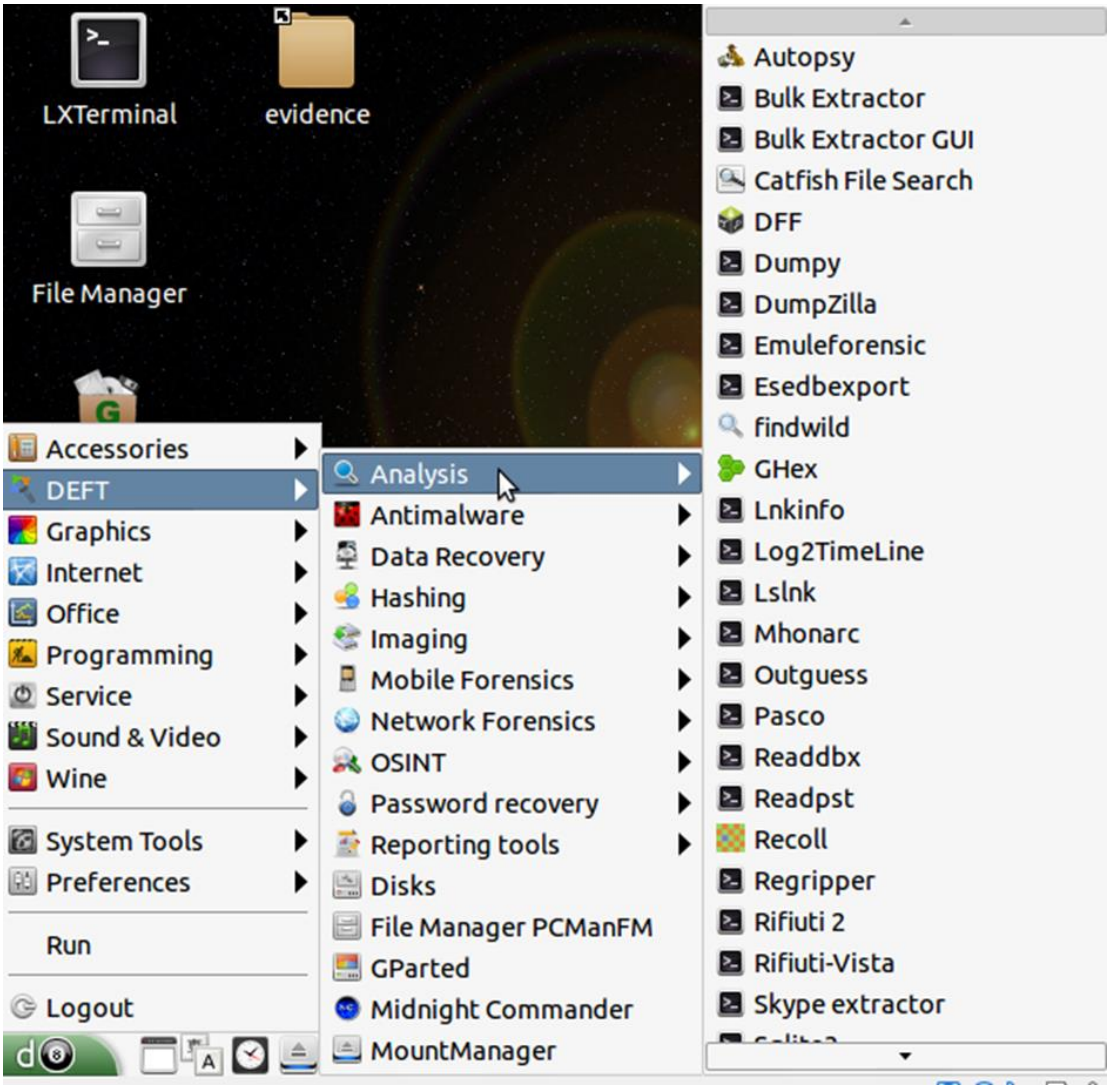

• Forensic Carving Tools
magicrescue
scalpel
scrounge-ntfs
• Forensic Imaging Tools
guymager (root)
• PDF Forensics Tools
• Sleuth Kit Suite
autopsy (root)
binwalk
bulk_extractor
hashdeep
xplico

Chapter 2: Introduction to Digital Forensics




deft
DEFT Linux 8 live
DEFT Linux 8 live text mode
23 s
Install DEFT Linux 8
Check disc for defects
Test memory
Boot from first hard disk

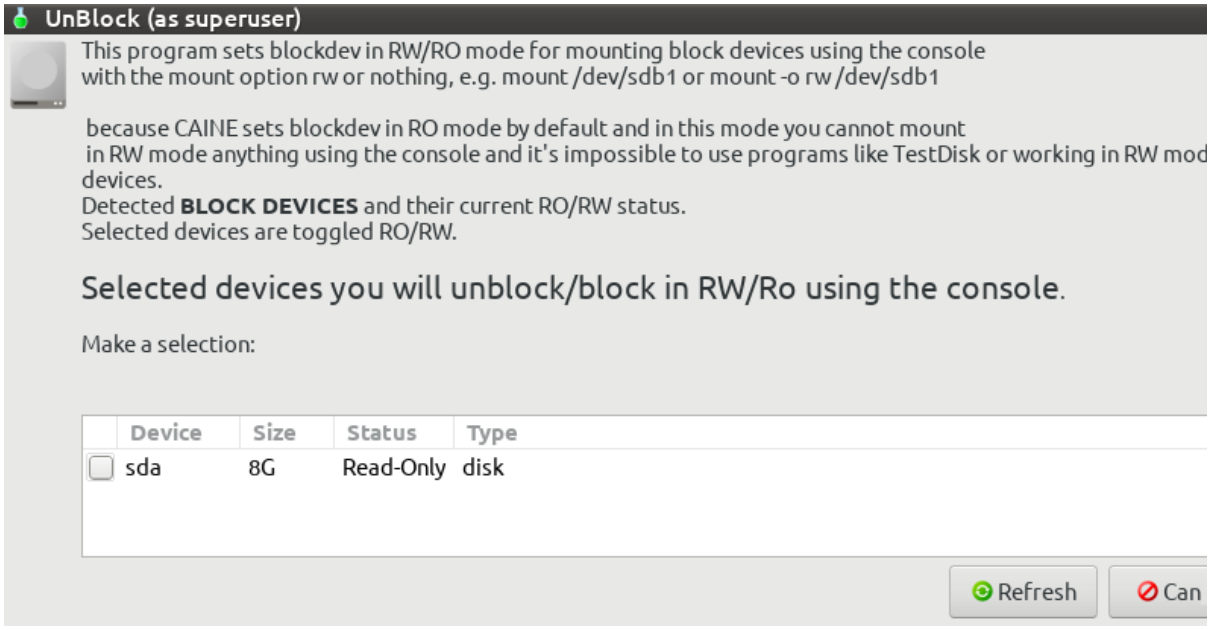

Accessories
DEFT
Graphics
Internet
Office
Programming
Service
Sound & Video
Wine
System Tools
Preferences
Run
Logout
Analysis
Antimalware
Data Recovery
Hashing
Imaging
Mobile Forensics
Network Forensics
OSINT
Password recovery
Reporting tools
Disks
File Manager PCManFM
GParted
Midnight Commander
MountManager

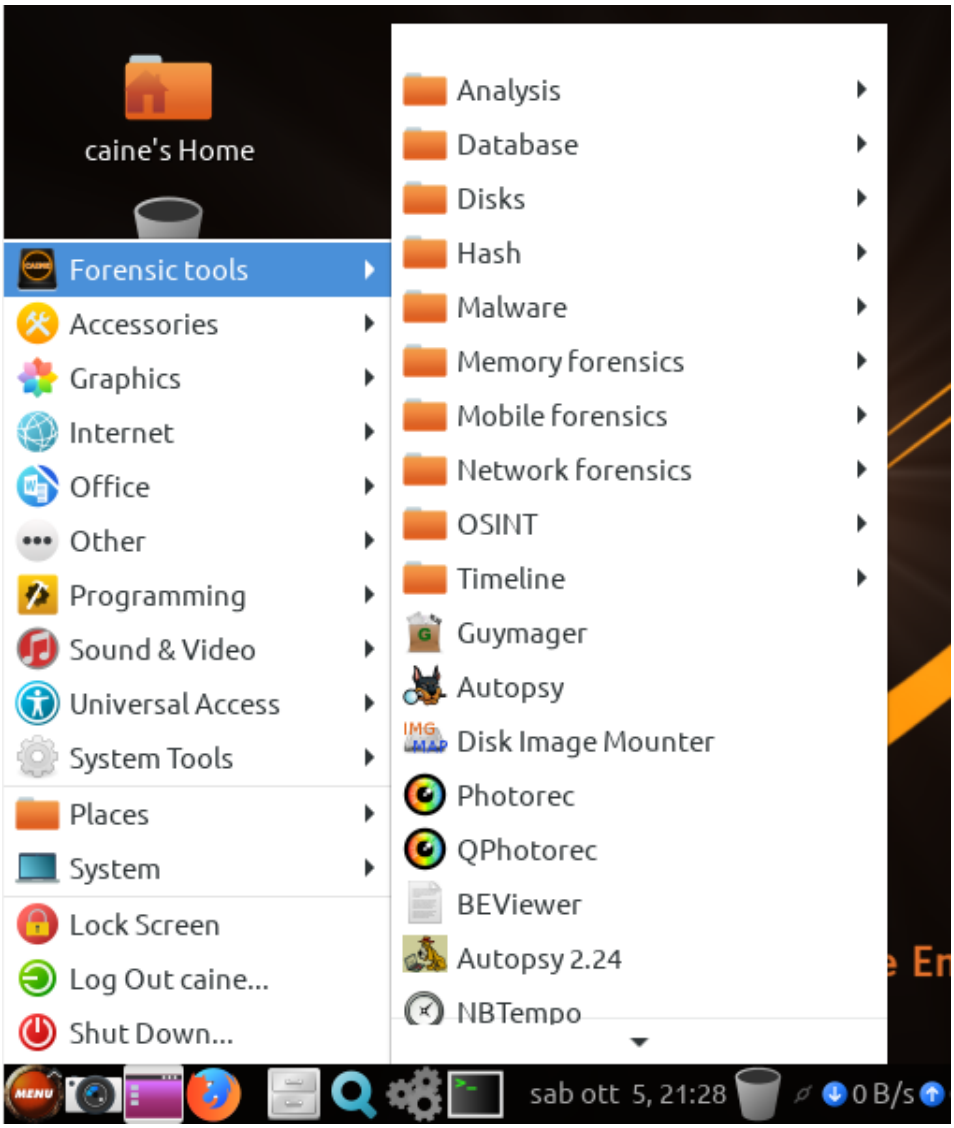

LXTerminal
evidence
File Manager
Accessories
DEFT
Graphics
Internet
Office
Programming
Service
Sound & Video
Wine
System Tools
Preferences
Run
Logout
Analysis
Antimalware
Data Recovery
Hashing
Imaging
Mobile Forensics
Network Forensics
OSINT
Password recovery
Reporting tools
Disks
File Manager PCManFM
GParted
Midnight Commander
MountManager
Autopsy
Bulk Extractor
Bulk Extractor GUI
Catfish File Search
DFF
Dumpy
DumpZilla
Emuleforensic
Esedbexport
findwild
GHex
Lnkinfo
Log2TimeLine
Lslnk
Mhonarc
Outguess
Pasco
Readdbx
Readpst
Recoll
Regripper
Rifiuti 2
Rifiuti-Vista
Skype extractor

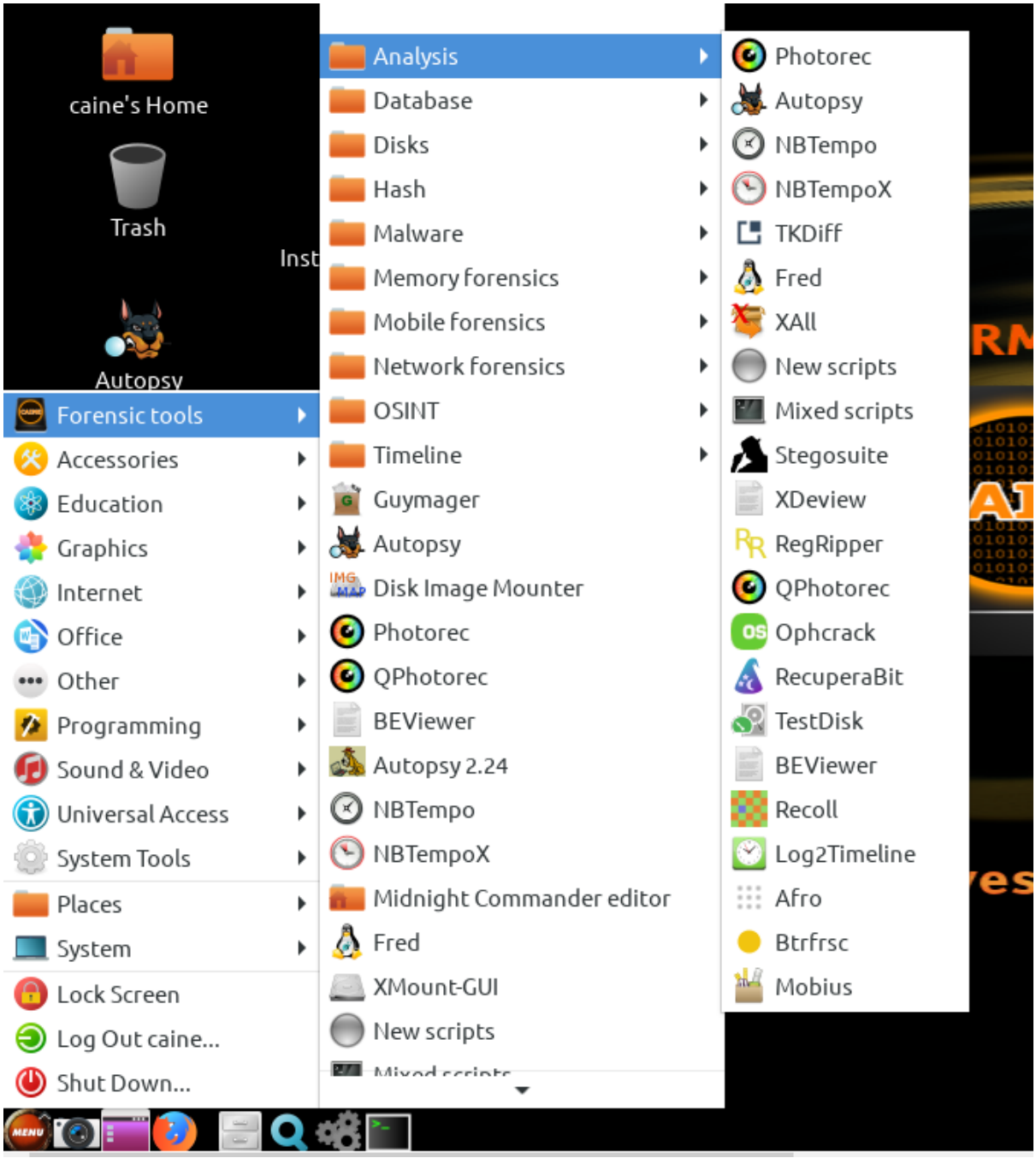

CAINE
START CAINE LIVE
Boot Live in safe graphics mode
Start in vesa compatibility mode
Boot Live in RAM
Boot Live in debug mode
Memory test
SIDEREAL
CAINE
Press TAB key to edit
Automatic boot in 1 second...
Computer Aided INvestigative Environment

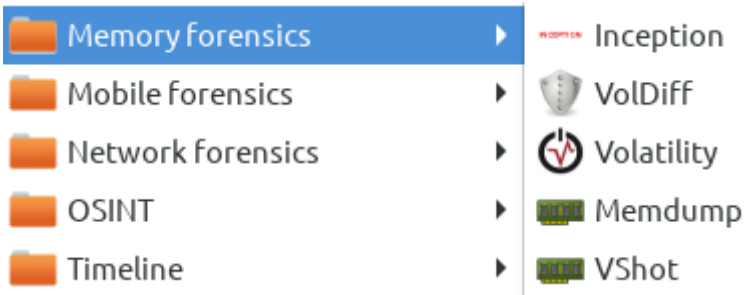

CAINE
START CAINE LIVE
Start in compatibility mode
Boot Live in safe graphics mode
Boot Live in RAM
Boot Live in debug mode
Memory test
WORMHOLE
CAINE
Press TAB key to edit
Automatic boot in 8 seconds...
Computer Aided INvestigative Environment


caine's Home
Autopsy
INFO
Trash
Caja-Root
keyboard
SIDEREAL
Install CAINE 20.04
Disk Image Mounter
Network
CAINE
Displays
UnBlock
Computer
Computer Aided INvestigative Environment
Guymager
Network Servers
mar ott 4, 16:39
0 B/s 0 B/s
en


UnBlock (as superuser)
This program sets blockdev in RW/RO mode for mounting block devices using the console
with the mount option rw or nothing, e.g. mount /dev/sdb1 or mount -o rw /dev/sdb1
because CAINE sets blockdev in RO mode by default and in this mode you cannot mount
in RW mode anything using the console and it's impossible to use programs like TestDisk or working in RW mod
devices.
Detected BLOCK DEVICES and their current RO/RW status.
Selected devices are toggled RO/RW.
Selected devices you will unblock/block in RW/Ro using the console.
Make a selection:
Device
Size
Status
Type
sda
8G
Read-Only
disk
Refresh
Can

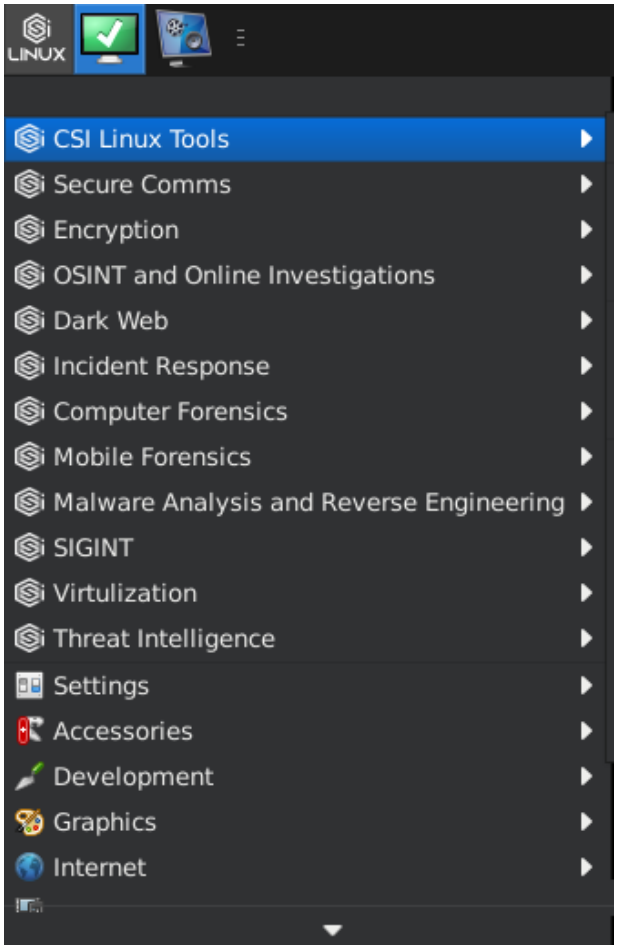

caine's Home
Forensic tools
Accessories
Graphics
Internet
Office
Other
Programming
Sound & Video
Universal Access
System Tools
Places
System
Lock Screen
Log Out caine...
Shut Down...
Analysis
Database
Disks
Hash
Malware
Memory forensics
Mobile forensics
Network forensics
OSINT
Timeline
Guymager
Autopsy
Disk Image Mounter
Photorec
QPhotorec
BEViewer
Autopsy 2.24
NBTempo
sab ott 5, 21:28
0 B/s


caine's Home
Trash
Autopsy
Forensic tools
Accessories
Education
Graphics
Internet
Office
Other
Programming
Sound & Video
Universal Access
System Tools
Places
System
Lock Screen
Log Out caine...
Shut Down...
Analysis
Database
Disks
Hash
Malware
Memory forensics
Mobile forensics
Network forensics
OSINT
Timeline
Guymager
Autopsy
Disk Image Mounter
Photorec
QPhotorec
BEViewer
Autopsy 2.24
NBTempo
NBTempoX
Midnight Commander editor
Fred
XMount-GUI
New scripts
Photorec
Autopsy
NBTempo
NBTempoX
TKDiff
Fred
XAll
New scripts
Mixed scripts
Stegosuite
XDeview
RegRipper
QPhotorec
Ophcrack
RecuperaBit
TestDisk
BEViewer
Recoll
Log2Timeline
Afro
Btrfrsc
Mobius

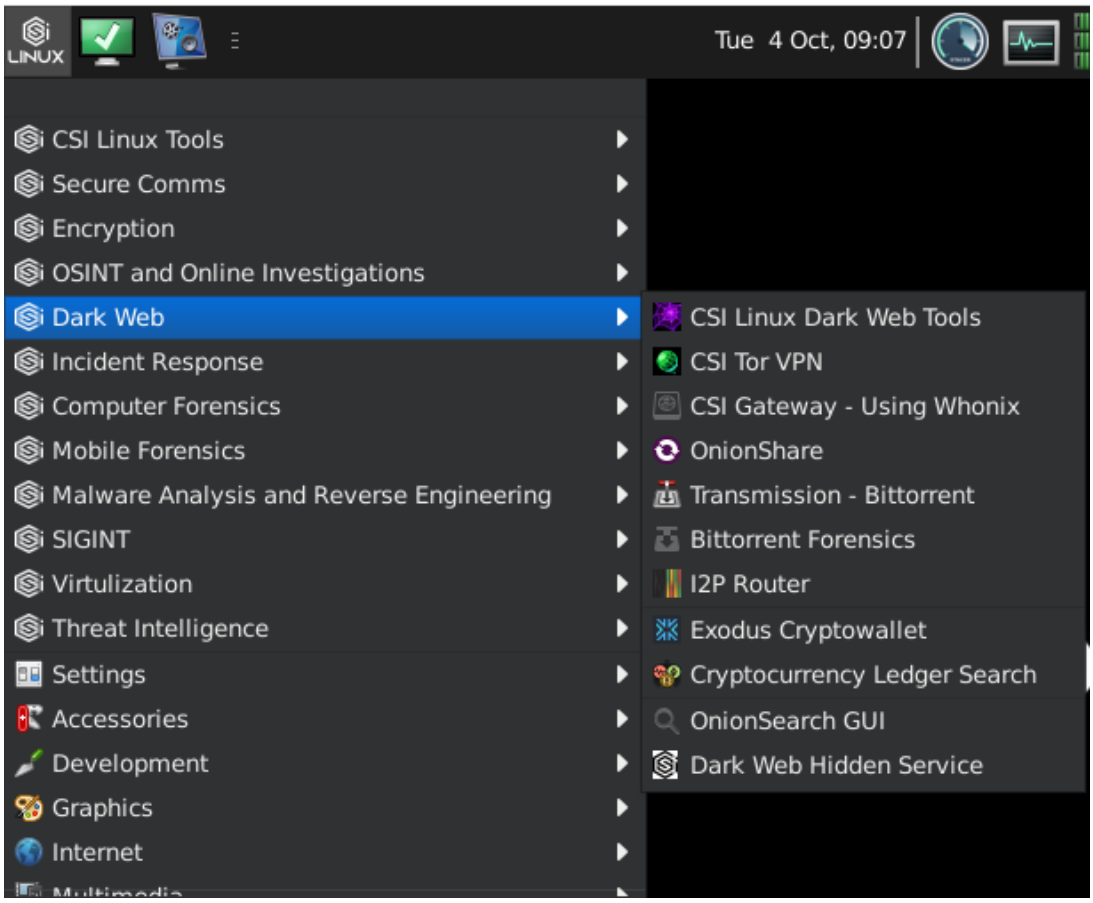

Memory forensics
Mobile forensics
Network forensics
OSINT
Timeline
Inception
VolDiff
Volatility
Memdump
VShot

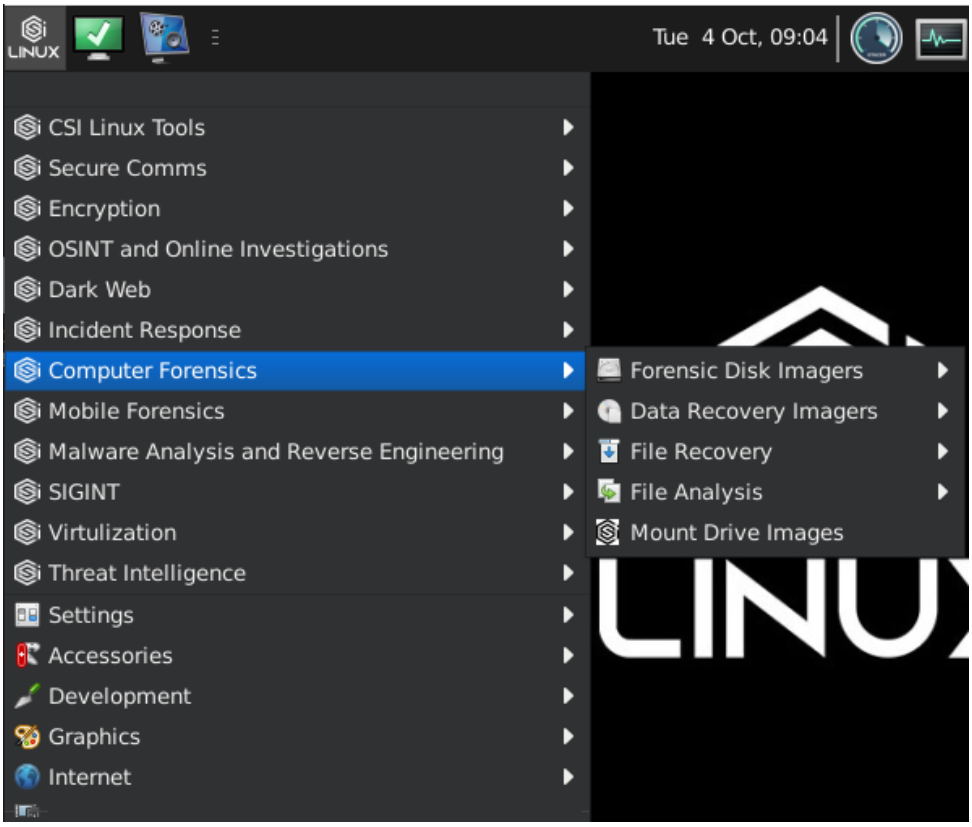

Login:

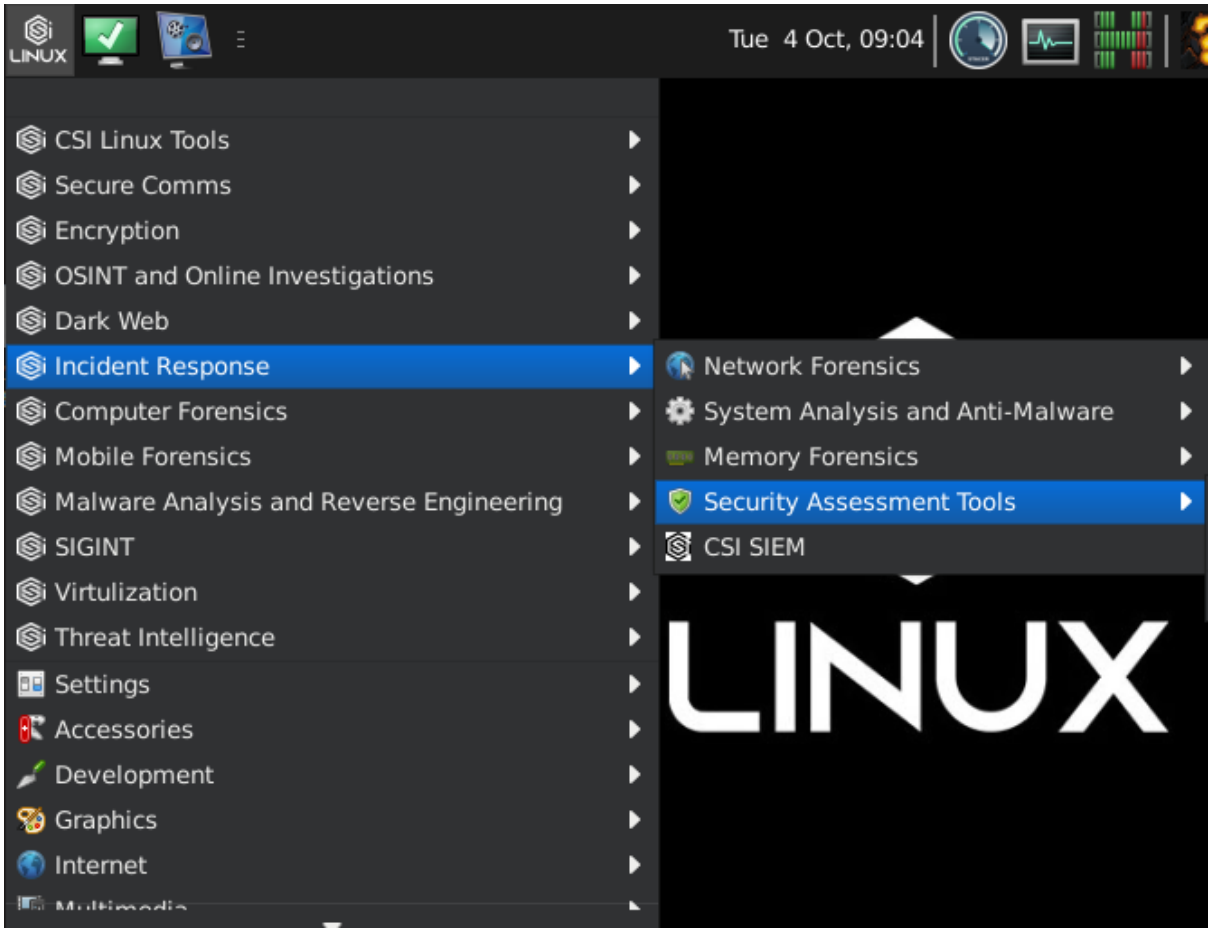

Tue 4 Oct, 08:58
(0:00, 98%)
Internet Incognito
ReadMe.ctb
Cases
LINUX
Start a Case
Trash
LINUX


LINUX
CSI Linux Tools
Secure Comms
Encryption
OSINT and Online Investigations
Dark Web
Incident Response
Computer Forensics
Mobile Forensics
Malware Analysis and Reverse Engineering
SIGINT
Virtulization
Threat Intelligence
Settings
Accessories
Development
Graphics
Internet

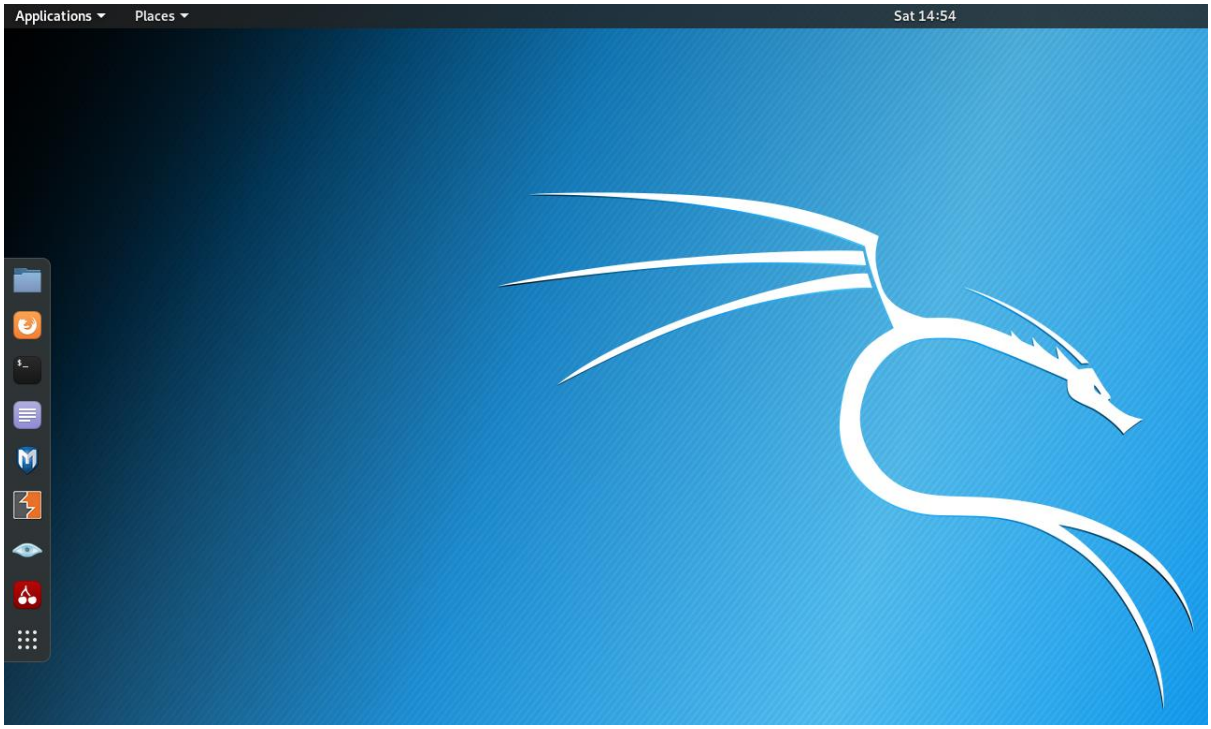

LINUX
Tue 4 Oct, 09:06
CSI Linux Tools
Secure Comms
Encryption
OSINT and Online Investigations
Dark Web
Incident Response
Computer Forensics
Mobile Forensics
Malware Analysis and Reverse Engineering
SIGINT
Virtulization
Threat Intelligence
Settings
Accessories
Development
Graphics
Internet
Domain OSINT - Recon
Email OSINT
Phone Number Information
SOCMINT Social Media Investigation
OSINT Frameworks
Geolocation and Socail Engineering
FBI Wanted List
Sock Puppet Builder
Open Corporates Search
Hunchly 2
CSI Social Media Investigation
CSI Video Downloader

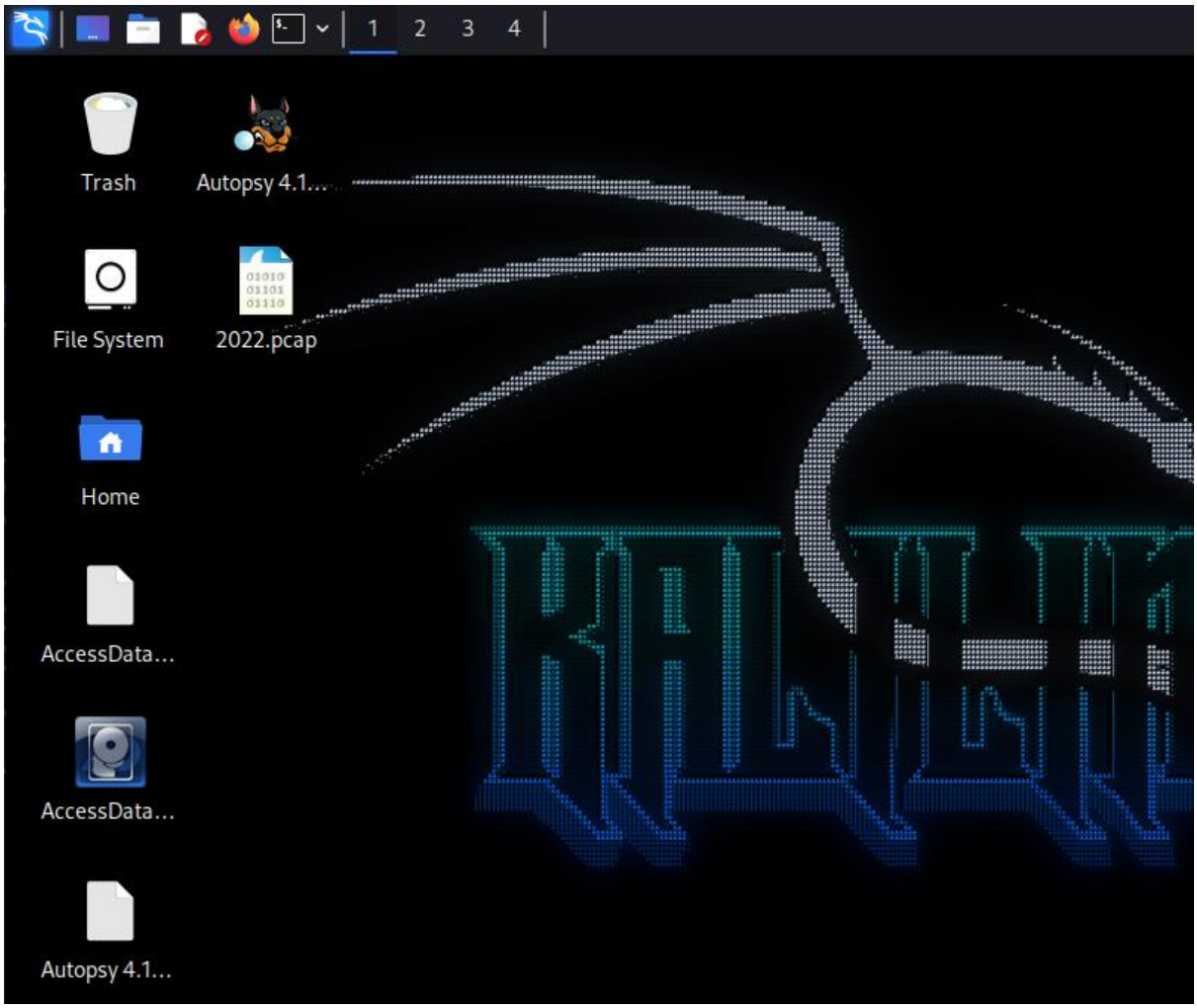

LINUX
Tue 4 Oct, 09:07
CSI Linux Tools
Secure Comms
Encryption
OSINT and Online Investigations
Dark Web
Incident Response
Computer Forensics
Mobile Forensics
Malware Analysis and Reverse Engineering
SIGINT
Virtulization
Threat Intelligence
Settings
Accessories
Development
Graphics
Internet
CSI Linux Dark Web Tools
CSI Tor VPN
CSI Gateway - Using Whonix
OnionShare
Transmission - Bittorrent
Bittorrent Forensics
I2P Router
Exodus Cryptowallet
Cryptocurrency Ledger Search
OnionSearch GUI
Dark Web Hidden Service

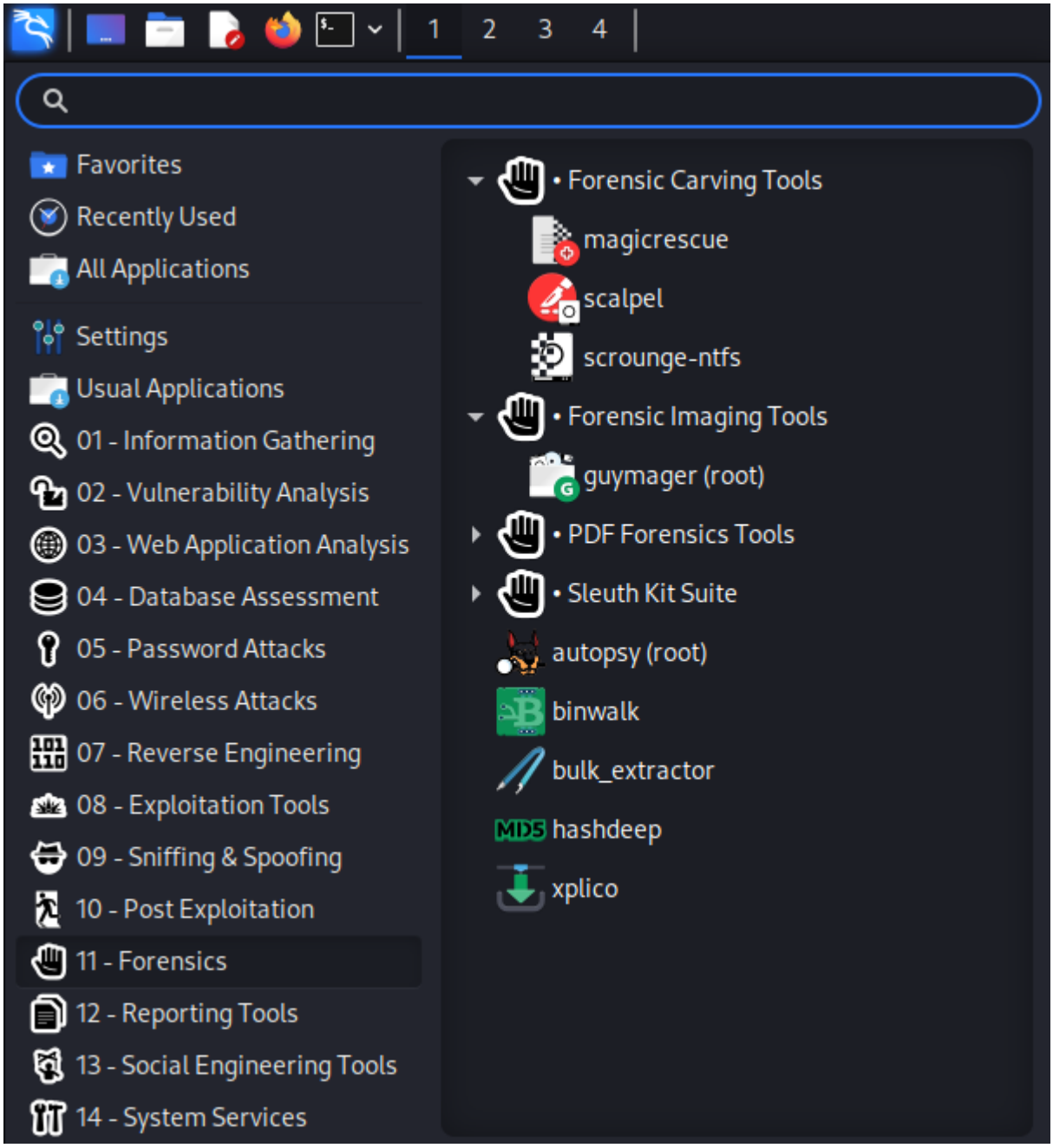

LINUX
Tue 4 Oct, 09:04
CSI Linux Tools
Secure Comms
Encryption
OSINT and Online Investigations
Dark Web
Incident Response
Computer Forensics
Mobile Forensics
Malware Analysis and Reverse Engineering
SIGINT
Virtulization
Threat Intelligence
Settings
Accessories
Development
Graphics
Internet
Forensic Disk Imagers
Data Recovery Imagers
File Recovery
File Analysis
Mount Drive Images


LINUX
Tue 4 Oct, 09:04
CSI Linux Tools
Secure Comms
Encryption
OSINT and Online Investigations
Dark Web
Incident Response
Computer Forensics
Mobile Forensics
Malware Analysis and Reverse Engineering
SIGINT
Virtulization
Threat Intelligence
Settings
Accessories
Development
Graphics
Internet
Network Forensics
System Analysis and Anti-Malware
Memory Forensics
Security Assessment Tools
CSI SIEM
LINUX

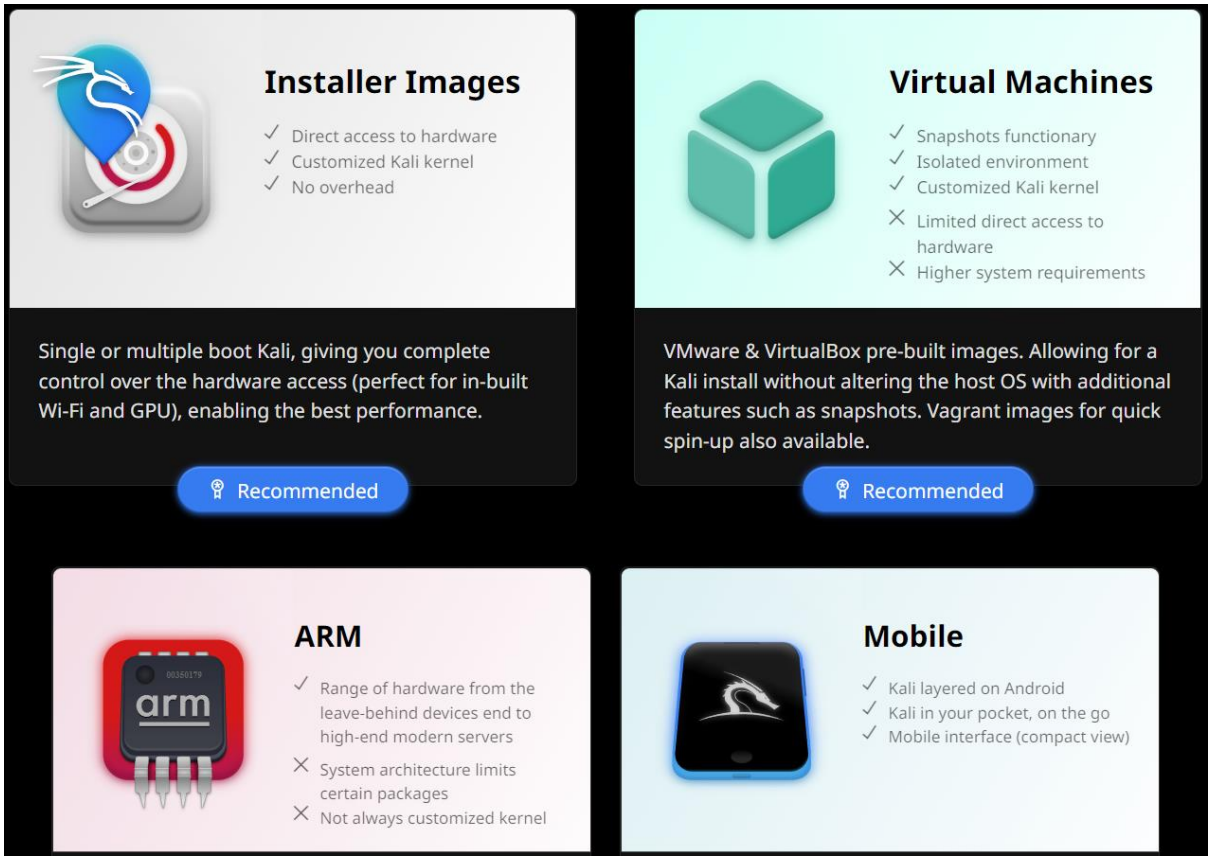

KALI
"the quieter you become, the more you are able to hear"
Boot menu
Live (amd64)
Live (amd64 failsafe)
Live (forensic mode)
Live USB Persistence (check kali.org/prst)
Live USB Encrypted Persistence (check kali.org/prst)
Install
Graphical install
Install with speech synthesis
Advanced options

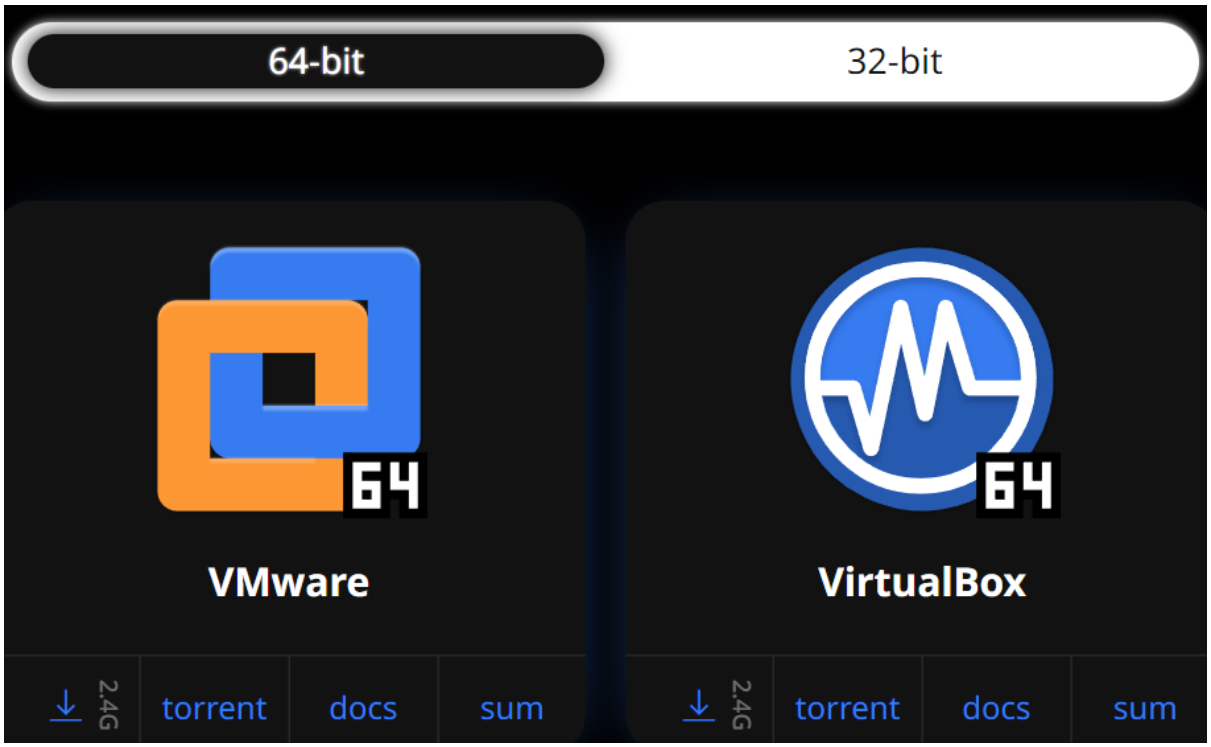

Applications
Places
Sat 14:54

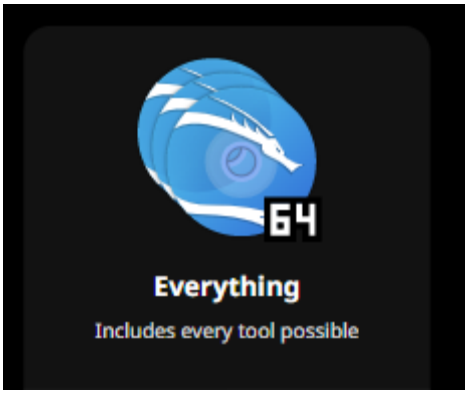

1
2
3
4
Trash
Autopsy 4.1...
File System
2022.pcap
Home
AccessData...
AccessData...
Autopsy 4.1...

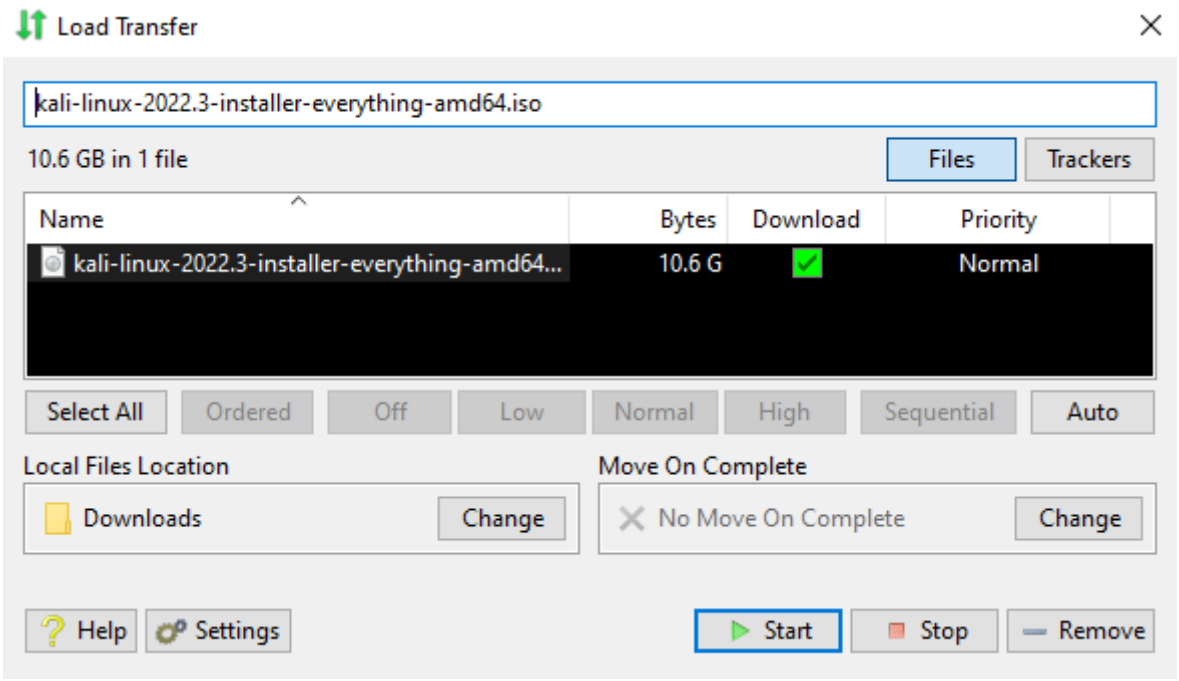

1
2
3
4
Favorites
Recently Used
All Applications
Settings
Usual Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
14 - System Services
• Forensic Carving Tools
magicrescue
scalpel
scrounge-ntfs
• Forensic Imaging Tools
guymager (root)
• PDF Forensics Tools
• Sleuth Kit Suite
autopsy (root)
binwalk
bulk_extractor
hashdeep
xplico

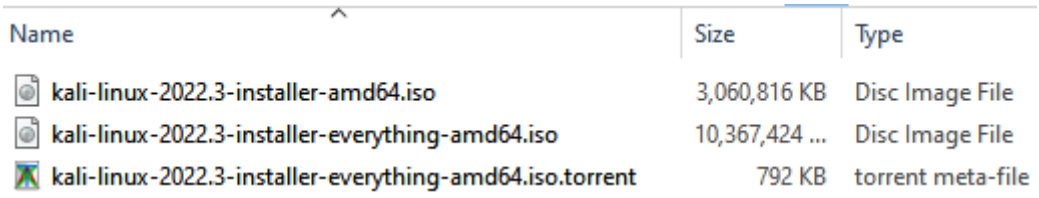
Chapter 3: Installing Kali Linux

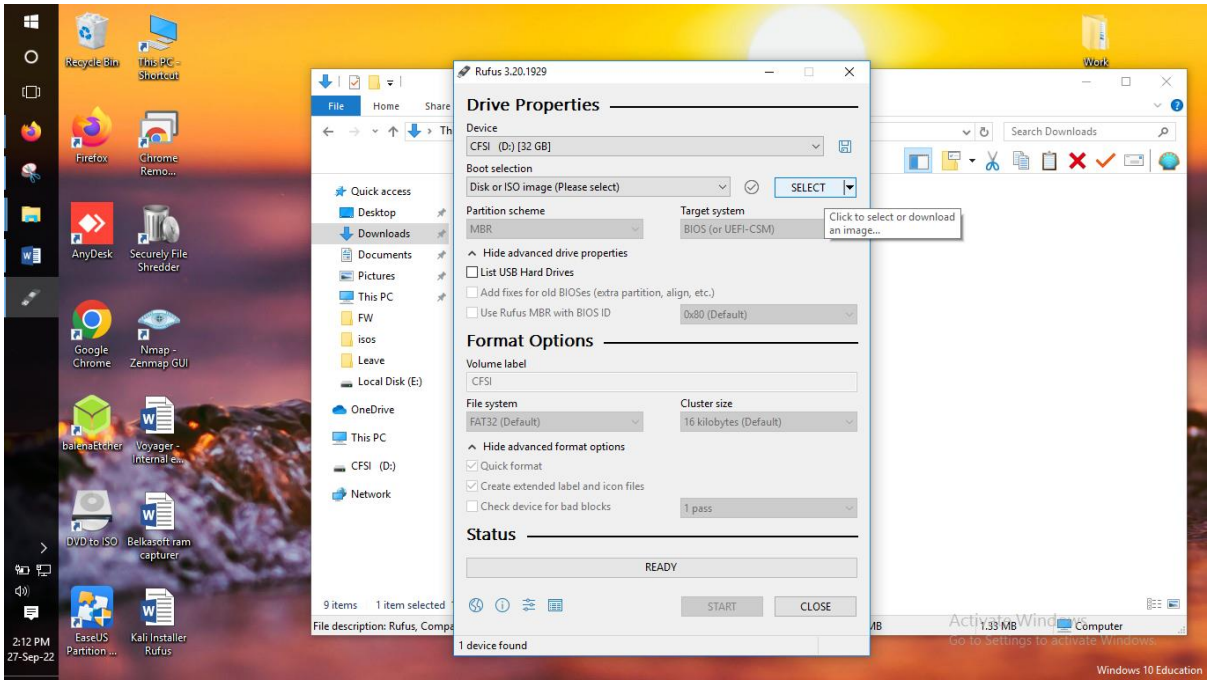


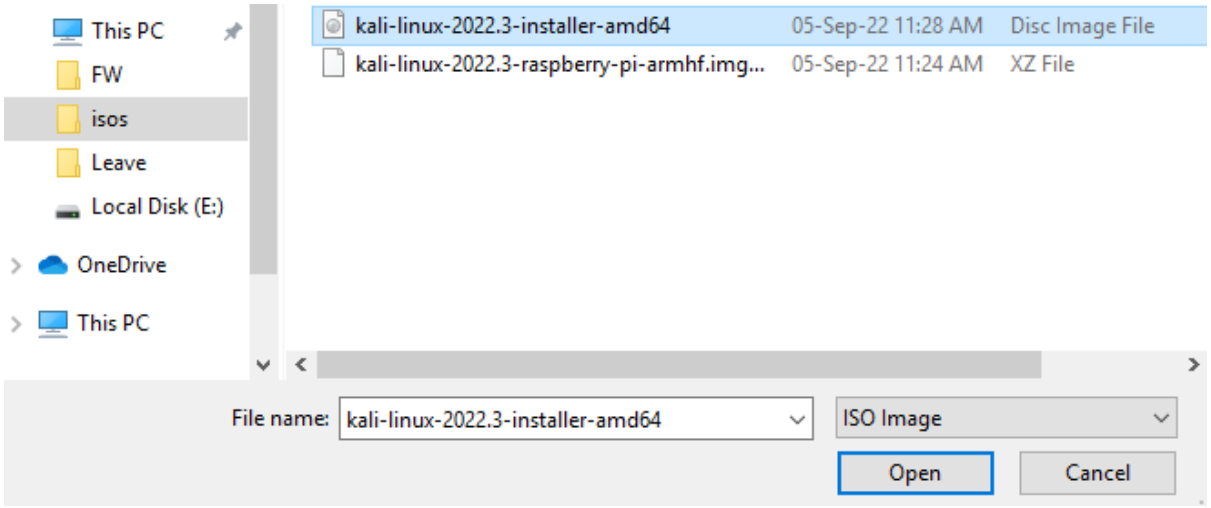


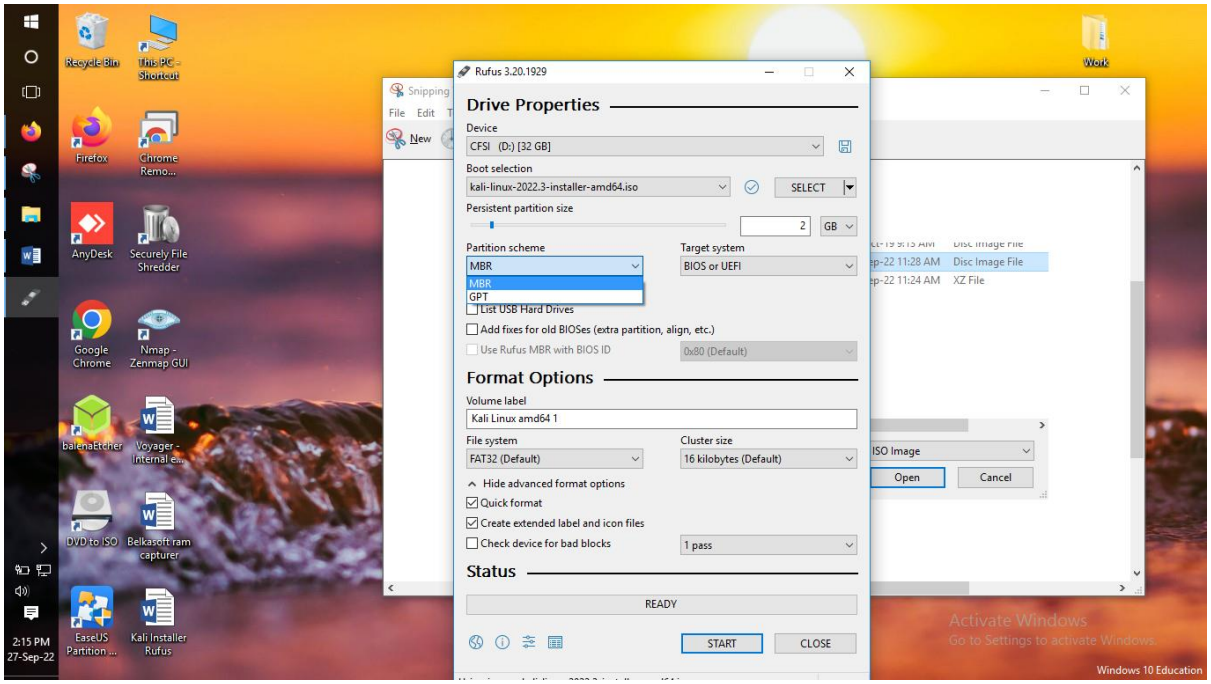

64
Everything
Includes every tool possible

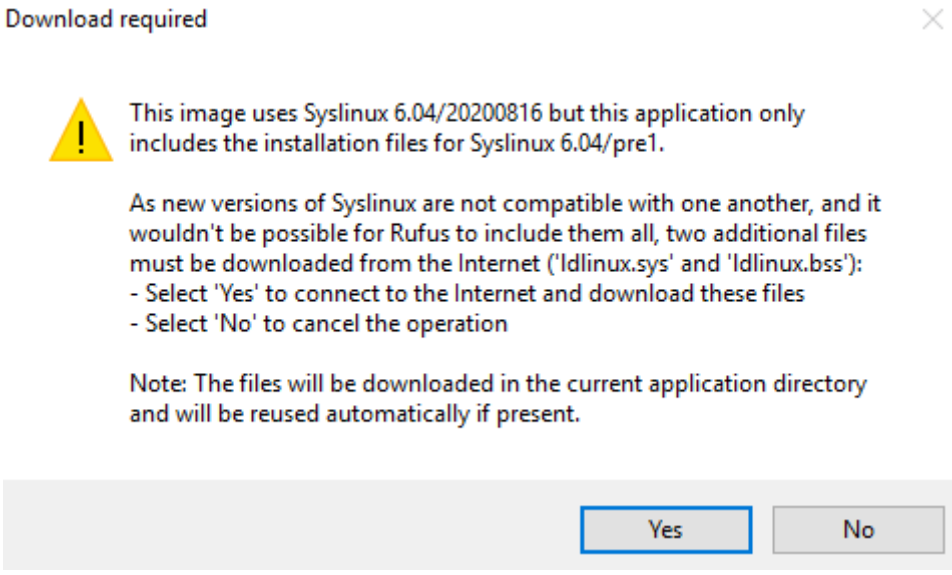

Load Transfer
kali-linux-2022.3-installer-everything-amd64.iso
10.6 GB in 1 file
Files
Trackers
Name
Bytes
Download
Priority
kali-linux-2022.3-installer-everything-amd64...
10.6 G
Normal
Select All
Ordered
Off
Low
Normal
High
Sequential
Auto
Local Files Location
Downloads
Change
Move On Complete
No Move On Complete
Change
Help
Settings
Start
Stop
Remove

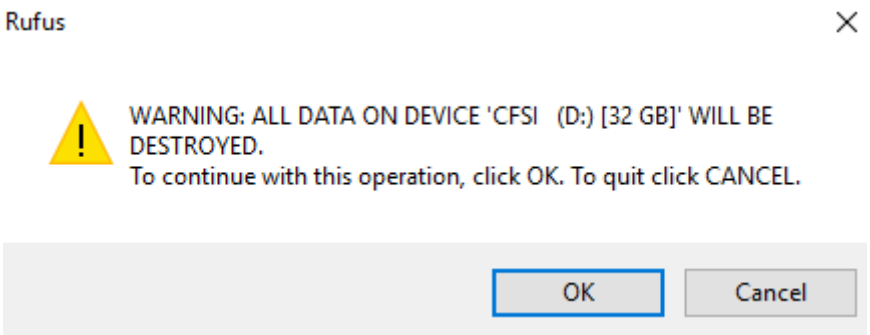

Name
Size
Type
kali-linux-2022.3-installer-amd64.iso
3,060,816 KB
Disc Image File
kali-linux-2022.3-installer-everything-amd64.iso
10,367,424 ...
Disc Image File
kali-linux-2022.3-installer-everything-amd64.iso.torrent
792 KB
torrent meta-file

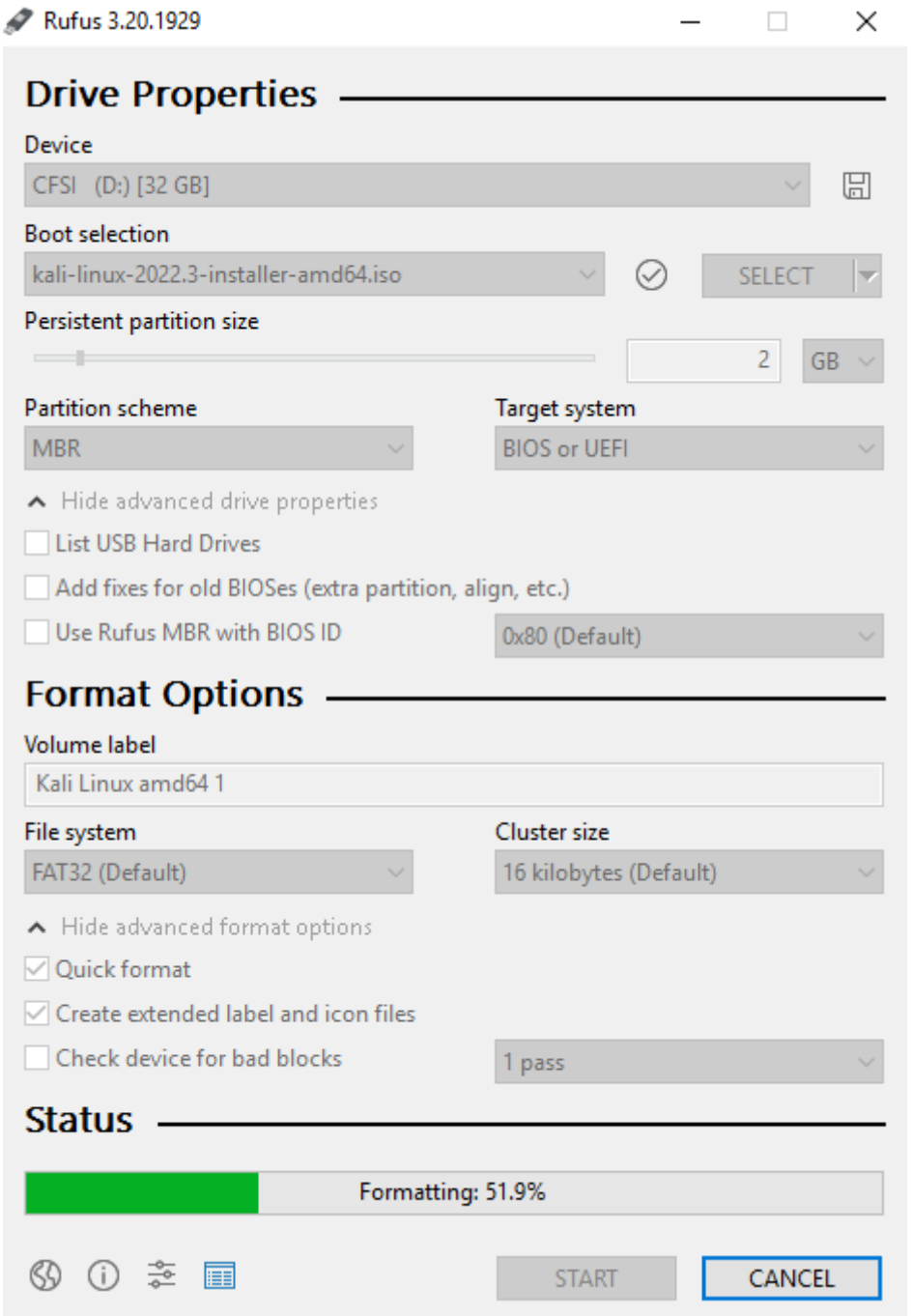

Rufus 3.20.1929
Drive Properties
Device
CFSI (D:) [32 GB]
Boot selection
Disk or ISO image (Please select)
SELECT
Partition scheme
MBR
Target system
BIOS (or UEFI-CSM)
Click to select or download an image...
Hide advanced drive properties
List USB Hard Drives
Add fixes for old BIOSes (extra partition, align, etc.)
Use Rufus MBR with BIOS ID
0x80 (Default)
Format Options
Volume label
CFSI
File system
FAT32 (Default)
Cluster size
16 kilobytes (Default)
Hide advanced format options
Quick format
Create extended label and icon files
Check device for bad blocks
1 pass
Status
READY
START
CLOSE
1 device found
Windows 10 Education

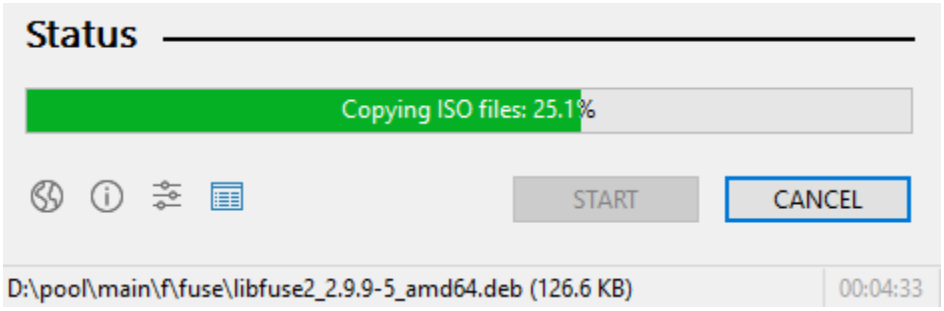

This PC
FW
isos
Leave
Local Disk (E:)
OneDrive
This PC
kali-linux-2022.3-installer-amd64
05-Sep-22 11:28 AM
Disc Image File
kali-linux-2022.3-raspberry-pi-armhf.img...
05-Sep-22 11:24 AM
XZ File
File name:
kali-linux-2022.3-installer-amd64
ISO Image
Open
Cancel

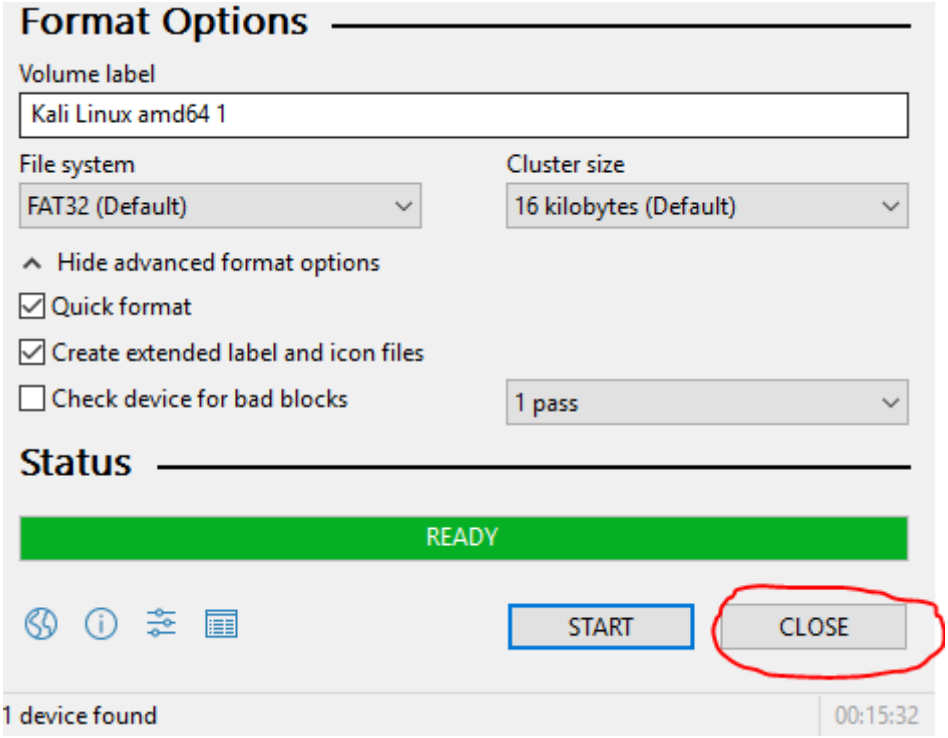

Rufus 3.20.1929
Drive Properties
Device
CFSI (D:) [32 GB]
Boot selection
kali-linux-2022.3-installer-amd64.iso
SELECT
Persistent partition size
Partition scheme
MBR
GPT
Target system
BIOS or UEFI
List USB Hard Drives
Add fixes for old BIOSes (extra partition, align, etc.)
Use Rufus MBR with BIOS ID
0x80 (Default)
Format Options
Volume label
Kali Linux amd64 1
File system
FAT32 (Default)
Cluster size
16 kilobytes (Default)
Hide advanced format options
Quick format
Create extended label and icon files
Check device for bad blocks
1 pass
Status
READY
START
CLOSE
Activate Windows
Windows 10 Education

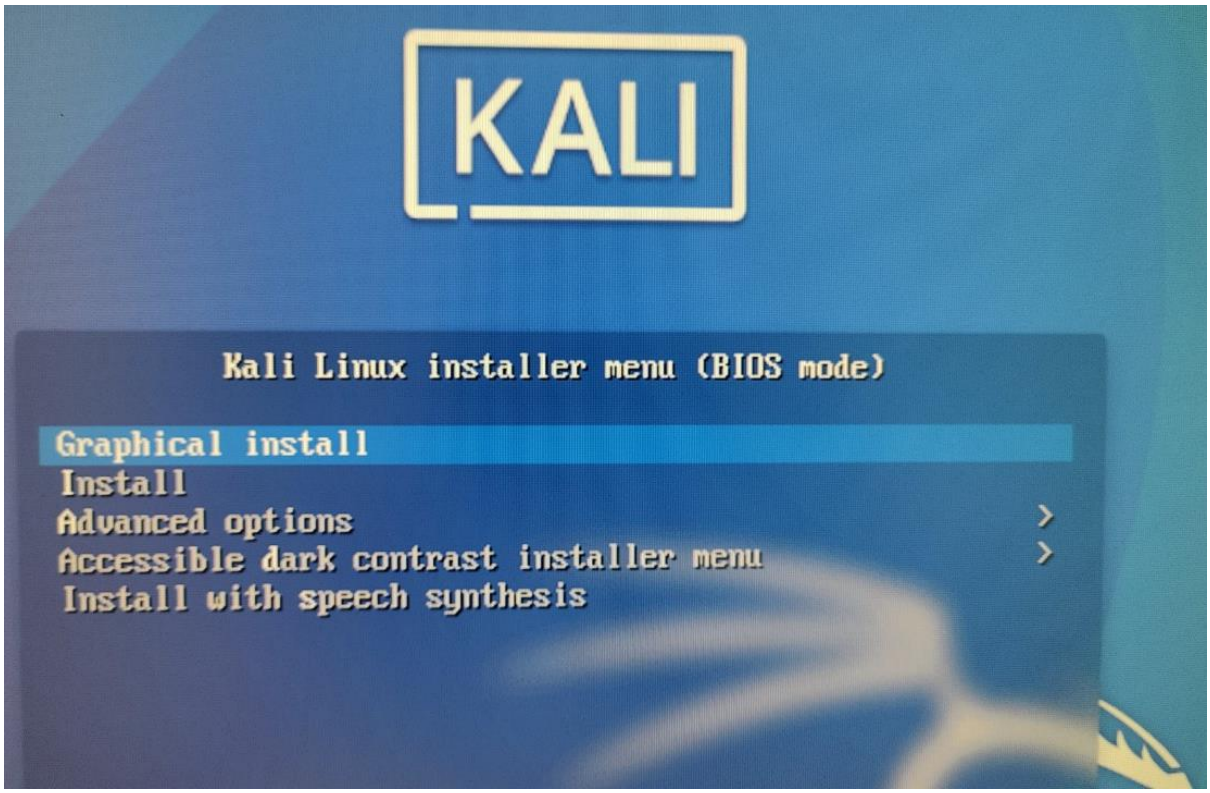

Download required
This image uses Syslinux 6.04/20200816 but this application only includes the installation files for Syslinux 6.04/pre1.
As new versions of Syslinux are not compatible with one another, and it wouldn't be possible for Rufus to include them all, two additional files must be downloaded from the Internet ('ldlinux.sys' and 'ldlinux.bss'):
- Select 'Yes' to connect to the Internet and download these files
- Select 'No' to cancel the operation
Note: The files will be downloaded in the current application directory and will be reused automatically if present.
Yes
No


Rufus
WARNING: ALL DATA ON DEVICE 'CFSI (D:) [32 GB]' WILL BE DESTROYED.
To continue with this operation, click OK. To quit click CANCEL.
OK
Cancel


Rufus 3.20.1929
Drive Properties
Device
CFSI (D:) [32 GB]
Boot selection
kali-linux-2022.3-installer-amd64.iso
SELECT
Persistent partition size
2
GB
Partition scheme
MBR
Target system
BIOS or UEFI
Hide advanced drive properties
List USB Hard Drives
Add fixes for old BIOSes (extra partition, align, etc.)
Use Rufus MBR with BIOS ID
0x80 (Default)
Format Options
Volume label
Kali Linux amd64 1
File system
FAT32 (Default)
Cluster size
16 kilobytes (Default)
Hide advanced format options
Quick format
Create extended label and icon files
Check device for bad blocks
1 pass
Status
Formatting: 51.9%
START
CANCEL


Status
Copying ISO files: 25.1%
START
CANCEL
D:\pool\main\f\fuse\libfuse2_2.9.9-5_amd64.deb (126.6 KB)
00:04:33


Format Options
Volume label
Kali Linux amd64 1
File system
FAT32 (Default)
Cluster size
16 kilobytes (Default)
Hide advanced format options
Quick format
Create extended label and icon files
Check device for bad blocks
1 pass
Status
READY
START
CLOSE
1 device found
00:15:32


KALI
Kali Linux installer menu (BIOS mode)
Graphical install
Install
Advanced options
Accessible dark contrast installer menu
Install with speech synthesis

VirtualBox 7.0.6 platform packages

- Windows hosts
- macOS / Intel hosts
- Developer preview for macOS / Arm64 (M1/M2) hosts
- Linux distributions
- Solaris hosts
- Solaris 11 IPS hosts

The binaries are released under the terms of the GPL version 3.

See the changelog for what has changed.

You might want to compare the checksums to verify the integrity of downloaded packages.

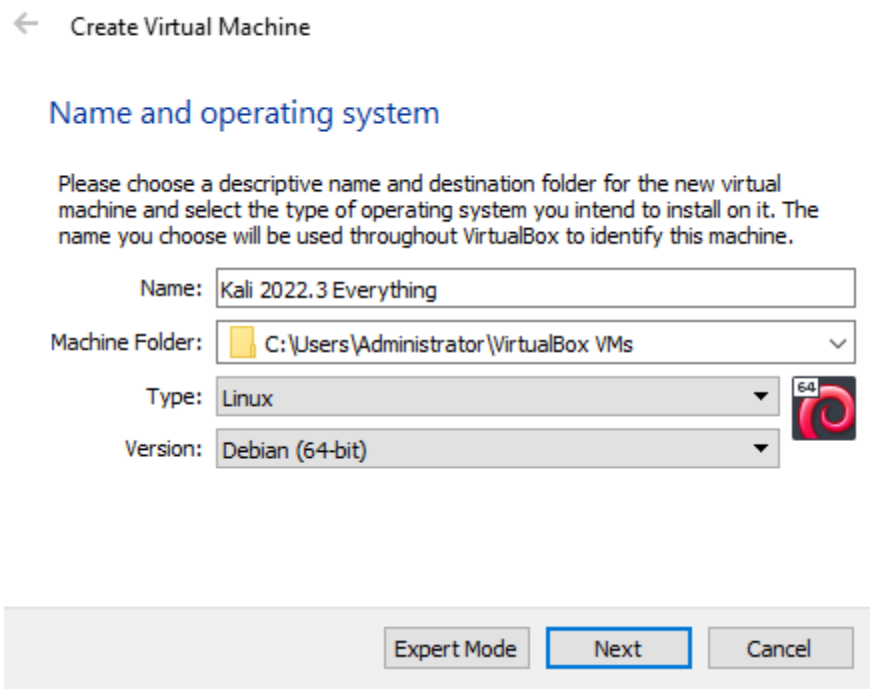
The SHA256 checksums should be favored as the MD5 algorithm must be treated as insecure!

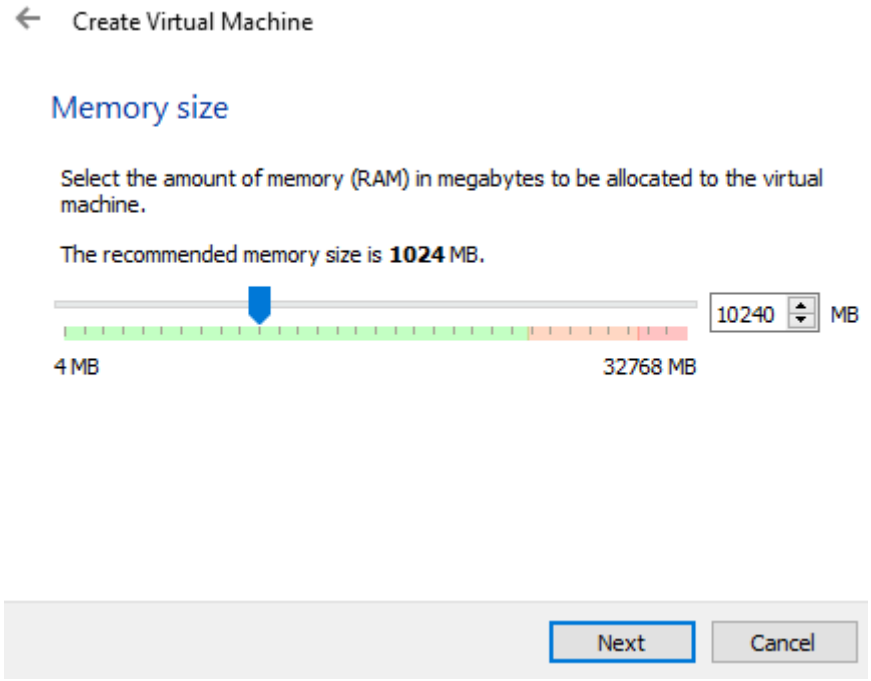
- SHA256 checksums, MD5 checksums

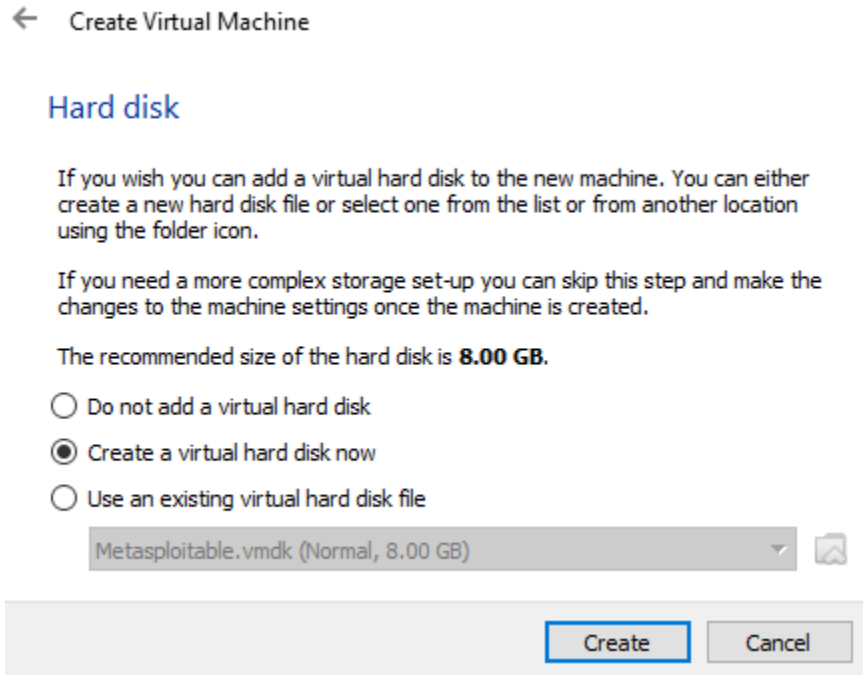
Note: After upgrading VirtualBox it is recommended to upgrade the guest additions as well.

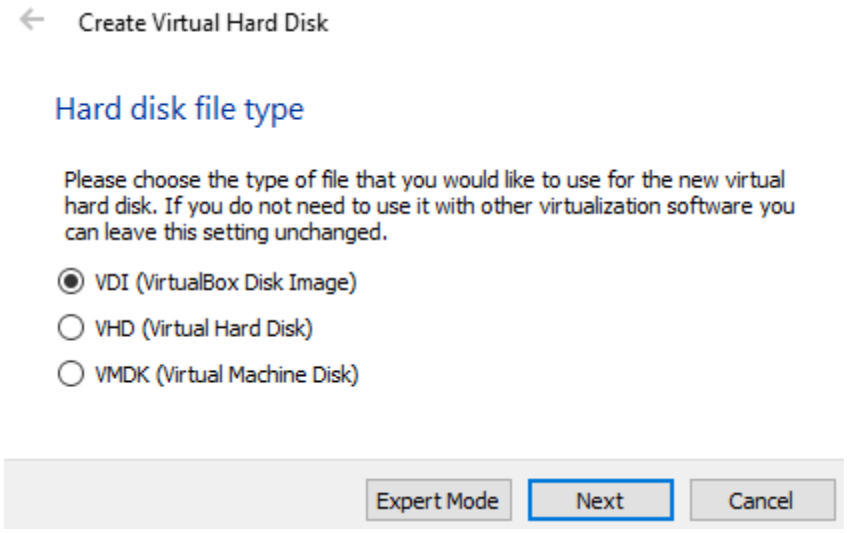
VirtualBox 7.0.6 Oracle VM VirtualBox Extension Pack

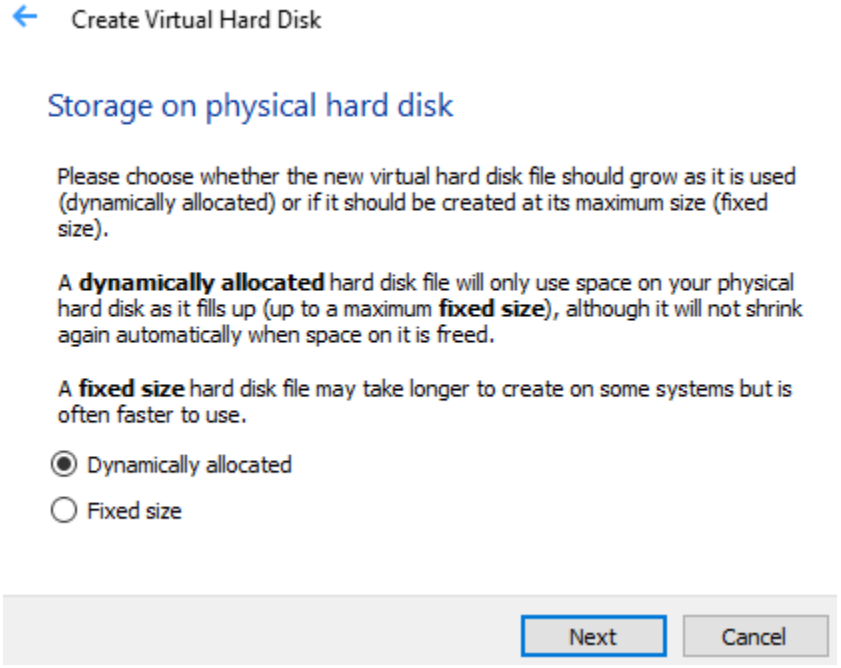
- All supported platforms

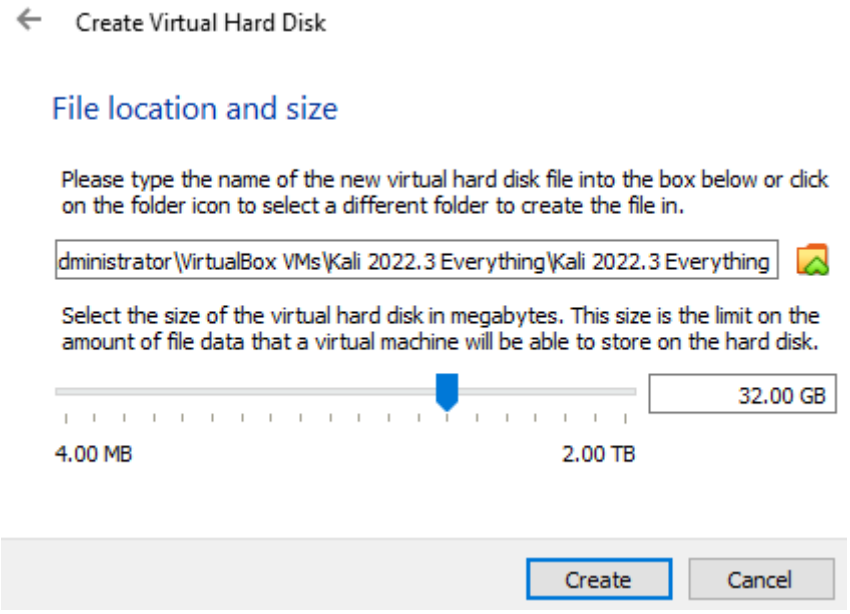


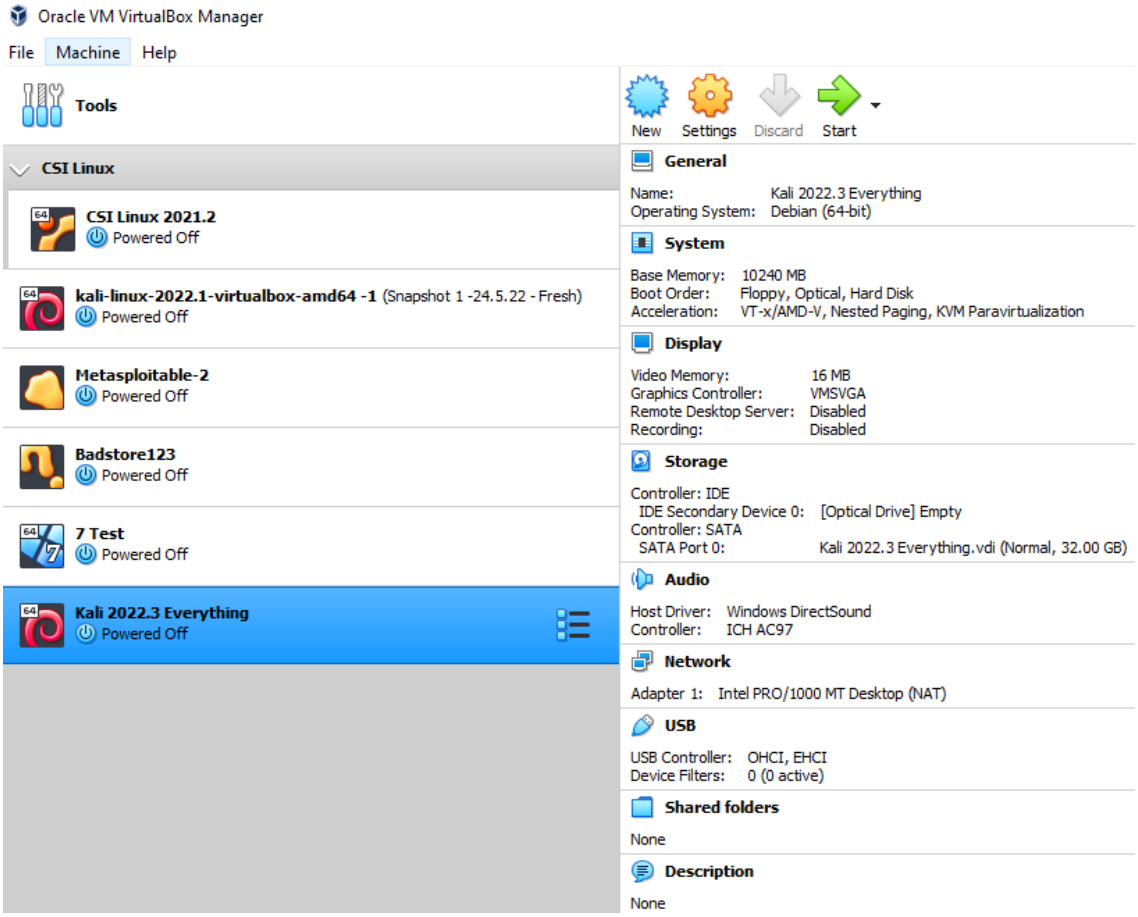

Create Virtual Machine
Memory size
Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.
The recommended memory size is 1024 MB.
10240
MB
4 MB
32768 MB
Next
Cancel

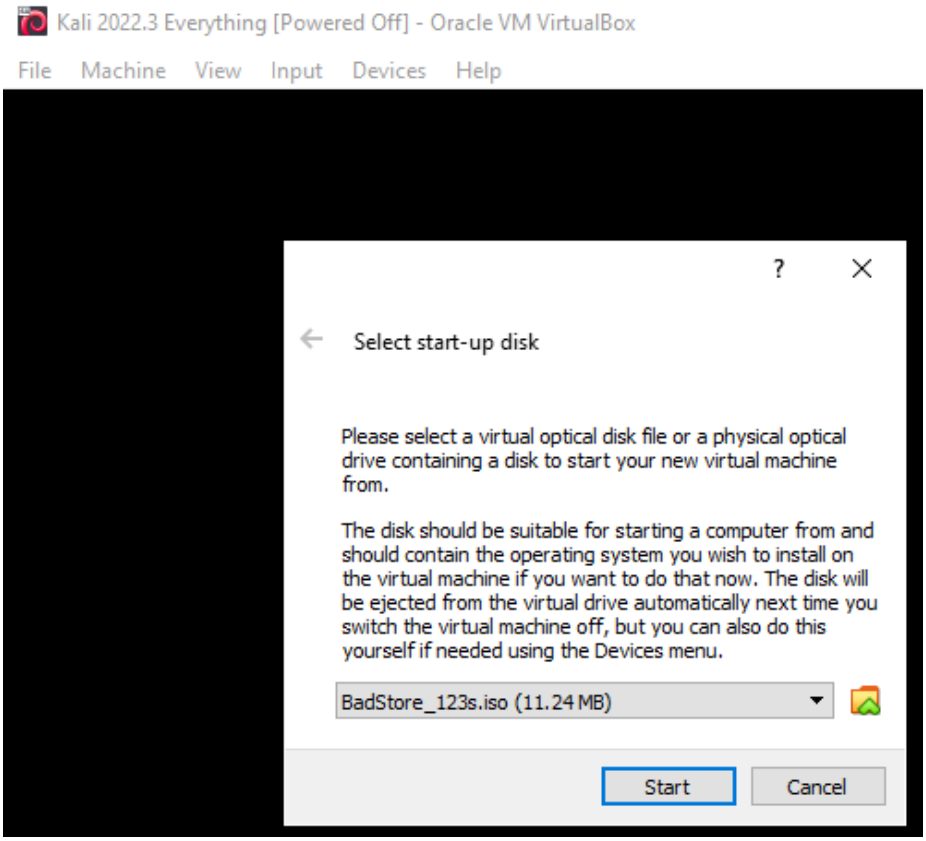

Create Virtual Machine
Hard disk
If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.
If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.
The recommended size of the hard disk is 8.00 GB.
Do not add a virtual hard disk
Create a virtual hard disk now
Use an existing virtual hard disk file
Metasploitable.vmdk (Normal, 8.00 GB)
Create
Cancel

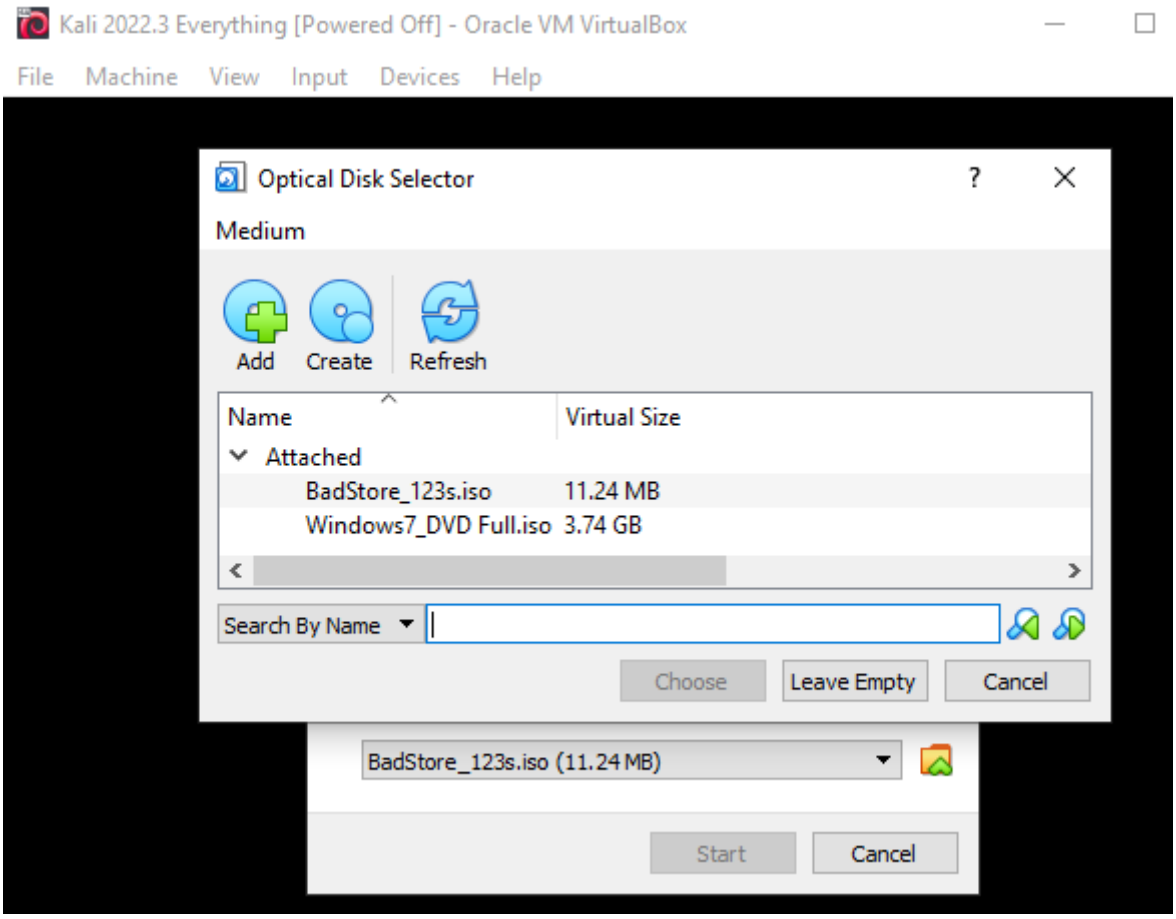

Create Virtual Hard Disk
Hard disk file type
Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.
VDI (VirtualBox Disk Image)
VHD (Virtual Hard Disk)
VMDK (Virtual Machine Disk)
Expert Mode
Next
Cancel

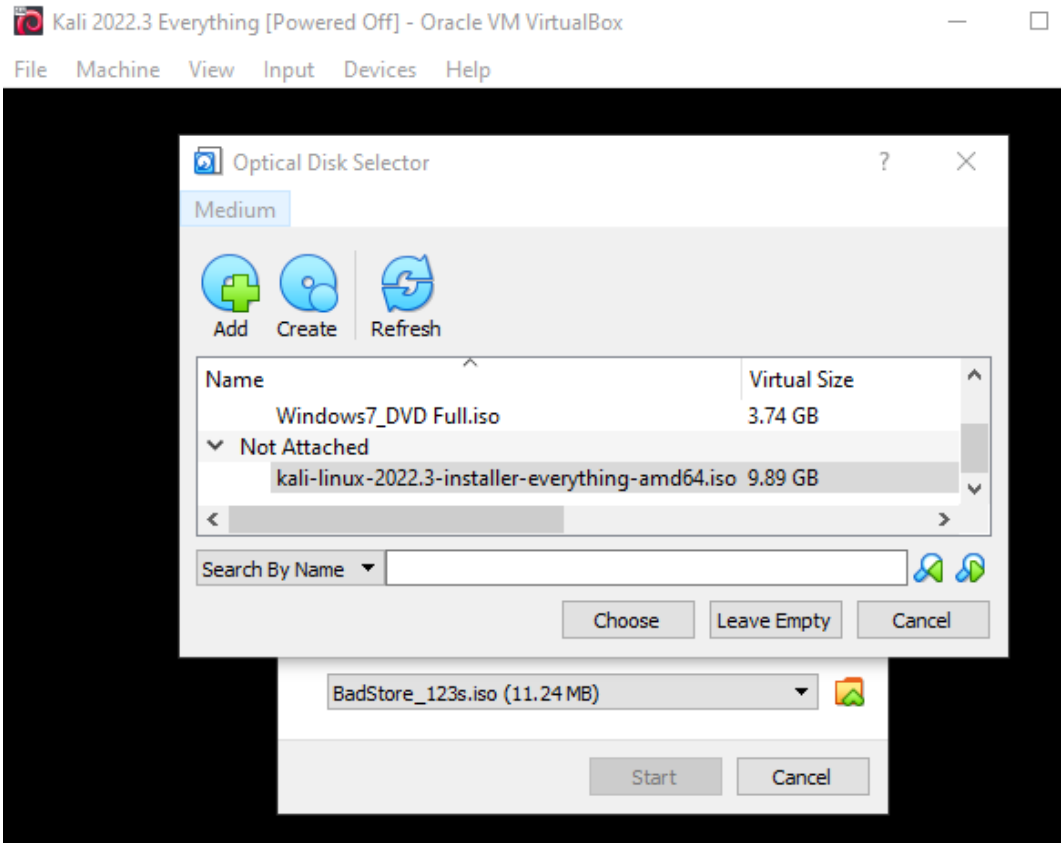

Create Virtual Hard Disk
Storage on physical hard disk
Please choose whether the new virtual hard disk file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).
A dynamically allocated hard disk file will only use space on your physical hard disk as it fills up (up to a maximum fixed size), although it will not shrink again automatically when space on it is freed.
A fixed size hard disk file may take longer to create on some systems but is often faster to use.
Dynamically allocated
Fixed size
Next
Cancel

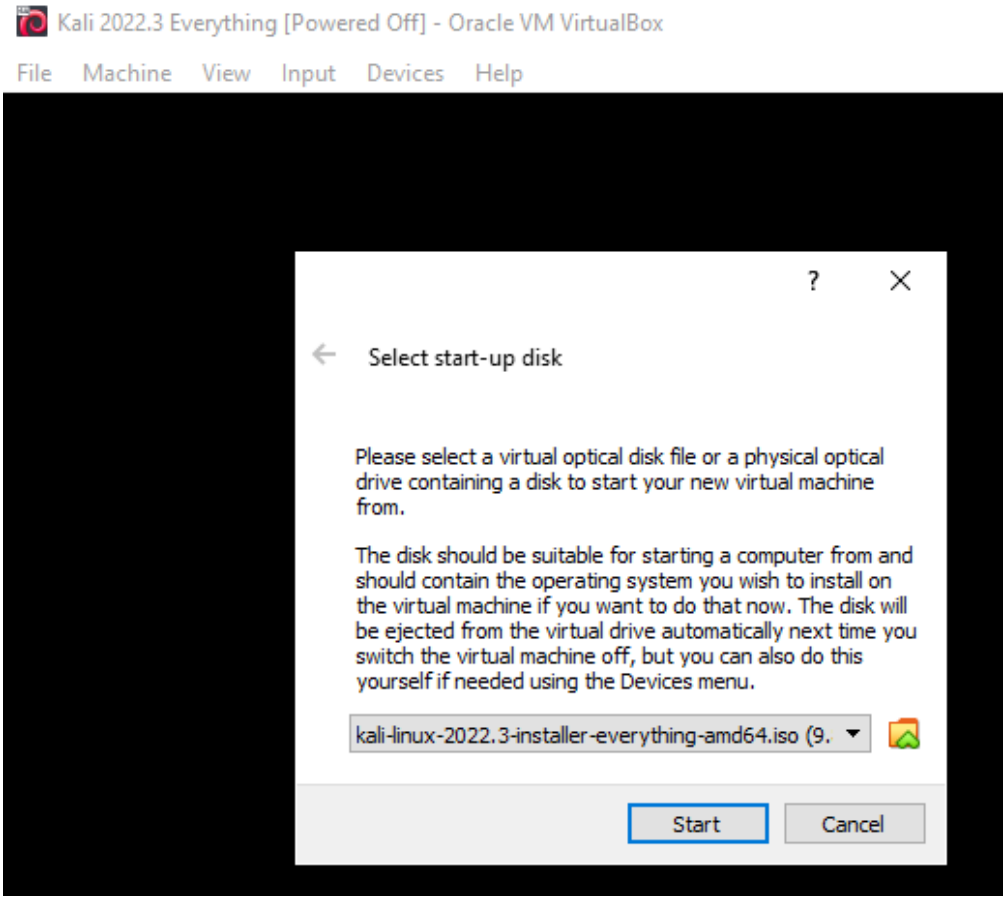

Create Virtual Hard Disk
File location and size
Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.
dministrator\VirtualBox VMs\Kali 2022.3 Everything\Kali 2022.3 Everything
Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.
32.00 GB
4.00 MB
2.00 TB
Create
Cancel

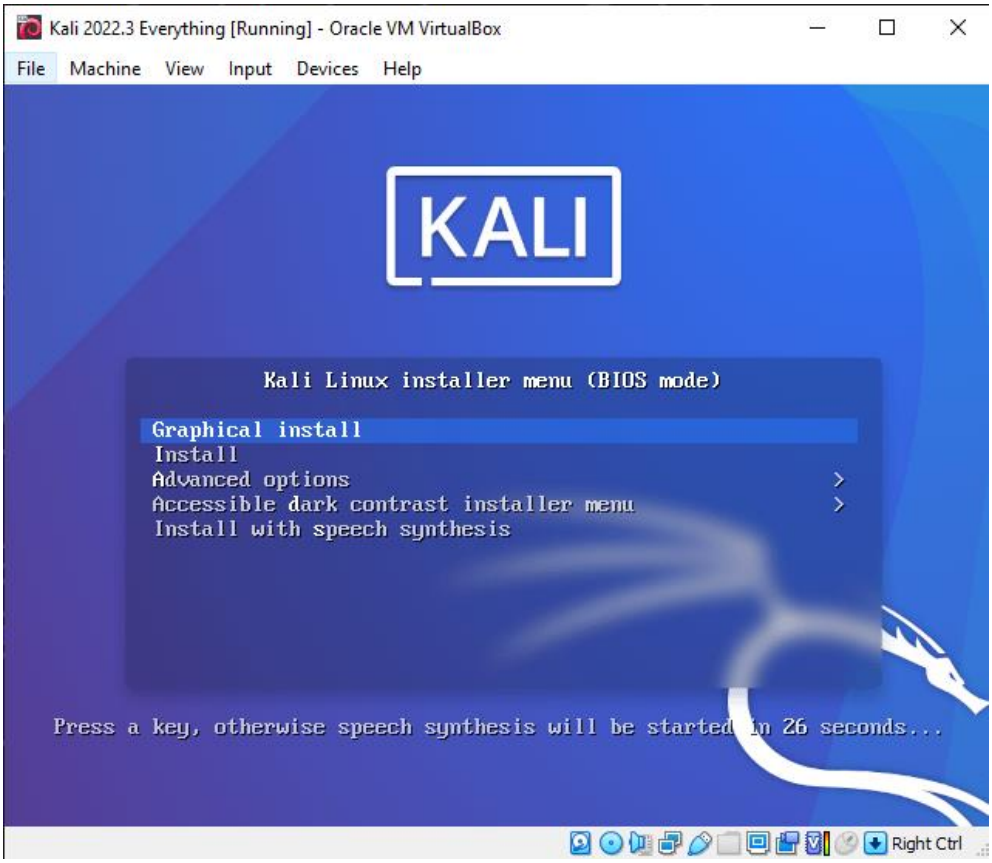

Oracle VM VirtualBox Manager
File
Machine
Help
Tools
CSI Linux
CSI Linux 2021.2
Powered Off
kali-linux-2022.1-virtualbox-amd64 -1 (Snapshot 1 -24.5.22 - Fresh)
Powered Off
Metasploitable-2
Powered Off
Badstore123
Powered Off
7 Test
Powered Off
Kali 2022.3 Everything
Powered Off
New
Settings
Discard
Start
General
Name: Kali 2022.3 Everything
Operating System: Debian (64-bit)
System
Base Memory: 10240 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization
Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Kali 2022.3 Everything.vdi (Normal, 32.00 GB)
Audio
Host Driver: Windows DirectSound
Controller: ICH AC97
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)
USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)
Shared folders
None
Description
None

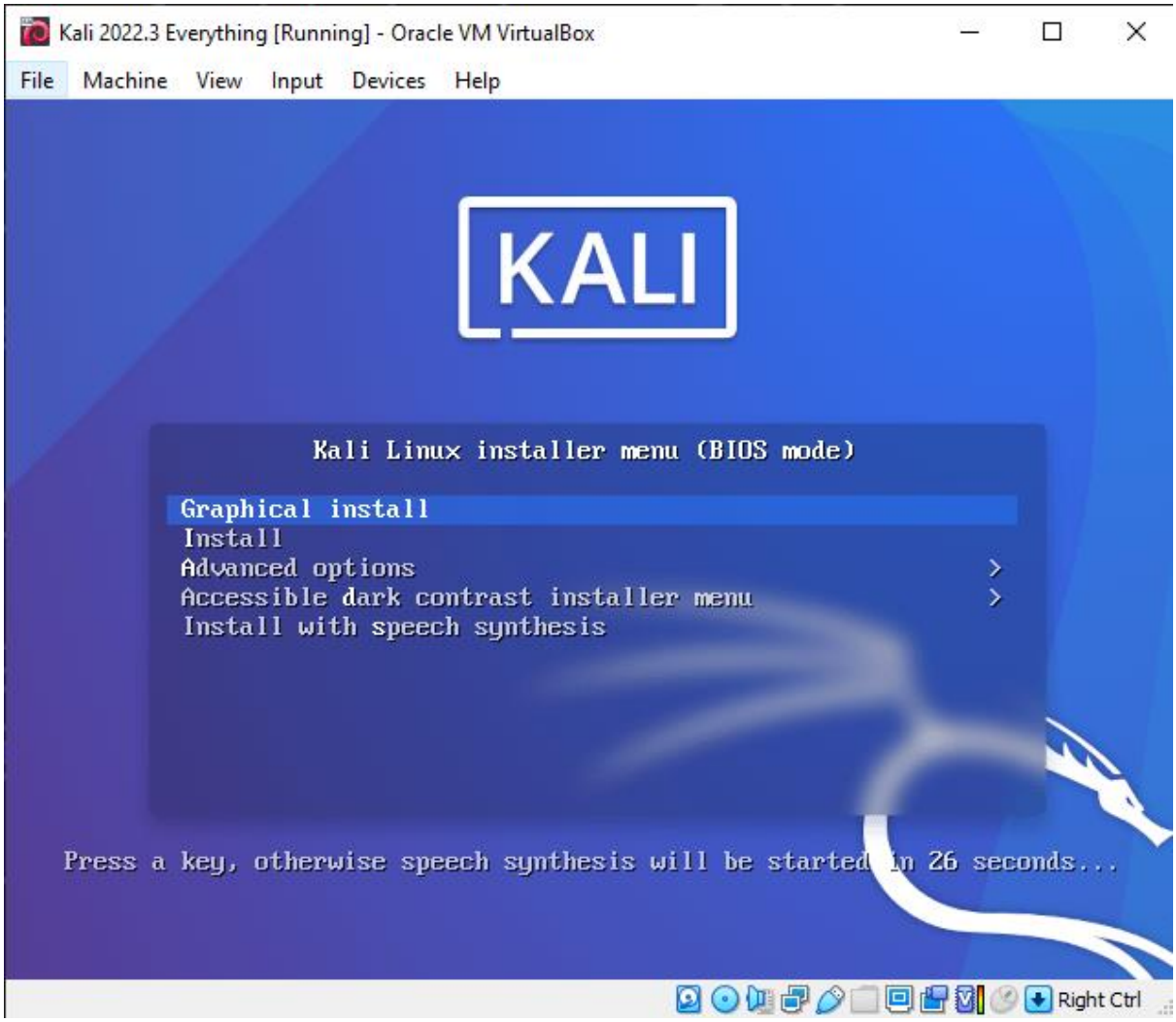

Kali 2022.3 Everything [Powered Off] - Oracle VM VirtualBox
File Machine View Input Devices Help
Select start-up disk
Please select a virtual optical disk file or a physical optical drive containing a disk to start your new virtual machine from.
The disk should be suitable for starting a computer from and should contain the operating system you wish to install on the virtual machine if you want to do that now. The disk will be ejected from the virtual drive automatically next time you switch the virtual machine off, but you can also do this yourself if needed using the Devices menu.
BadStore_123s.iso (11.24 MB)
Start
Cancel

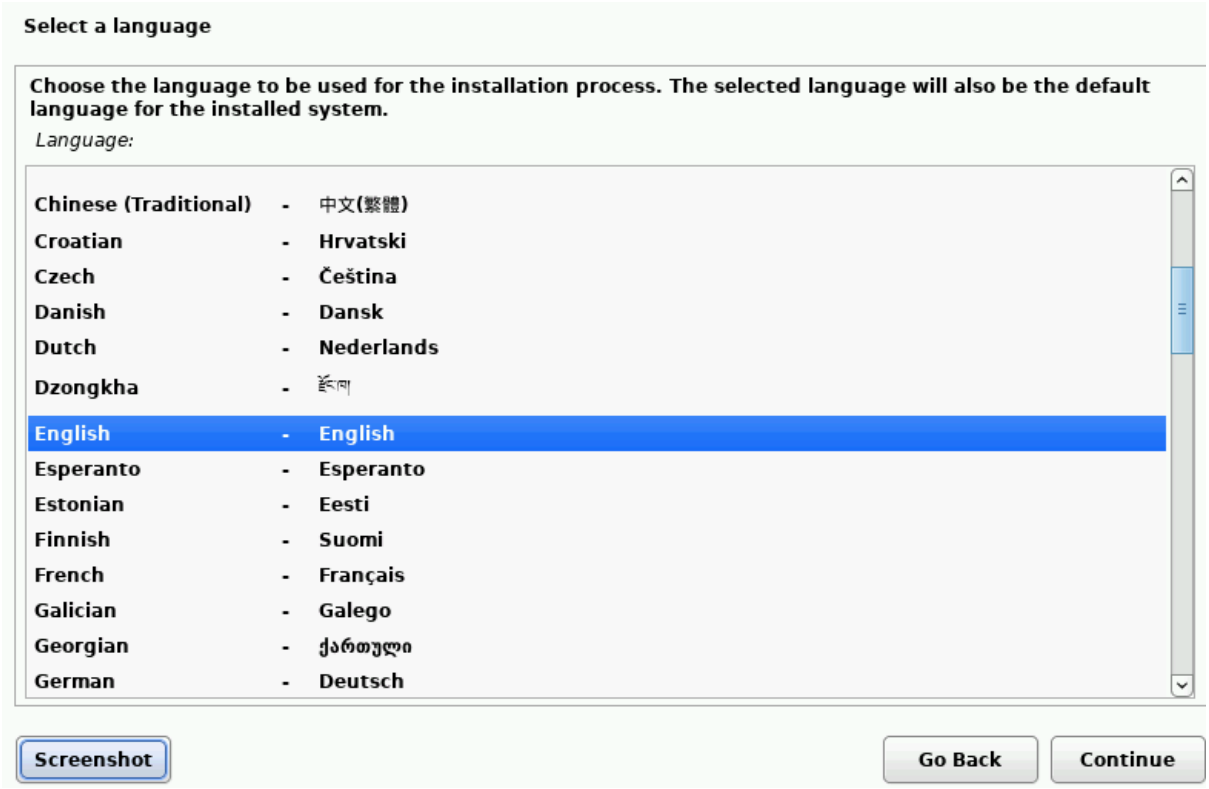

Kali 2022.3 Everything [Powered Off] - Oracle VM VirtualBox
File Machine View Input Devices Help
Optical Disk Selector
Medium
Add
Create
Refresh
Name
Virtual Size
Attached
BadStore_123s.iso 11.24 MB
Windows7_DVD Full.iso 3.74 GB
Search By Name
Choose
Leave Empty
Cancel
BadStore_123s.iso (11.24 MB)
Start
Cancel

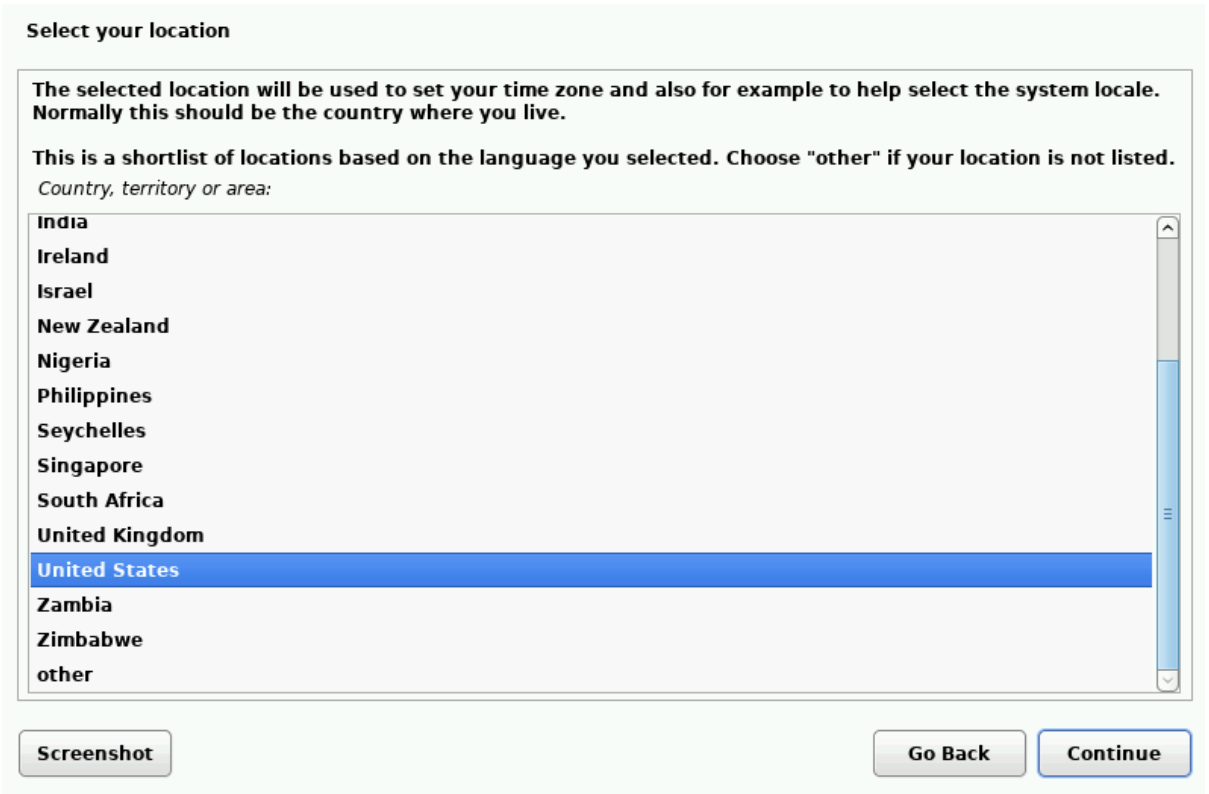

Kali 2022.3 Everything [Powered Off] - Oracle VM VirtualBox
File Machine View Input Devices Help
Optical Disk Selector
Medium
Add
Create
Refresh
Name
Virtual Size
Windows7_DVD Full.iso
3.74 GB
Not Attached
kali-linux-2022.3-installer-everything-amd64.iso
9.89 GB
Search By Name
Choose
Leave Empty
Cancel
BadStore_123s.iso (11.24 MB)
Start
Cancel

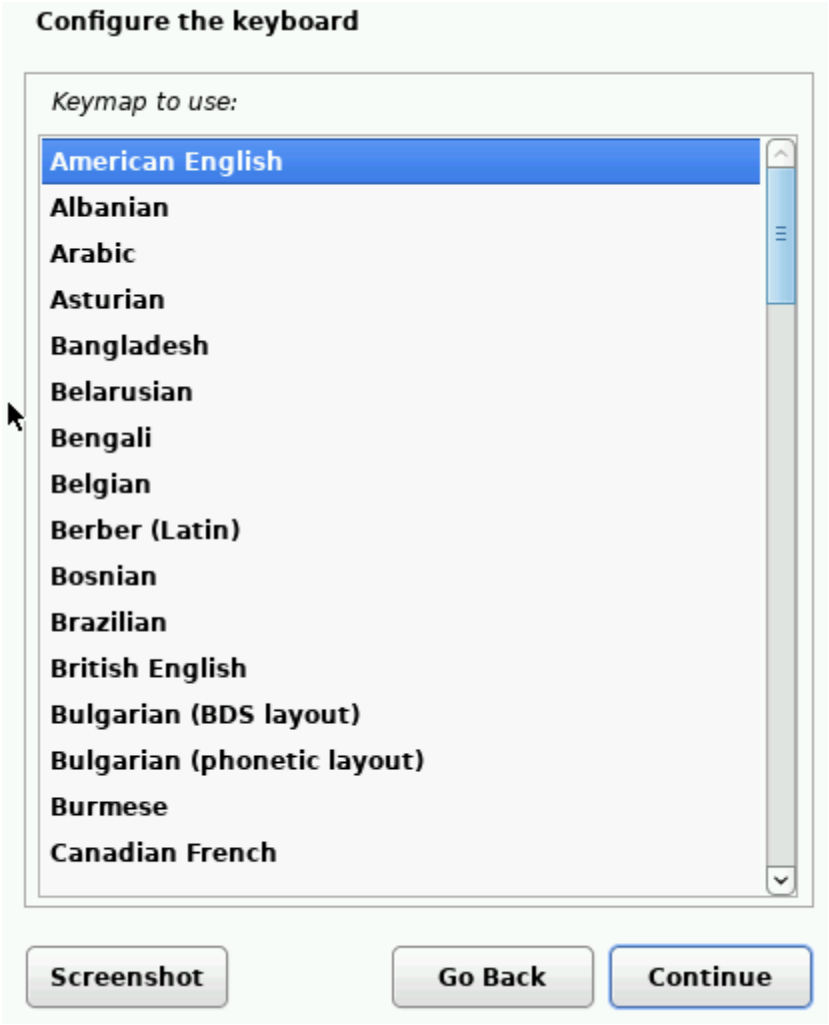

Kali 2022.3 Everything [Powered Off] - Oracle VM VirtualBox
File Machine View Input Devices Help
Select start-up disk
Please select a virtual optical disk file or a physical optical drive containing a disk to start your new virtual machine from.
The disk should be suitable for starting a computer from and should contain the operating system you wish to install on the virtual machine if you want to do that now. The disk will be ejected from the virtual drive automatically next time you switch the virtual machine off, but you can also do this yourself if needed using the Devices menu.
kali-linux-2022.3-installer-everything-amd64.iso (9.
Start
Cancel

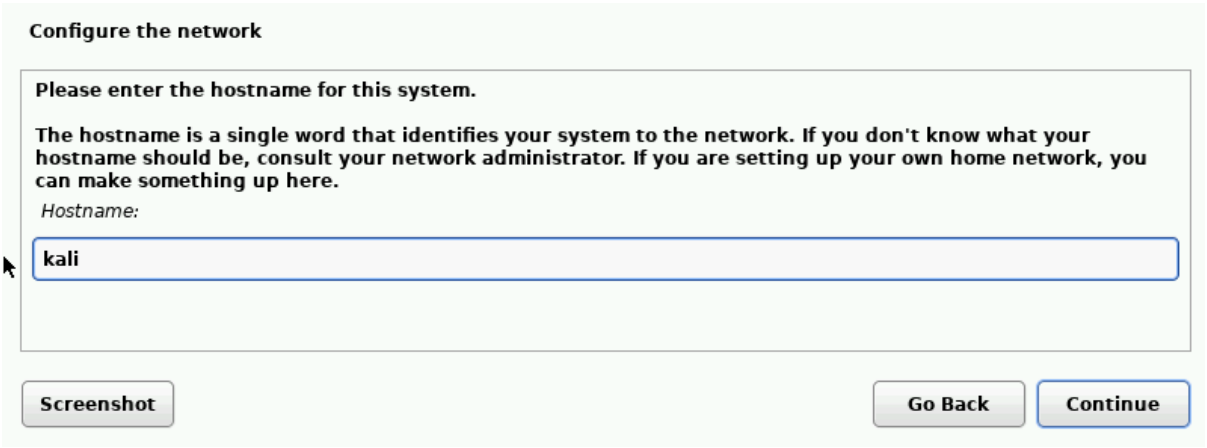

Kali 2022.3 Everything [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Kali Linux installer menu (BIOS mode)
Graphical install
Install
Advanced options
Accessible dark contrast installer menu
Install with speech synthesis
Press a key, otherwise speech synthesis will be started in 26 seconds...
Right Ctrl

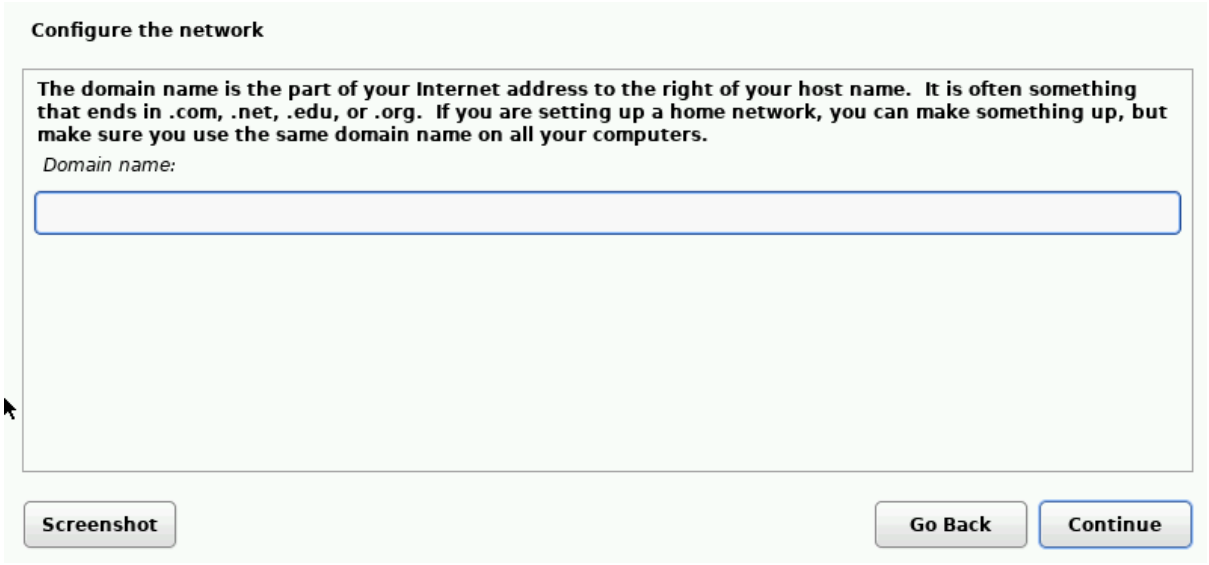

Kali 2022.3 Everything [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Kali Linux installer menu (BIOS mode)
Graphical install
Install
Advanced options >
Accessible dark contrast installer menu >
Install with speech synthesis
Press a key, otherwise speech synthesis will be started in 26 seconds...
Right Ctrl

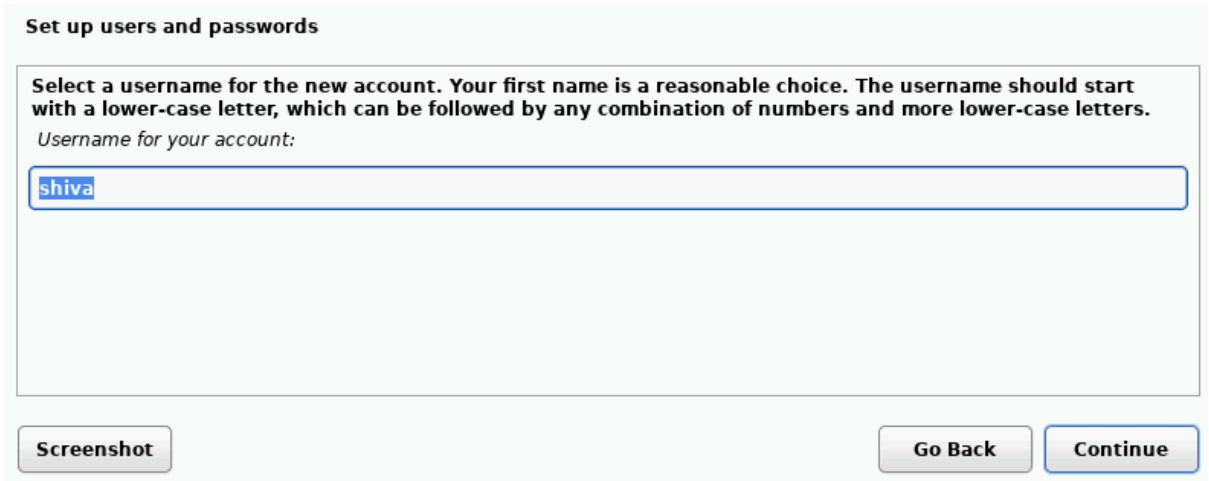

Select a language
Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.
Language:
Chinese (Traditional) - 中文(繁體)
Croatian - Hrvatski
Czech - Čeština
Danish - Dansk
Dutch - Nederlands
Dzongkha - རྫོང་ཁ
English - English
Esperanto - Esperanto
Estonian - Eesti
Finnish - Suomi
French - Français
Galician - Galego
Georgian - ქართული
German - Deutsch
Screenshot
Go Back
Continue

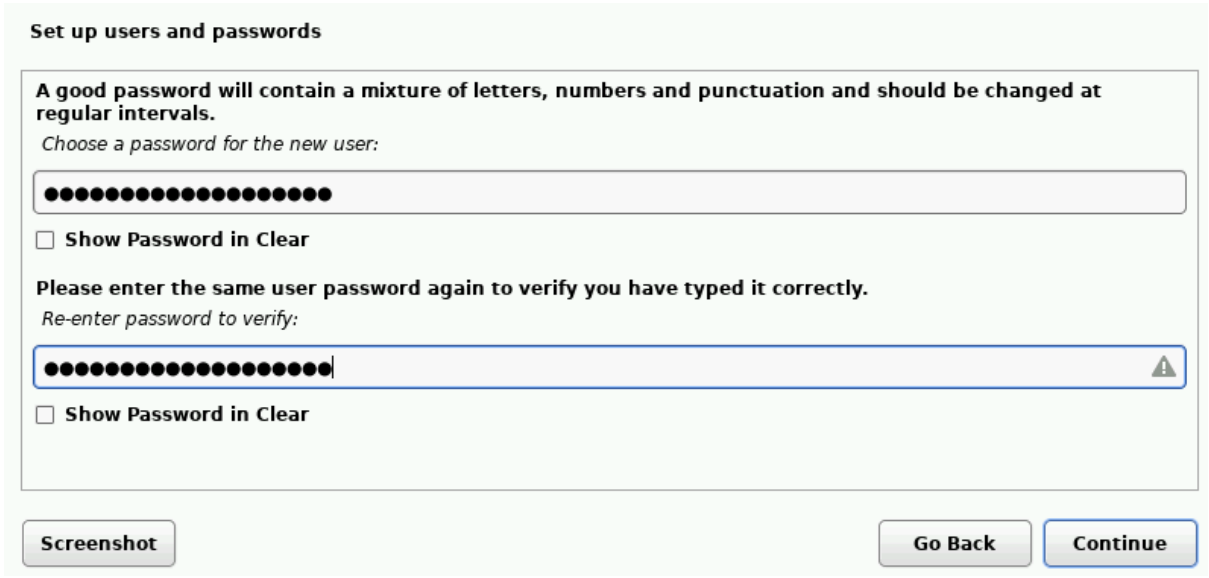

Select your location
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.
This is a shortlist of locations based on the language you selected. Choose "other" if your location is not listed.
Country, territory or area:
India
Ireland
Israel
New Zealand
Nigeria
Philippines
Seychelles
Singapore
South Africa
United Kingdom
United States
Zambia
Zimbabwe
other
Screenshot
Go Back
Continue


Configure the keyboard
Keymap to use:
American English
Albanian
Arabic
Asturian
Bangladesh
Belarusian
Bengali
Belgian
Berber (Latin)
Bosnian
Brazilian
British English
Bulgarian (BDS layout)
Bulgarian (phonetic layout)
Burmese
Canadian French
Screenshot
Go Back
Continue

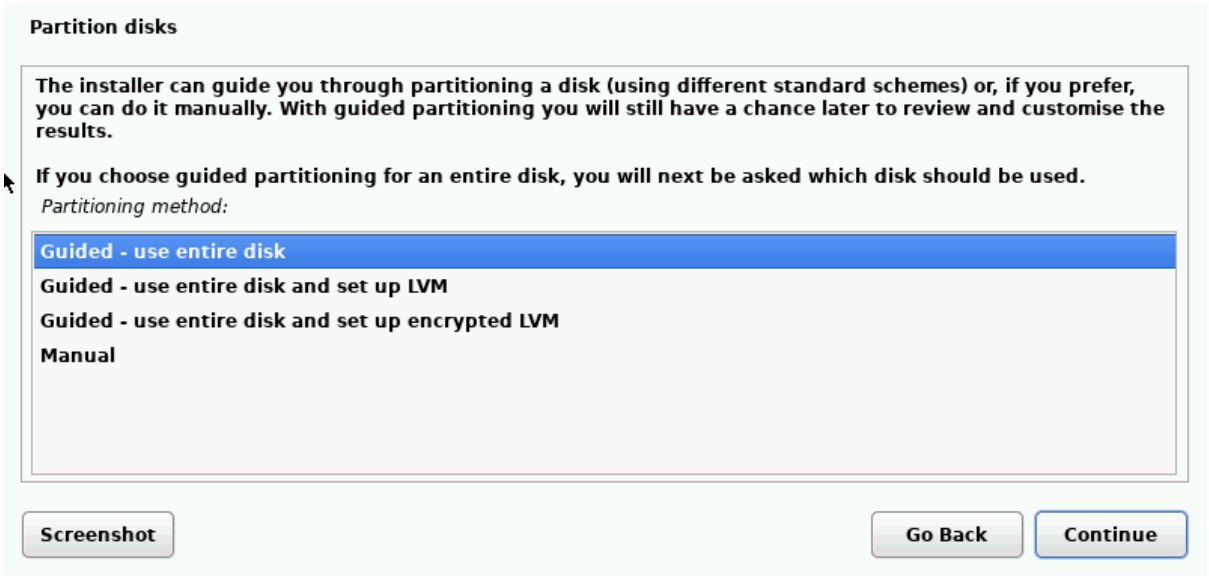

Configure the network
Please enter the hostname for this system.
The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.
Hostname:
kali
Screenshot
Go Back
Continue

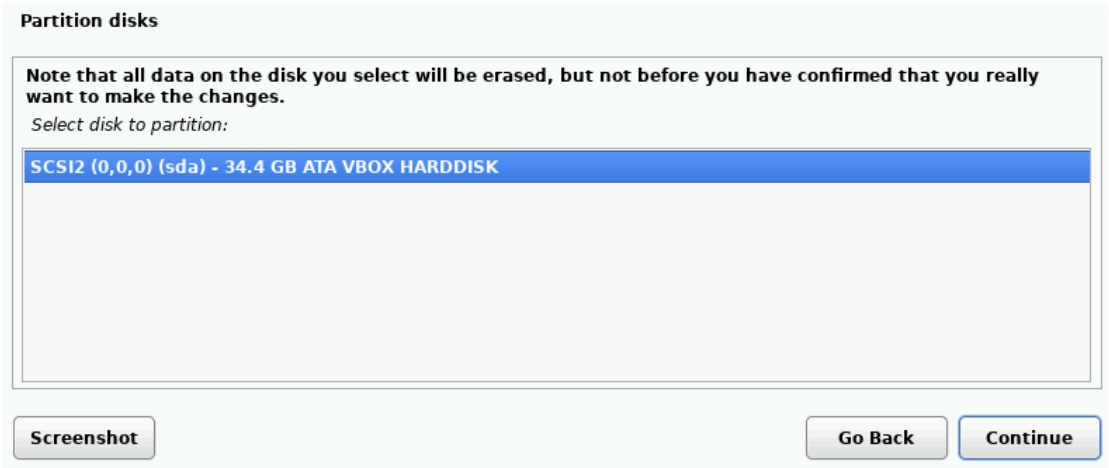

Configure the network
The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers.
Domain name:
Screenshot
Go Back
Continue

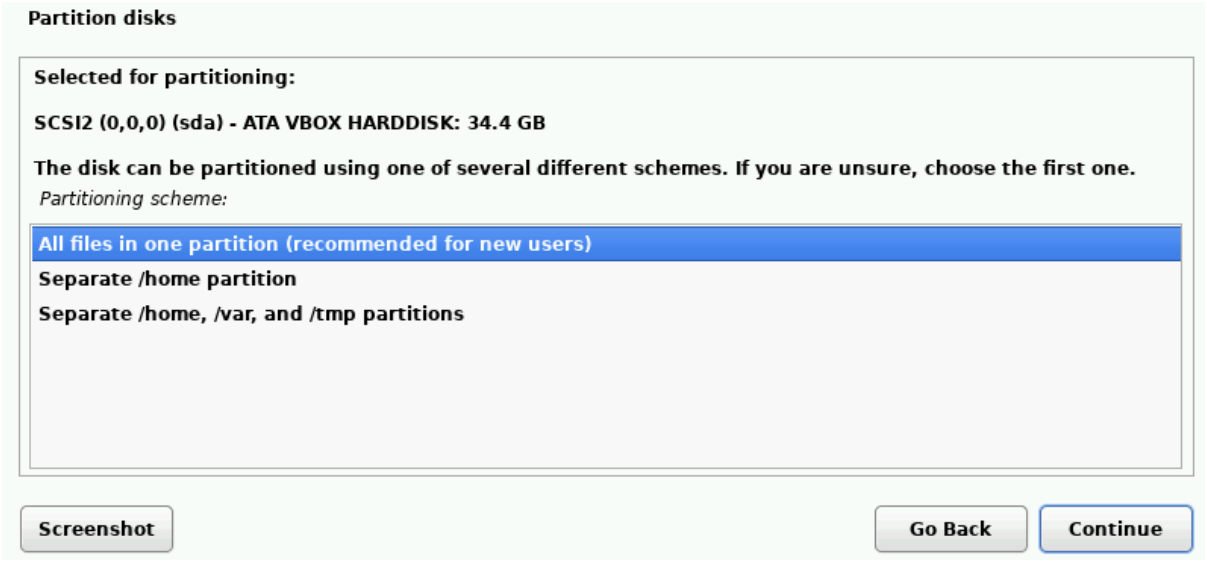

Set up users and passwords
Select a username for the new account. Your first name is a reasonable choice. The username should start with a lower-case letter, which can be followed by any combination of numbers and more lower-case letters.
Username for your account:
shiva
Screenshot
Go Back
Continue

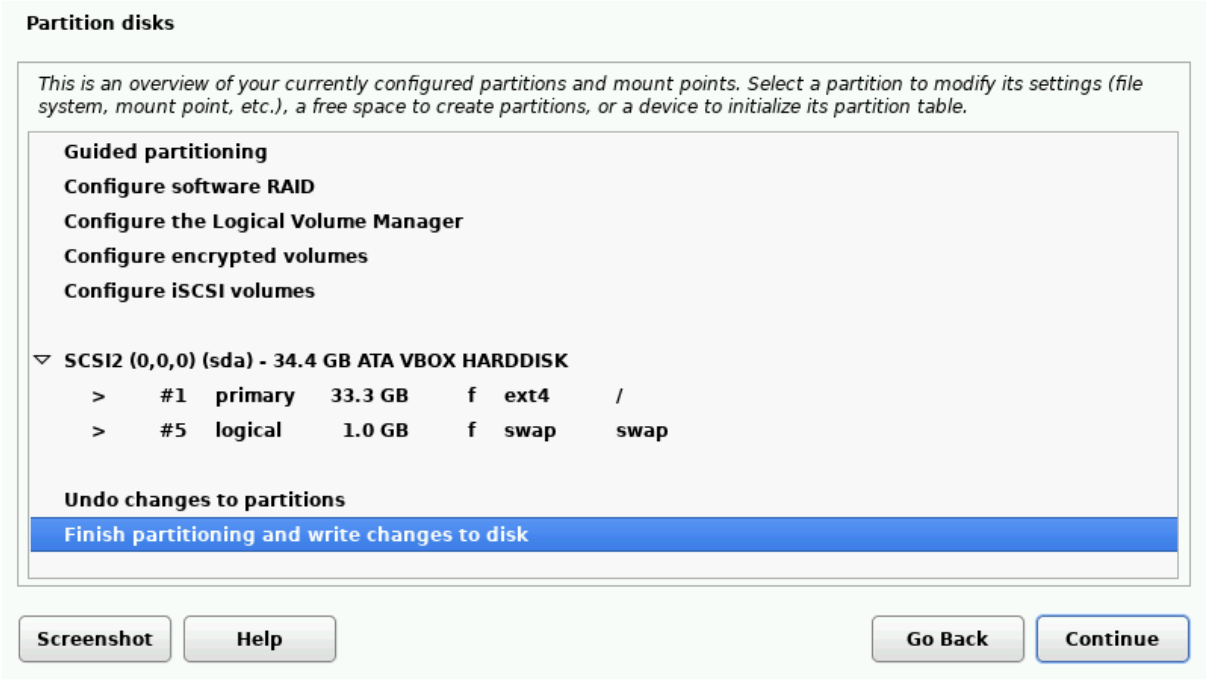

Set up users and passwords
A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.
Choose a password for the new user:
Show Password in Clear
Please enter the same user password again to verify you have typed it correctly.
Re-enter password to verify:
Show Password in Clear
Screenshot
Go Back
Continue

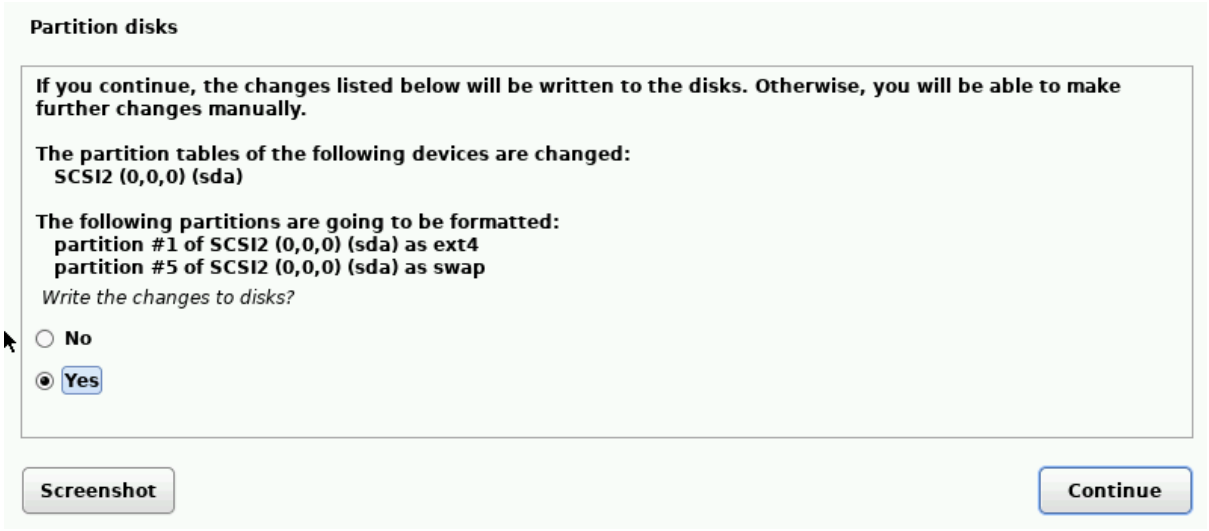

Configure the clock
If the desired time zone is not listed, then please go back to the step "Choose language" and select a country that uses the desired time zone (the country where you live or are located).
Select your time zone:
Eastern
Central
Mountain
Pacific
Alaska
Hawaii
Arizona
East Indiana
Samoa
Screenshot
Go Back
Continue


Partition disks
The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.
If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.
Partitioning method:
Guided - use entire disk
Guided - use entire disk and set up LVM
Guided - use entire disk and set up encrypted LVM
Manual
Screenshot
Go Back
Continue

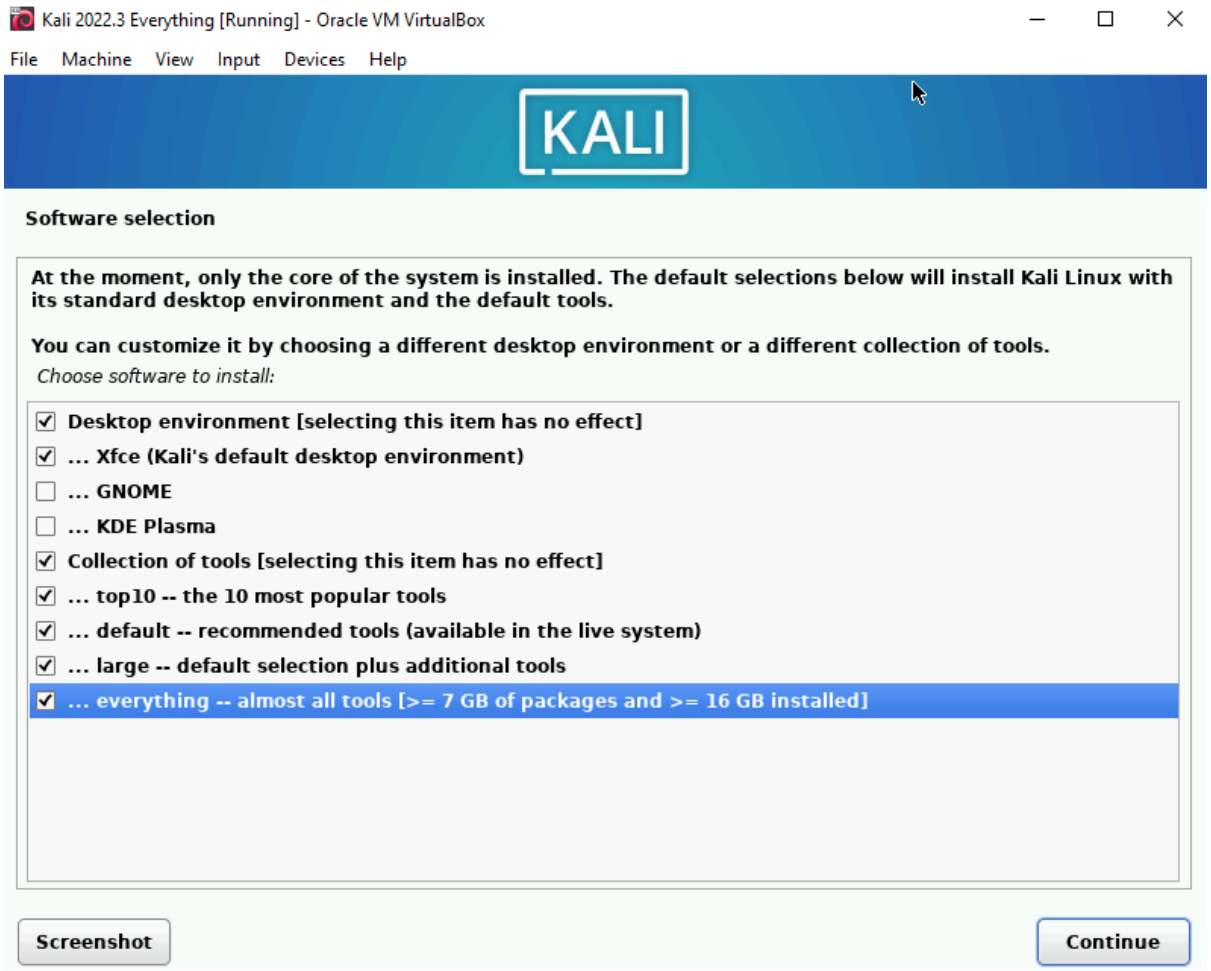

Partition disks
Note that all data on the disk you select will be erased, but not before you have confirmed that you really want to make the changes.
Select disk to partition:
SCSI2 (0,0,0) (sda) - 34.4 GB ATA VBOX HARDDISK
Screenshot
Go Back
Continue


Partition disks
Selected for partitioning:
SCSI2 (0,0,0) (sda) - ATA VBOX HARDDISK: 34.4 GB
The disk can be partitioned using one of several different schemes. If you are unsure, choose the first one.
Partitioning scheme:
All files in one partition (recommended for new users)
Separate /home partition
Separate /home, /var, and /tmp partitions
Screenshot
Go Back
Continue

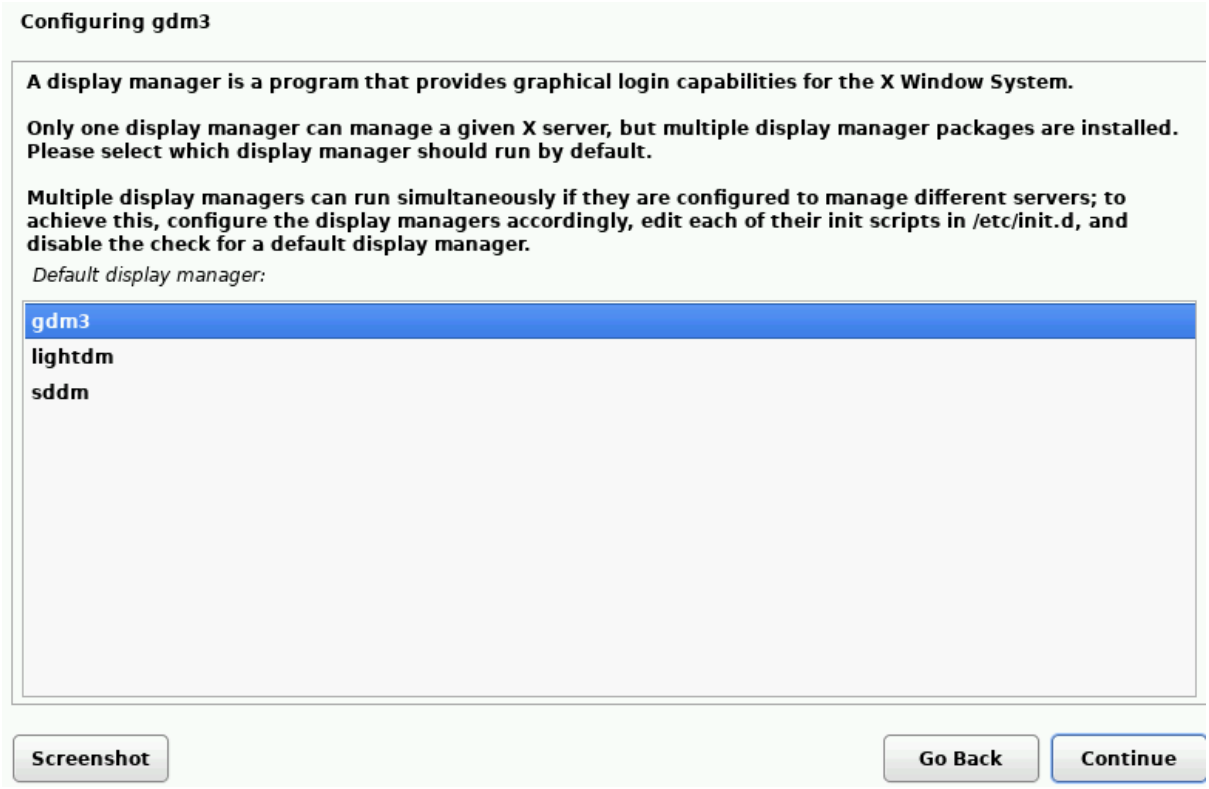

Partition disks
This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.
Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes
SCSI2 (0,0,0) (sda) - 34.4 GB ATA VBOX HARDDISK
> #1 primary 33.3 GB f ext4 /
> #5 logical 1.0 GB f swap swap
Undo changes to partitions
Finish partitioning and write changes to disk
Screenshot
Help
Go Back
Continue


Partition disks
If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.
The partition tables of the following devices are changed:
SCSI2 (0,0,0) (sda)
The following partitions are going to be formatted:
partition #1 of SCSI2 (0,0,0) (sda) as ext4
partition #5 of SCSI2 (0,0,0) (sda) as swap
Write the changes to disks?
No
Yes
Screenshot
Continue

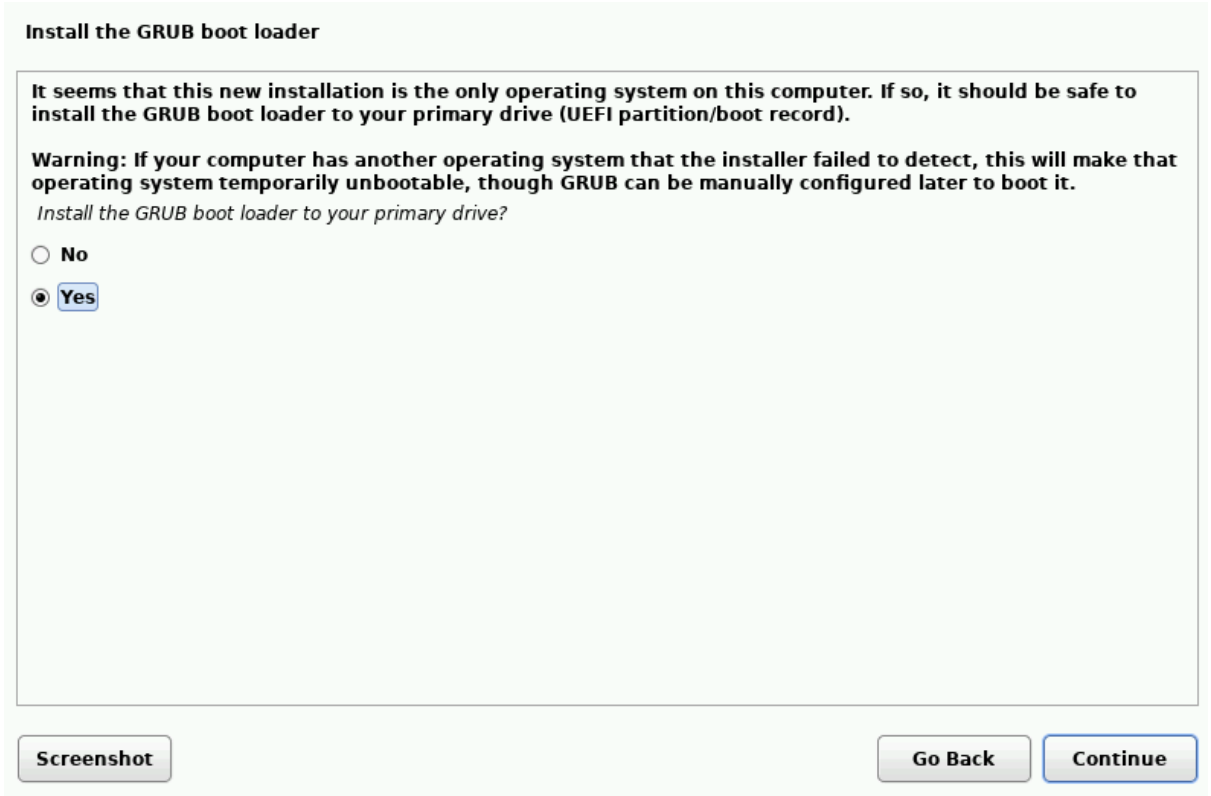

Install the base system
Installing the base system
Extracting dpkg...

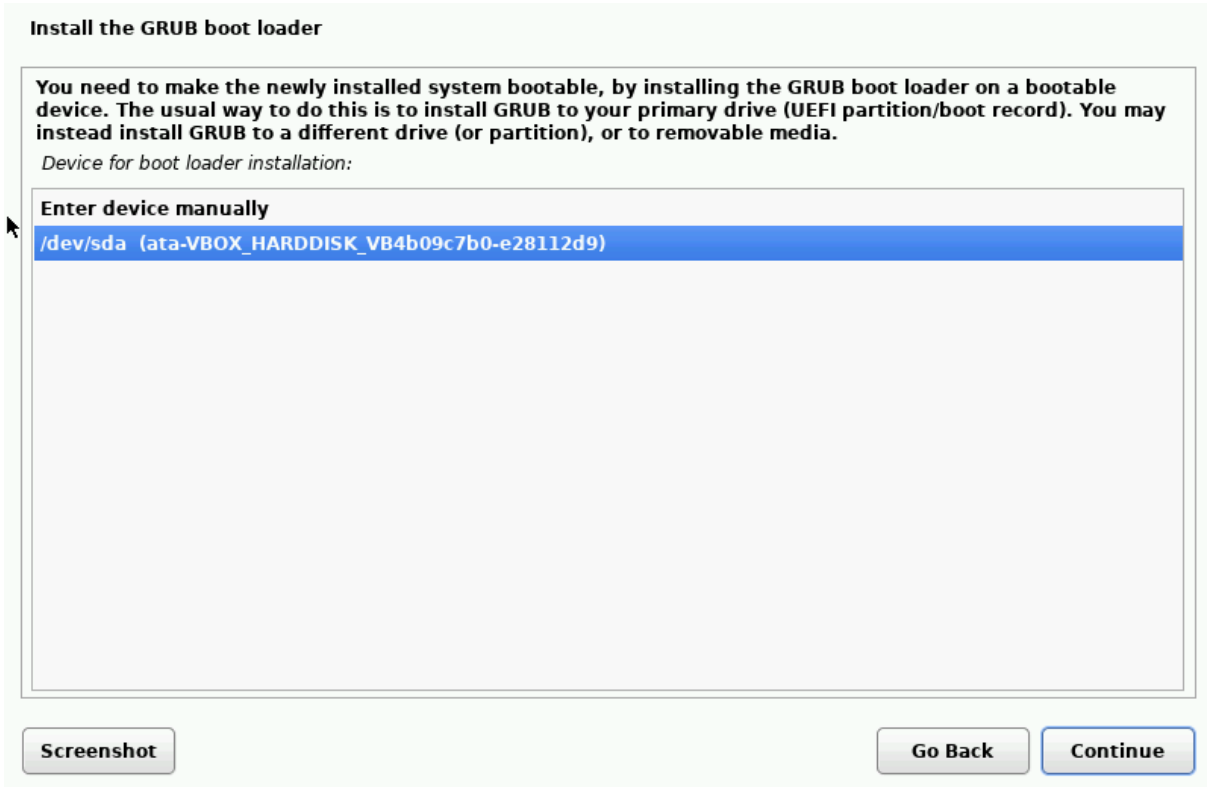

Kali 2022.3 Everything [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Software selection
At the moment, only the core of the system is installed. The default selections below will install Kali Linux with its standard desktop environment and the default tools.
You can customize it by choosing a different desktop environment or a different collection of tools.
Choose software to install:
Desktop environment [selecting this item has no effect]
... Xfce (Kali's default desktop environment)
... GNOME
... KDE Plasma
Collection of tools [selecting this item has no effect]
... top10 -- the 10 most popular tools
... default -- recommended tools (available in the live system)
... large -- default selection plus additional tools
... everything -- almost all tools [>= 7 GB of packages and >= 16 GB installed]
Screenshot
Continue


Select and install software
Select and install software
Retrieving file 309 of 4491

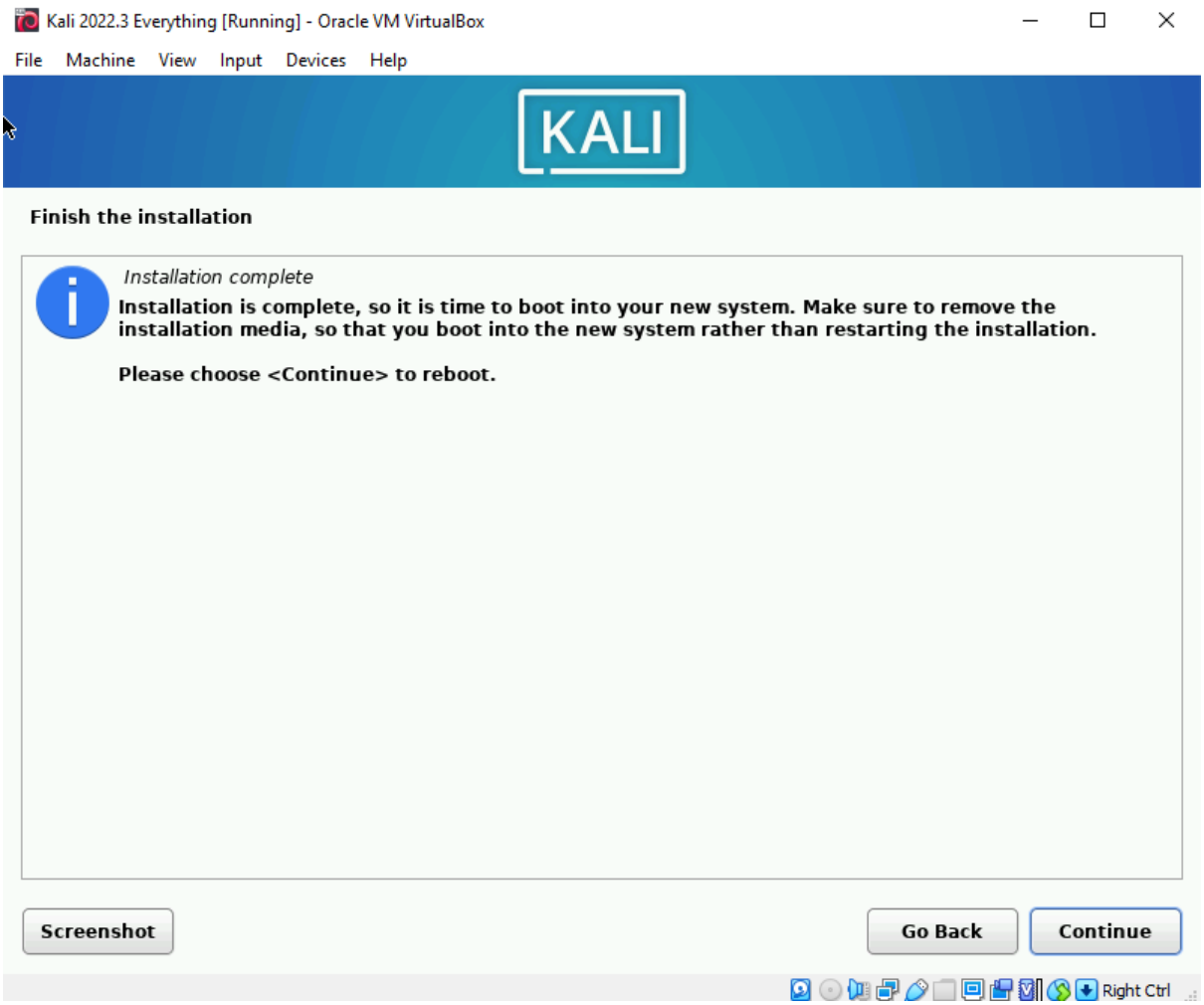

Configuring gdm3
A display manager is a program that provides graphical login capabilities for the X Window System.
Only one display manager can manage a given X server, but multiple display manager packages are installed. Please select which display manager should run by default.
Multiple display managers can run simultaneously if they are configured to manage different servers; to achieve this, configure the display managers accordingly, edit each of their init scripts in /etc/init.d, and disable the check for a default display manager.
Default display manager:
gdm3
lightdm
sddm
Screenshot
Go Back
Continue

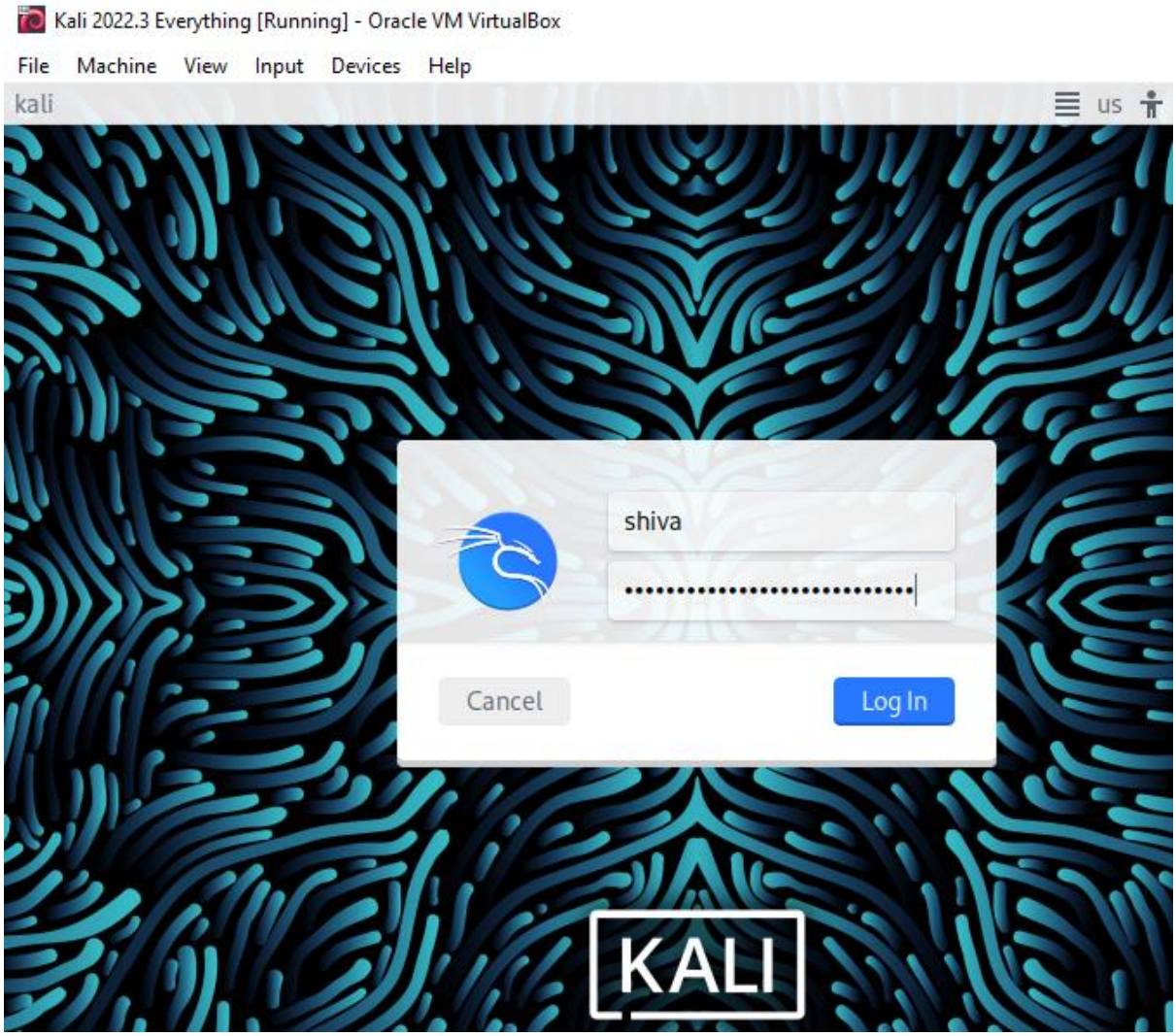

Select and install software
Select and install software
Installing binfmt-support (amd64)


Install the GRUB boot loader
It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to your primary drive (UEFI partition/boot record).
Warning: If your computer has another operating system that the installer failed to detect, this will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.
Install the GRUB boot loader to your primary drive?
No
Yes
Screenshot
Go Back
Continue

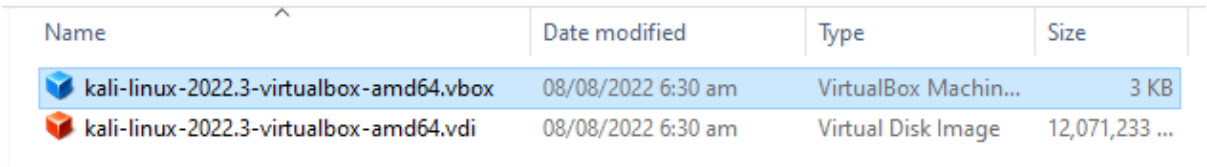

Install the GRUB boot loader
You need to make the newly installed system bootable, by installing the GRUB boot loader on a bootable device. The usual way to do this is to install GRUB to your primary drive (UEFI partition/boot record). You may instead install GRUB to a different drive (or partition), or to removable media.
Device for boot loader installation:
Enter device manually
/dev/sda (ata-VBOX_HARDDISK_VB4b09c7b0-e28112d9)
Screenshot
Go Back
Continue

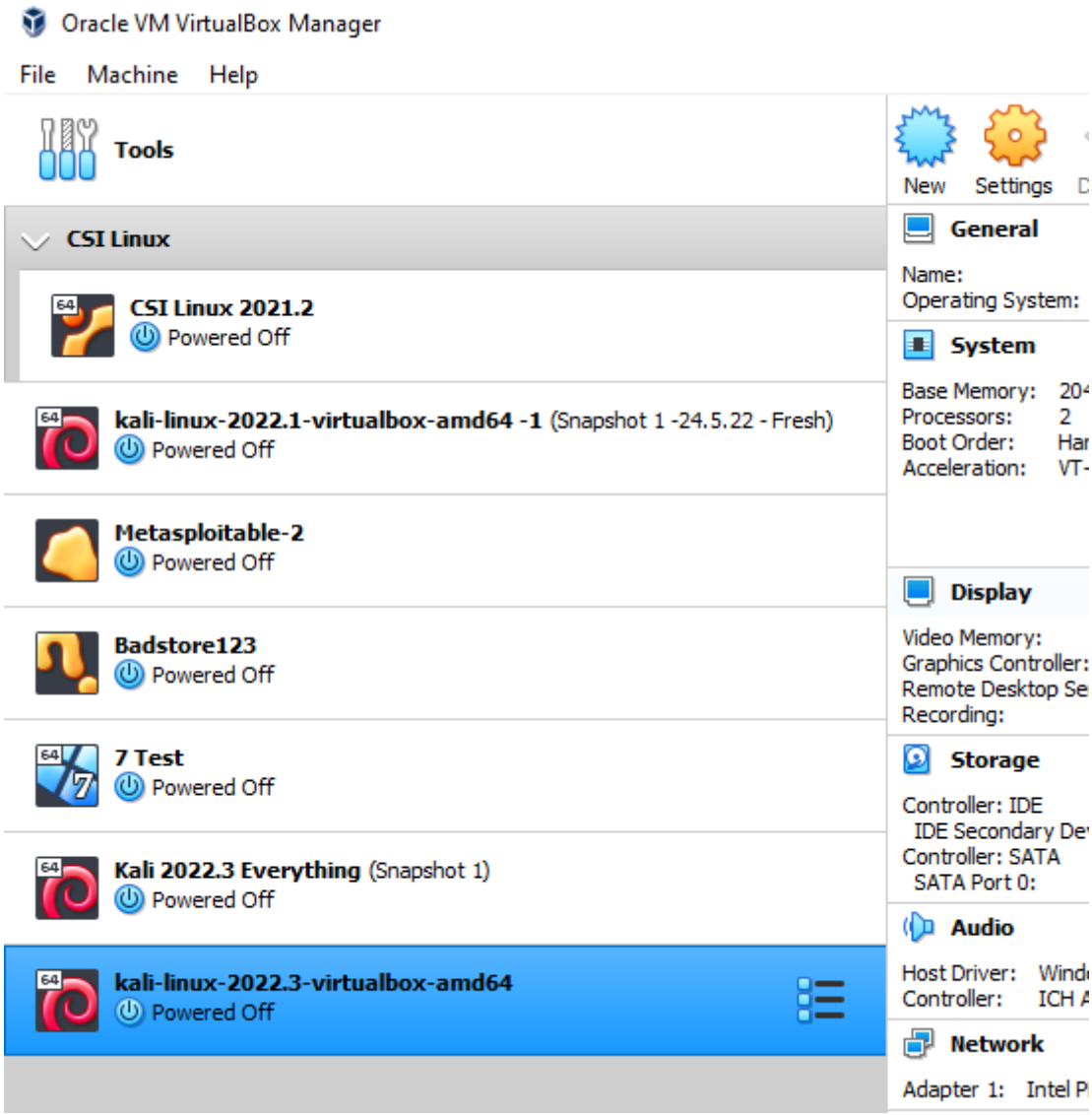

Finish the installation
Finishing the installation
Installed virtualbox-guest-x11 (amd64)

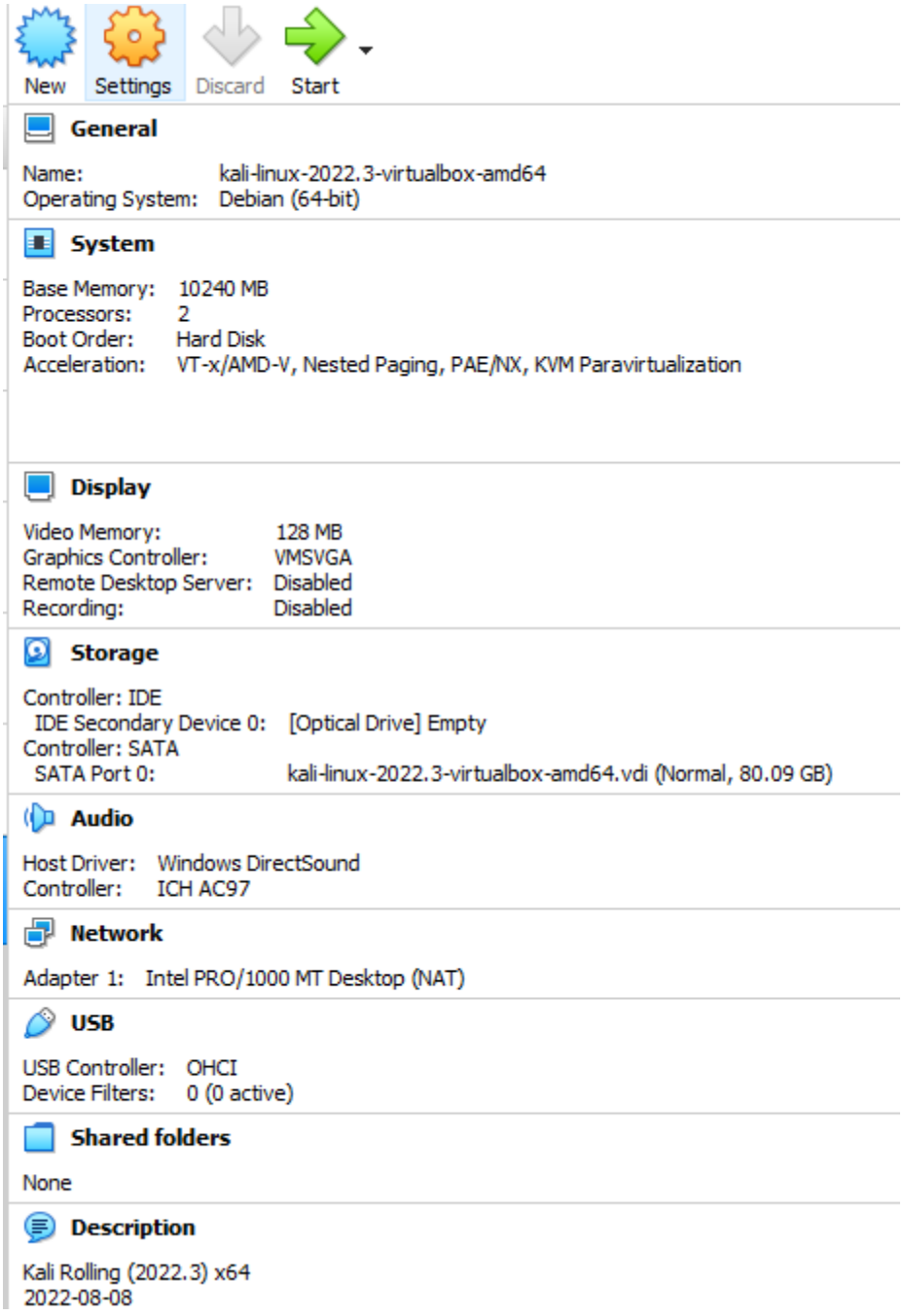

Kali 2022.3 Everything [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
Finish the installation
Installation complete
Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media, so that you boot into the new system rather than restarting the installation.
Please choose <Continue> to reboot.
Screenshot
Go Back
Continue
Right Ctrl

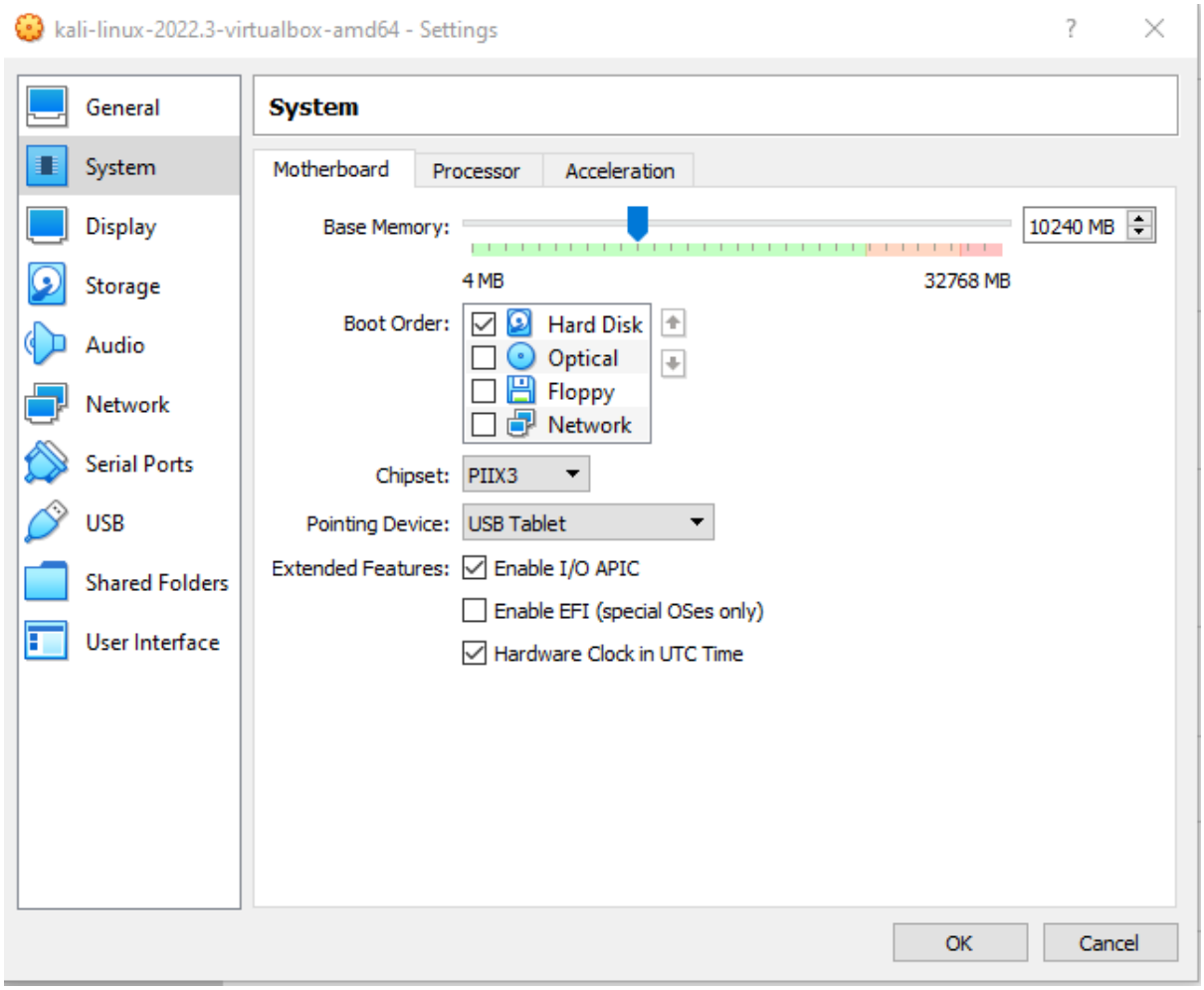

Kali 2022.3 Everything [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali
us
shiva
Cancel
Log In
KALI

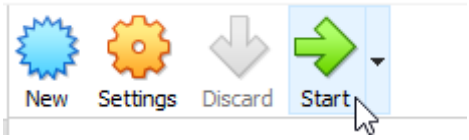
Chapter 4: Additional Kali Installations and Post-Installation Tasks

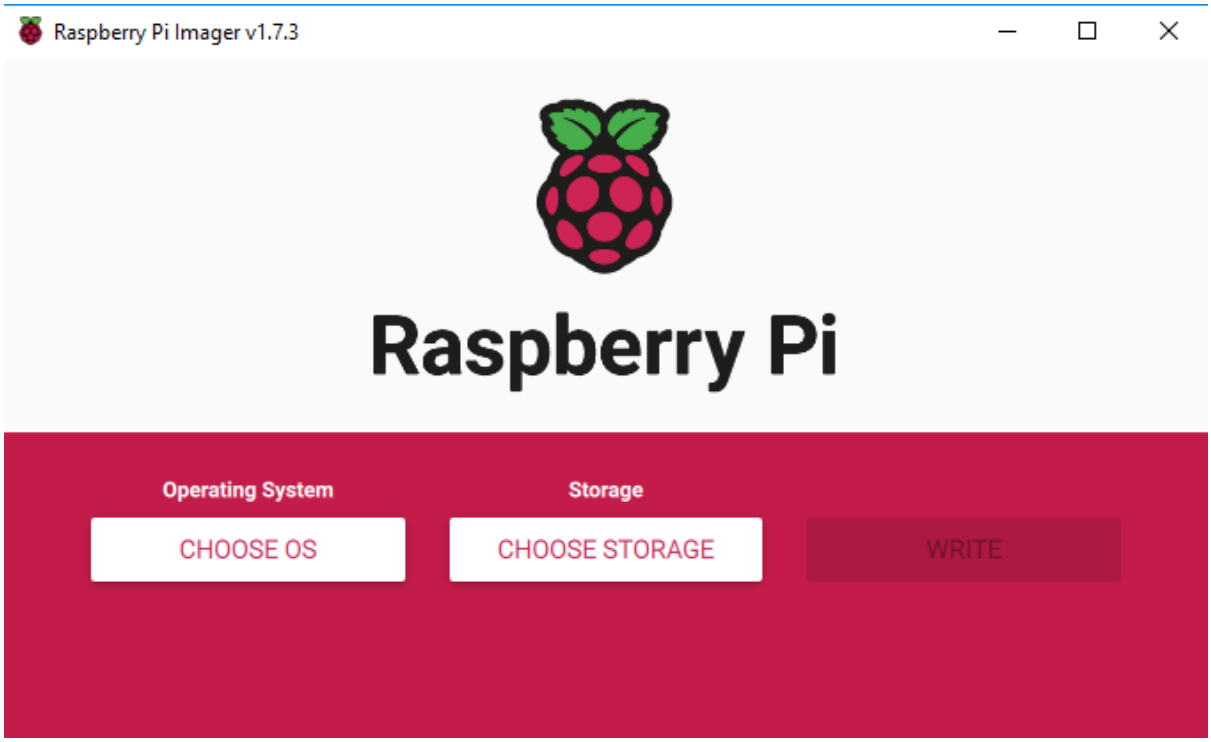


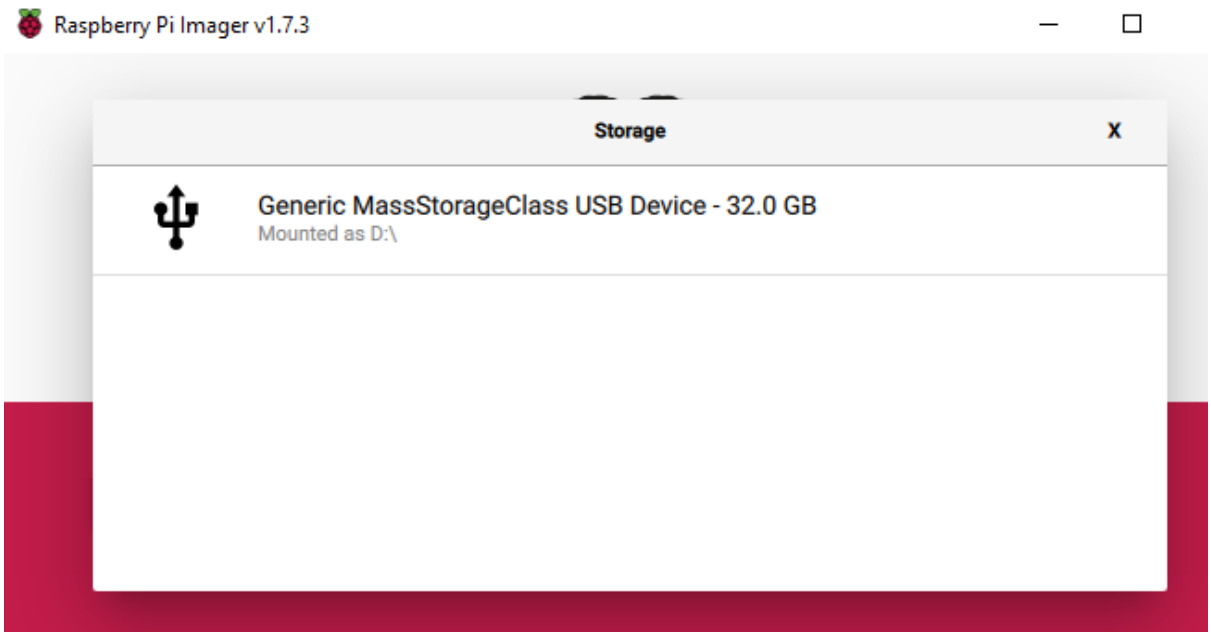


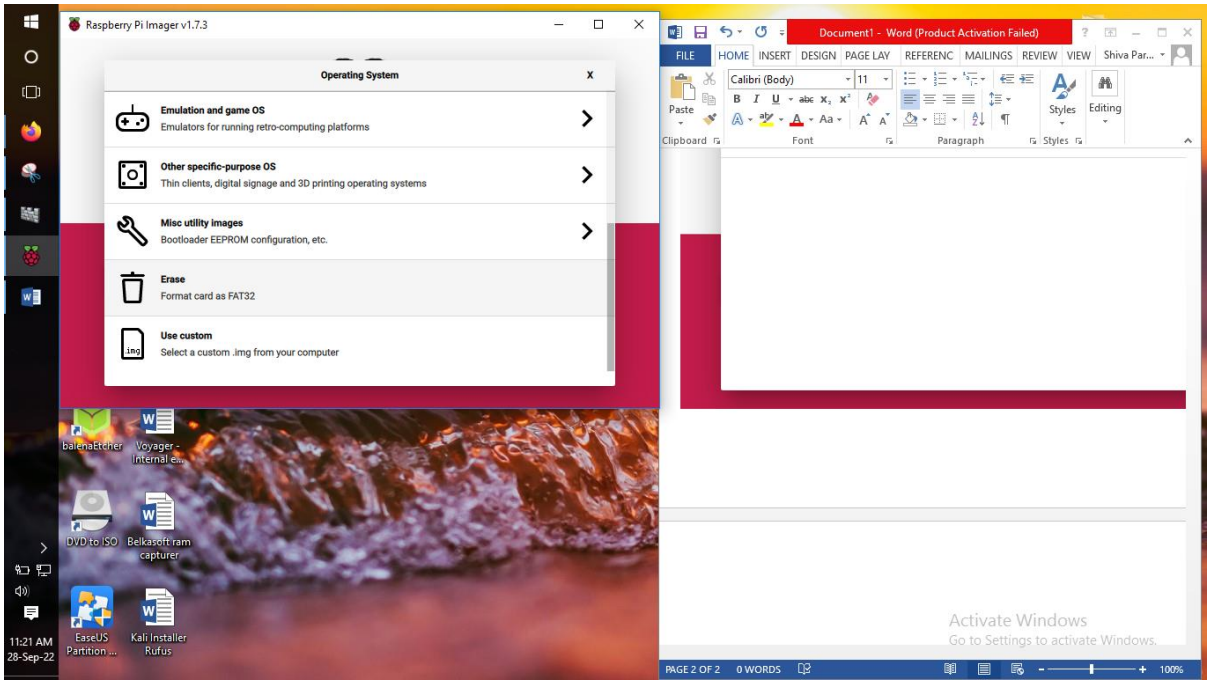

New
Settings
Discard
Start
General
Name: kali-linux-2022.3-virtualbox-amd64
Operating System: Debian (64-bit)
System
Base Memory: 10240 MB
Processors: 2
Boot Order: Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization
Display
Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: kali-linux-2022.3-virtualbox-amd64.vdi (Normal, 80.09 GB)
Audio
Host Driver: Windows DirectSound
Controller: ICH AC97
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)
USB
USB Controller: OHCI
Device Filters: 0 (0 active)
Shared folders
None
Description
Kali Rolling (2022.3) x64
2022-08-08

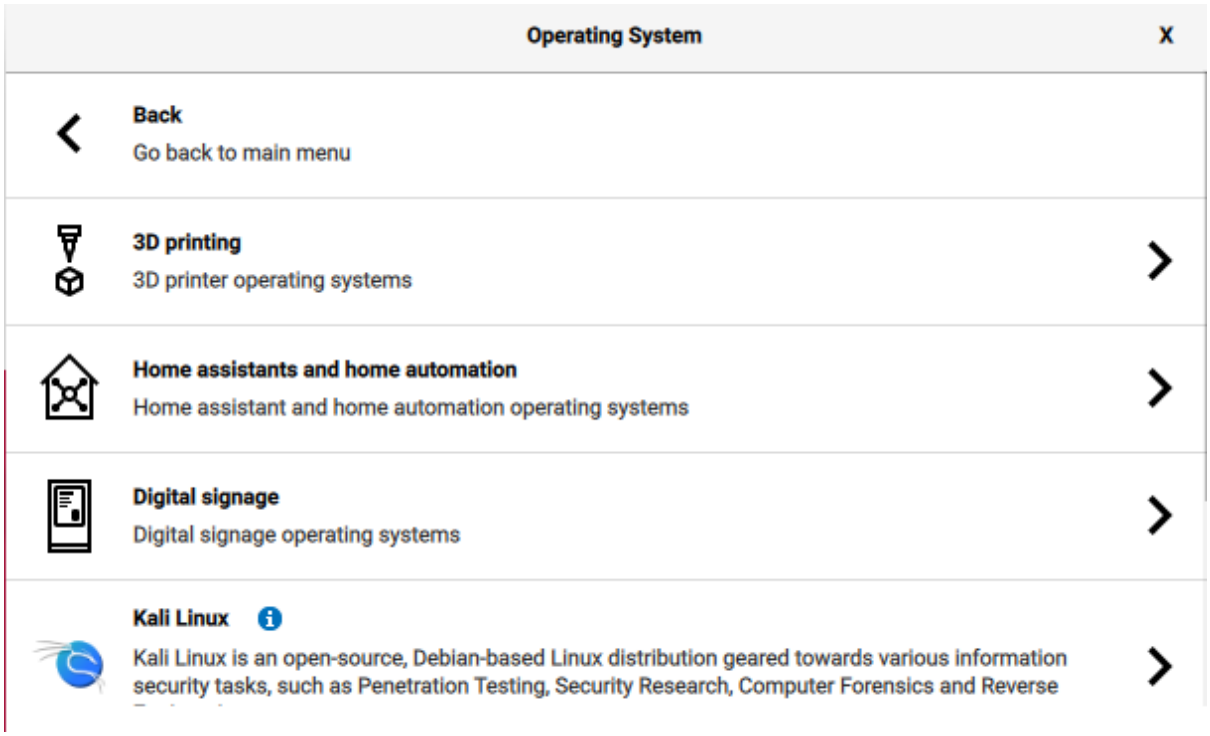

kali-linux-2022.3-virtualbox-amd64 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
System
Motherboard
Processor
Acceleration
Base Memory:
10240 MB
4 MB
32768 MB
Boot Order:
Hard Disk
Optical
Floppy
Network
Chipset:
PIIX3
Pointing Device:
USB Tablet
Extended Features:
Enable I/O APIC
Enable EFI (special OSes only)
Hardware Clock in UTC Time
OK
Cancel

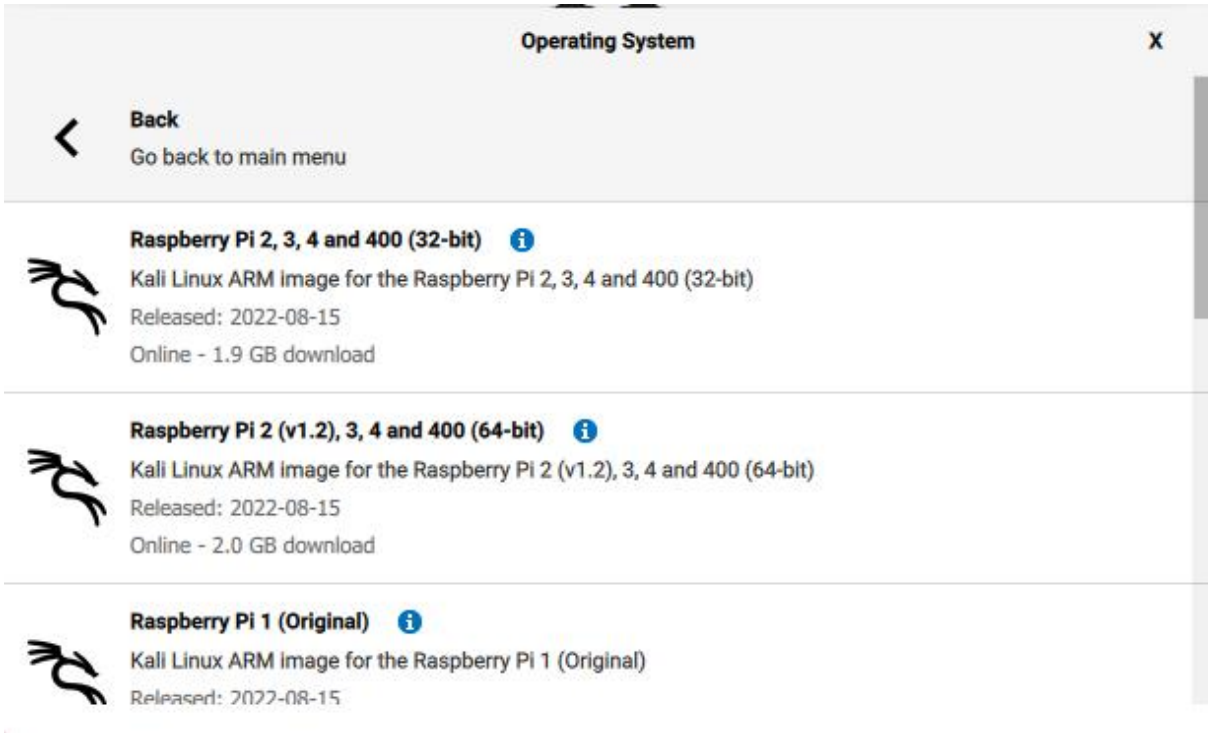

New
Settings
Discard
Start


Raspberry Pi Imager v1.7.3
Raspberry Pi
Operating System
CHOOSE OS
Storage
CHOOSE STORAGE
WRITE

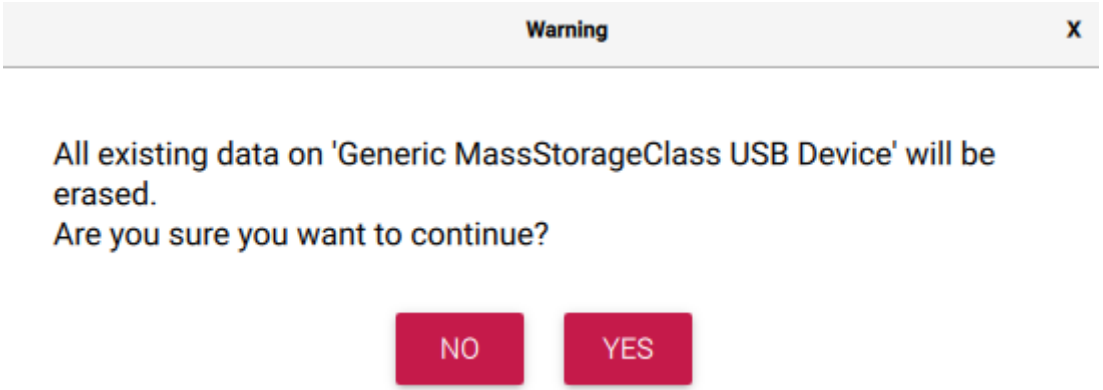

Raspberry Pi Imager v1.7.3
Storage
Generic MassStorageClass USB Device - 32.0 GB
Mounted as D:\

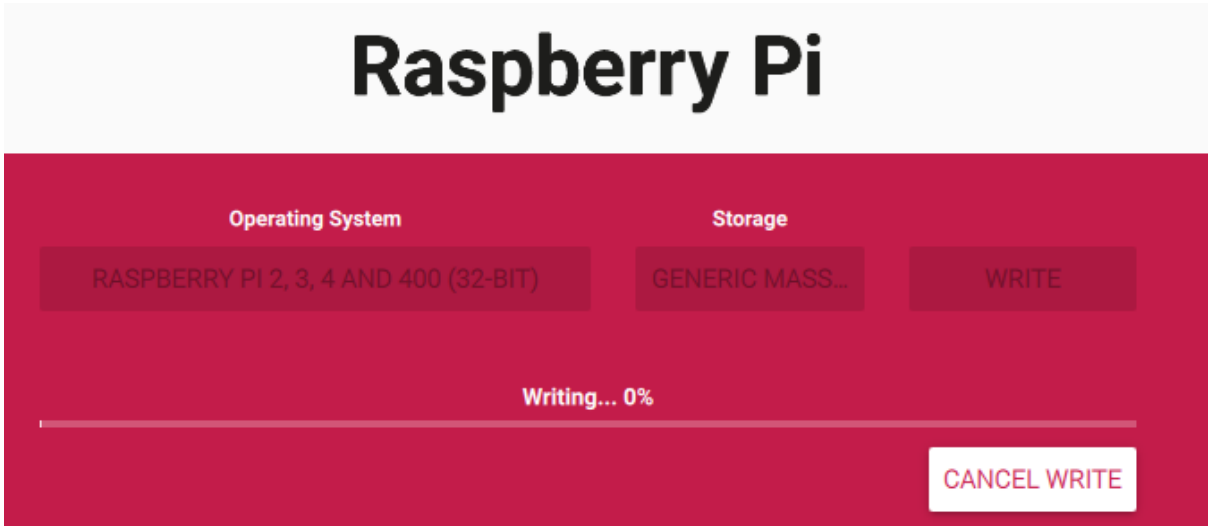

Raspberry Pi Imager v1.7.3
Operating System
Emulation and game OS
Emulators for running retro-computing platforms
Other specific-purpose OS
Thin clients, digital signage and 3D printing operating systems
Misc utility images
Bootloader EEPROM configuration, etc.
Erase
Format card as FAT32
Use custom
Select a custom .img from your computer
balenaEtcher
Voyager - Internal e...
DVD to ISO
Belkasoft ram capturer
EaseUS Partition ...
Kali Installer Rufus
11:21 AM
28-Sep-22
Document1 - Word (Product Activation Failed)
Activate Windows
Go to Settings to activate Windows.
PAGE 2 OF 2
0 WORDS
100%

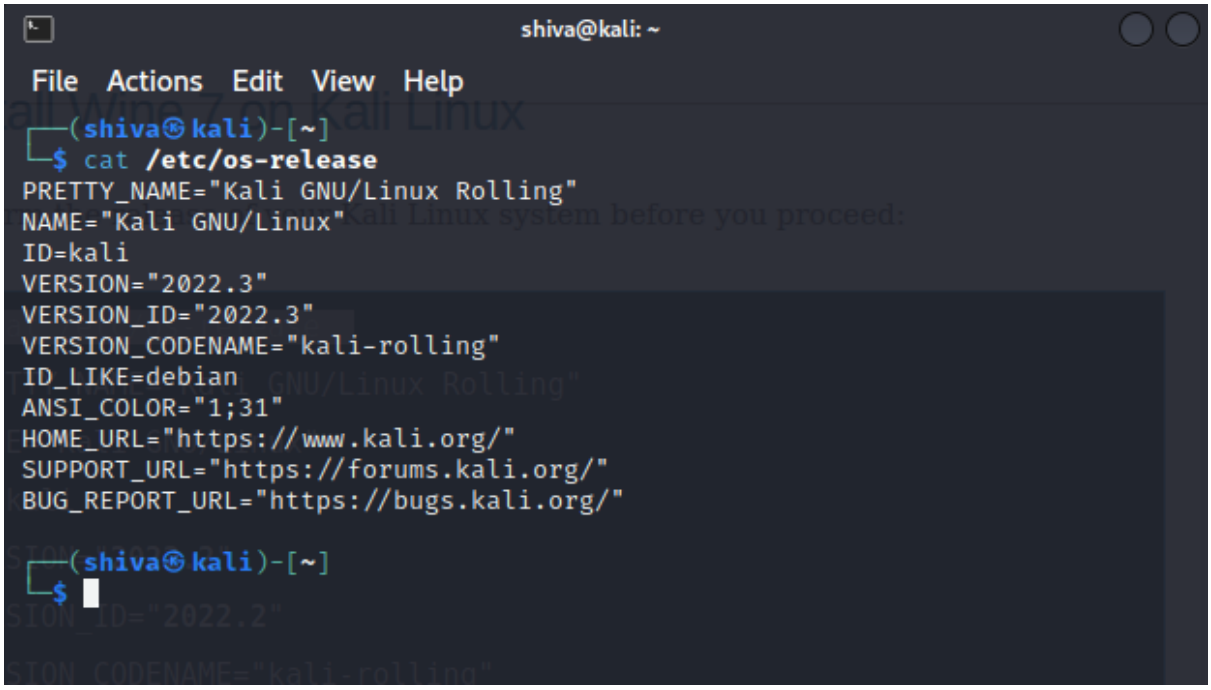

Operating System
X
Back
Go back to main menu
3D printing
3D printer operating systems
Home assistants and home automation
Home assistant and home automation operating systems
Digital signage
Digital signage operating systems
Kali Linux
Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse


Operating System
X
Back
Go back to main menu
Raspberry Pi 2, 3, 4 and 400 (32-bit)
Kali Linux ARM image for the Raspberry Pi 2, 3, 4 and 400 (32-bit)
Released: 2022-08-15
Online - 1.9 GB download
Raspberry Pi 2 (v1.2), 3, 4 and 400 (64-bit)
Kali Linux ARM image for the Raspberry Pi 2 (v1.2), 3, 4 and 400 (64-bit)
Released: 2022-08-15
Online - 2.0 GB download
Raspberry Pi 1 (Original)
Kali Linux ARM image for the Raspberry Pi 1 (Original)
Released: 2022-08-15


Raspberry Pi Imager v1.7.3
Raspberry Pi
Operating System
Storage
RASPBERRY PI 2, 3, 4 AND 400 (32-BIT)
GENERIC MASS...
WRITE


Warning
X
All existing data on 'Generic MassStorageClass USB Device' will be erased.
Are you sure you want to continue?
NO
YES


Raspberry Pi
Operating System
Storage
RASPBERRY PI 2, 3, 4 AND 400 (32-BIT)
GENERIC MASS...
WRITE
Writing... 0%
CANCEL WRITE

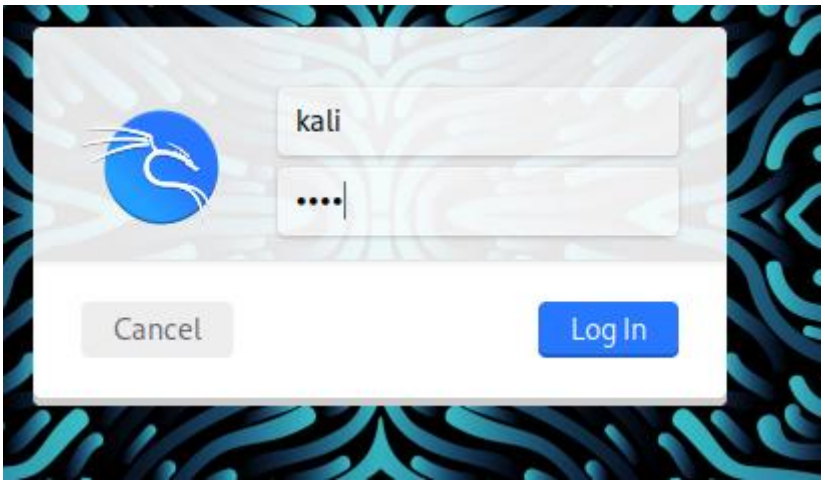

shiva@kali: ~
File Actions Edit View Help
(shiva㉿kali)-[~]
$ cat /etc/os-release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2022.3"
VERSION_ID="2022.3"
VERSION_CODENAME="kali-rolling"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
(shiva㉿kali)-[~]
$

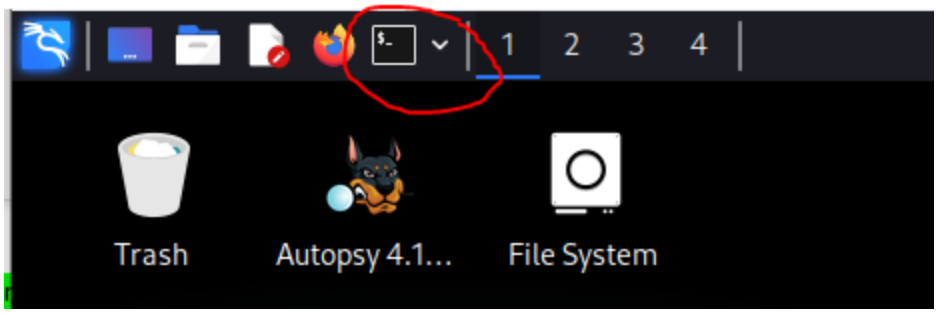
```
┌──(shiva㉿kali)-[~]
└─$ sudo apt update
[sudo] password for shiva:
Get:1 http://kali.download/kali kali-rolling InRelease [30.6 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [18.3 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [42.5
MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [109 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [15
8 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [221 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [8
98 kB]
Fetched 62.2 MB in 27s (2,273 kB/s)
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
674 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```
┌──(shiva㉿kali)-[~]
└─$ apt list --upgradable
Listing ... Done
apparmor/kali-rolling 3.0.7-1 amd64 [upgradable from: 3.0.5-1]
atftpd/kali-rolling 0.7.git20210915-6 amd64 [upgradable from: 0.7.git20210915
-4]
base-passwd/kali-rolling 3.6.0 amd64 [upgradable from: 3.5.52]
bash/kali-rolling 5.2~rc2-2 amd64 [upgradable from: 5.1-6.1]
bettercap/kali-rolling 2.32.0-1+b3 amd64 [upgradable from: 2.32.0-1+b2]
busybox/kali-rolling 1:1.35.0-1+b1 amd64 [upgradable from: 1:1.35.0-1]
cherrytree/kali-rolling 0.99.48+dfsg-1 amd64 [upgradable from: 0.99.47+dfsg-1
]
chkrootkit/kali-rolling 0.55-4+b2 amd64 [upgradable from: 0.55-4+b1]
cifs-utils/kali-rolling 2:7.0-2 amd64 [upgradable from: 2:6.14-1.1]
cpp/kali-rolling 4:12.1.0-3 amd64 [upgradable from: 4:11.2.0-2]
cryptsetup-bin/kali-rolling 2:2.5.0-2 amd64 [upgradable from: 2:2.4.3-1+b1]
cryptsetup-initramfs/kali-rolling 2:2.5.0-2 all [upgradable from: 2:2.4.3-1]
cryptsetup/kali-rolling 2:2.5.0-2 amd64 [upgradable from: 2:2.4.3-1+b1]
dash/kali-rolling 0.5.11+git20210903+057cd650a4ed-9 amd64 [upgradable from: 0
.5.11+git20210903+057cd650a4ed-8]
diffutils/kali-rolling 1:3.8-1 amd64 [upgradable from: 1:3.7-5]
dradis/kali-rolling 4.5.0-0kali1 amd64 [upgradable from: 4.4.0-0kali1]
ethtool/kali-rolling 1:5.19-1 amd64 [upgradable from: 1:5.18-1]
ewf-tools/kali-rolling 20140813-1 amd64 [upgradable from: 20140807-2.1]
exiv2/kali-rolling 0.27.5-4 amd64 [upgradable from: 0.27.5-3]
firefox-esr/kali-rolling 102.2.0esr-1 amd64 [upgradable from: 91.11.0esr-1]
```

```
┌──(shiva㉿kali)-[~]
└─$ sudo apt upgrade -y
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Calculating upgrade ... Done
The following packages were automatically installed and are no longer require
d:
  libhttp-server-simple-perl liblerc3 libwacom-bin python3-dataclasses-json
  python3-limiter python3-mypy-extensions python3-responses python3-spyse
  python3-token-bucket python3-typing-inspect python3.9 python3.9-minimal
  ruby2.7-dev ruby2.7-doc xprobe
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  certipy-ad colly faraday-agent-dispatcher google-nexus-tools
  libdbus-1-dev liblerc4 libpcap-dev libpcap0.8-dev libwebsockets17
  mongo-tools python3-cryptography37 python3-json-pointer python3-munkres
  python3-rfc3987 python3-webcolors python3-zapv2 ruby-websocket
The following packages have been kept back:
  apparmor atftpd base-passwd bash bettercap busybox cherrytree chkrootkit
  cifs-utils cpp cryptsetup cryptsetup-bin cryptsetup-initramfs dash
  diffutils dradis ethtool ewf-tools exiv2 firefox-esr g++ gcc gcc-12-base
  gir1.2-javascriptcoregtk-4.0 gir1.2-nm-1.0 gir1.2-vte-2.91
```

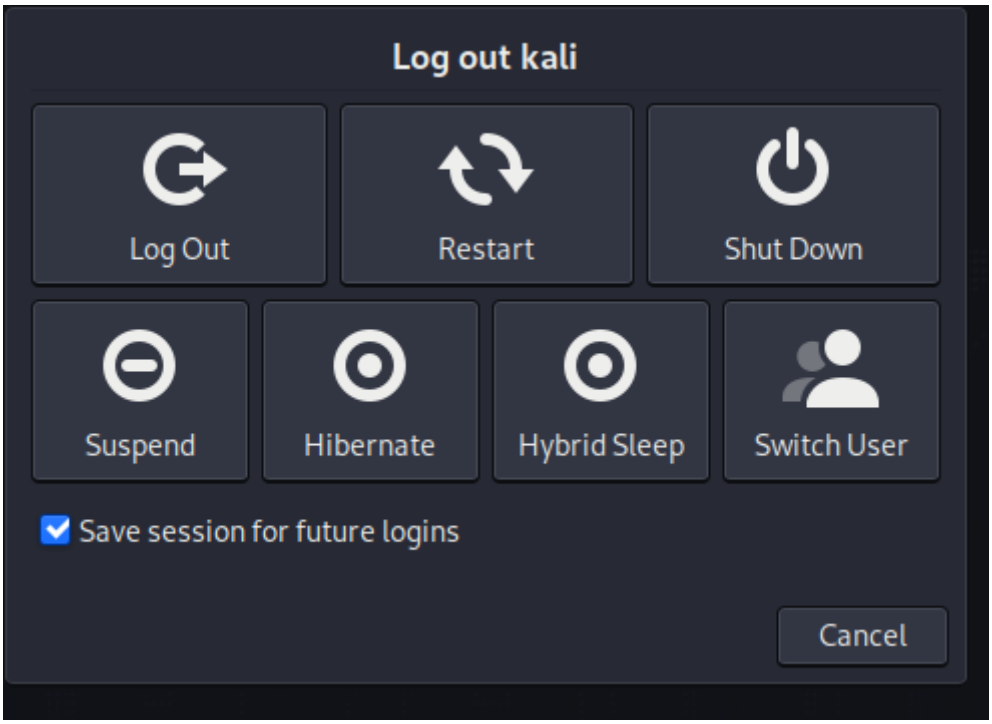
```
┌──(shiva㉿kali)-[~]
└─$ sudo reboot
```

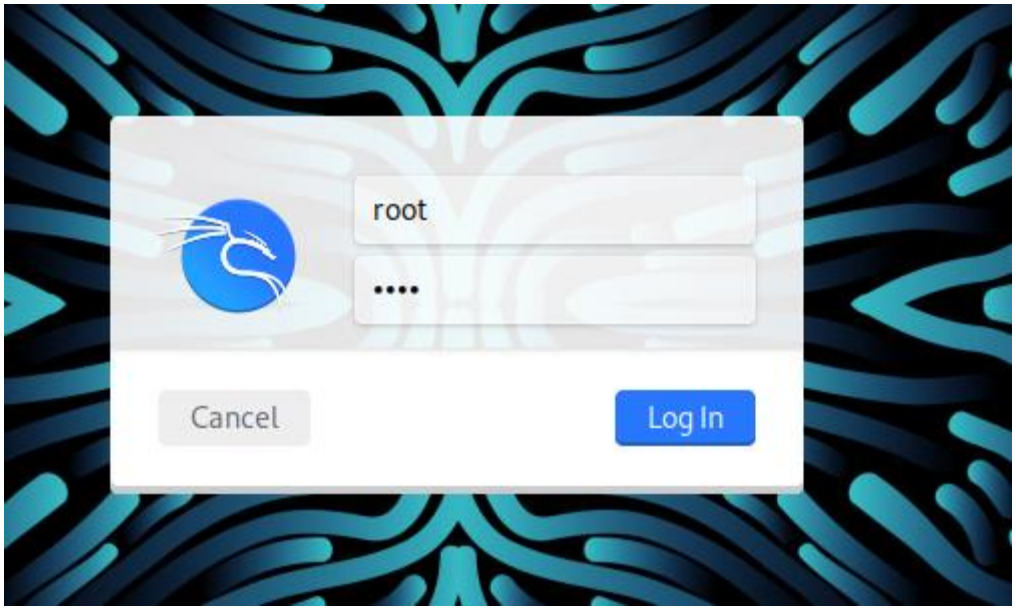


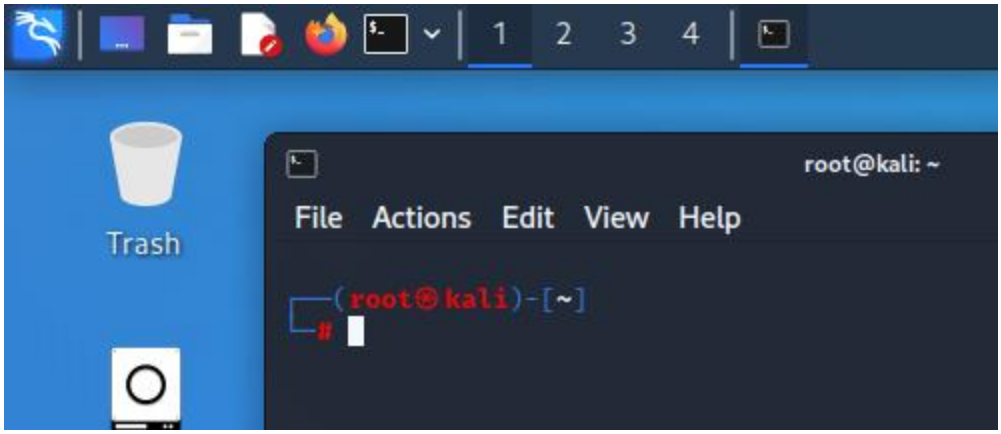



File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
#


(root㉿kali)-[/home/kali]
passwd root
New password:
Retype new password:
passwd: password updated successfully
(root㉿kali)-[/home/kali]
#

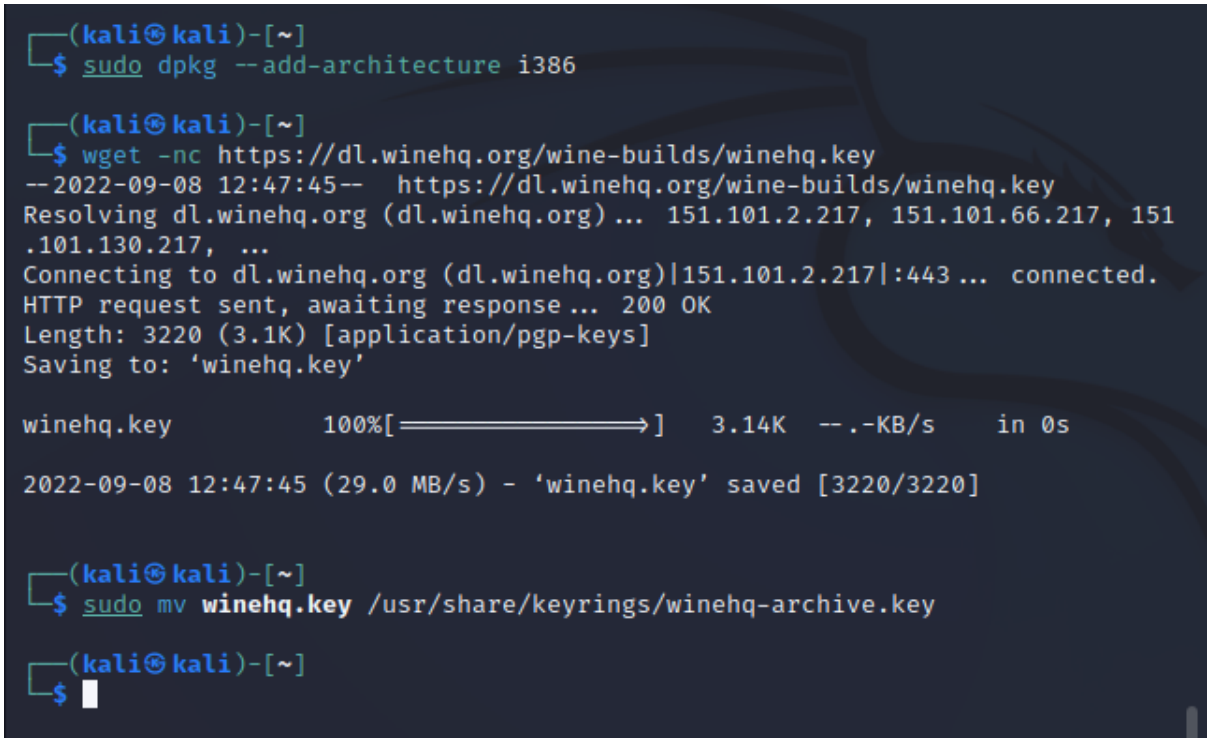

Log out kali
Log Out
Restart
Shut Down
Suspend
Hibernate
Hybrid Sleep
Switch User
Save session for future logins
Cancel

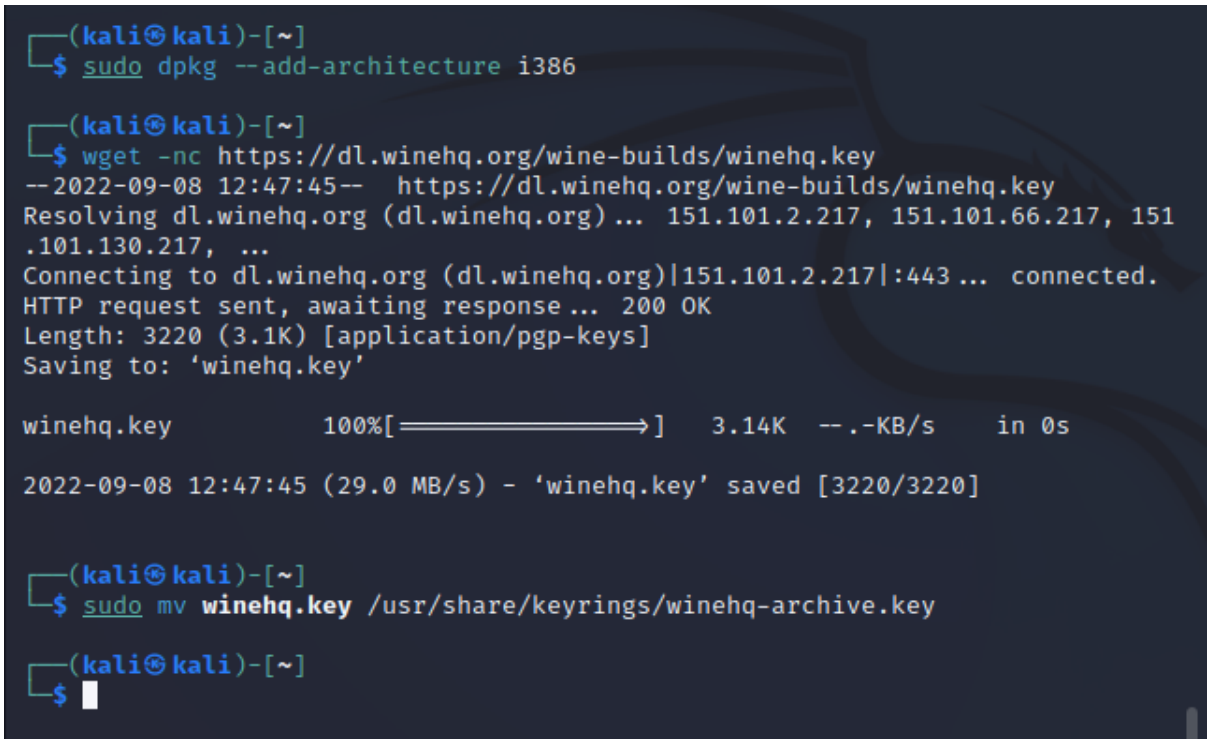





```
┌──(kali㉿kali)-[~]
└─$ sudo apt install kali-tools-forensics
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
```

Chapter 5: Installing WINE in Kali Linux





```
┌──(kali㉿kali)-[~]
└─$ sudo dpkg --add-architecture i386

┌──(kali㉿kali)-[~]
└─$ wget -nc https://dl.winehq.org/wine-builds/winehq.key
--2022-09-08 12:47:45--  https://dl.winehq.org/wine-builds/winehq.key
Resolving dl.winehq.org (dl.winehq.org)... 151.101.2.217, 151.101.66.217, 151
.101.130.217, ...
Connecting to dl.winehq.org (dl.winehq.org)|151.101.2.217|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3220 (3.1K) [application/pgp-keys]
Saving to: 'winehq.key'

winehq.key          100%[===================>]   3.14K  --.-KB/s    in 0s

2022-09-08 12:47:45 (29.0 MB/s) - 'winehq.key' saved [3220/3220]


┌──(kali㉿kali)-[~]
└─$ sudo mv winehq.key /usr/share/keyrings/winehq-archive.key

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ wget -nc https://dl.winehq.org/wine-builds/debian/dists/bullseye/winehq-b
ullseye.sources
--2022-09-08 12:49:50--  https://dl.winehq.org/wine-builds/debian/dists/bulls
eye/winehq-bullseye.sources
Resolving dl.winehq.org (dl.winehq.org)... 151.101.130.217, 151.101.194.217,
151.101.2.217, ...
Connecting to dl.winehq.org (dl.winehq.org)|151.101.130.217|:443... connected
.
HTTP request sent, awaiting response... 200 OK
Length: 168
Saving to: 'winehq-bullseye.sources'

winehq-bullseye.sou 100%[===================>]     168  --.-KB/s    in 0s

2022-09-08 12:49:50 (16.5 MB/s) - 'winehq-bullseye.sources' saved [168/168]


┌──(kali㉿kali)-[~]
└─$ sudo mv winehq-bullseye.sources /etc/apt/sources.list.d/

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ wget -nc https://dl.winehq.org/wine-builds/debian/dists/bullseye/winehq-b
ullseye.sources
--2022-09-08 12:49:50--  https://dl.winehq.org/wine-builds/debian/dists/bulls
eye/winehq-bullseye.sources
Resolving dl.winehq.org (dl.winehq.org)... 151.101.130.217, 151.101.194.217,
151.101.2.217, ...
Connecting to dl.winehq.org (dl.winehq.org)|151.101.130.217|:443... connected
.
HTTP request sent, awaiting response... 200 OK
Length: 168
Saving to: 'winehq-bullseye.sources'

winehq-bullseye.sou 100%[===================>]     168  --.-KB/s    in 0s

2022-09-08 12:49:50 (16.5 MB/s) - 'winehq-bullseye.sources' saved [168/168]


┌──(kali㉿kali)-[~]
└─$ sudo mv winehq-bullseye.sources /etc/apt/sources.list.d/

┌──(kali㉿kali)-[~]
└─$
```

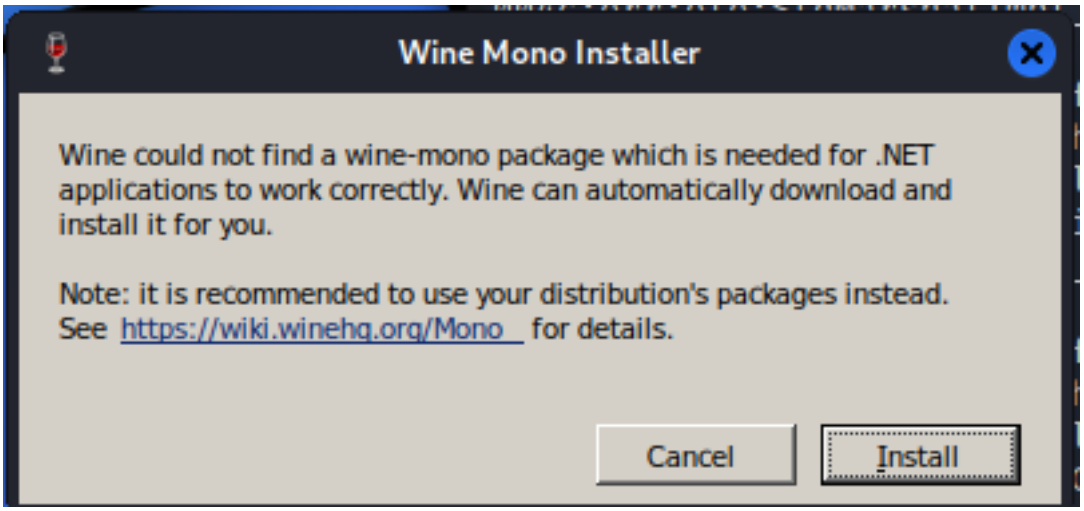
```
┌──(kali㉿kali)-[~]
└─$ echo "deb http://ftp.us.debian.org/debian bullseye main " | sudo tee -a /
etc/apt/sources.list
deb http://ftp.us.debian.org/debian bullseye main
```

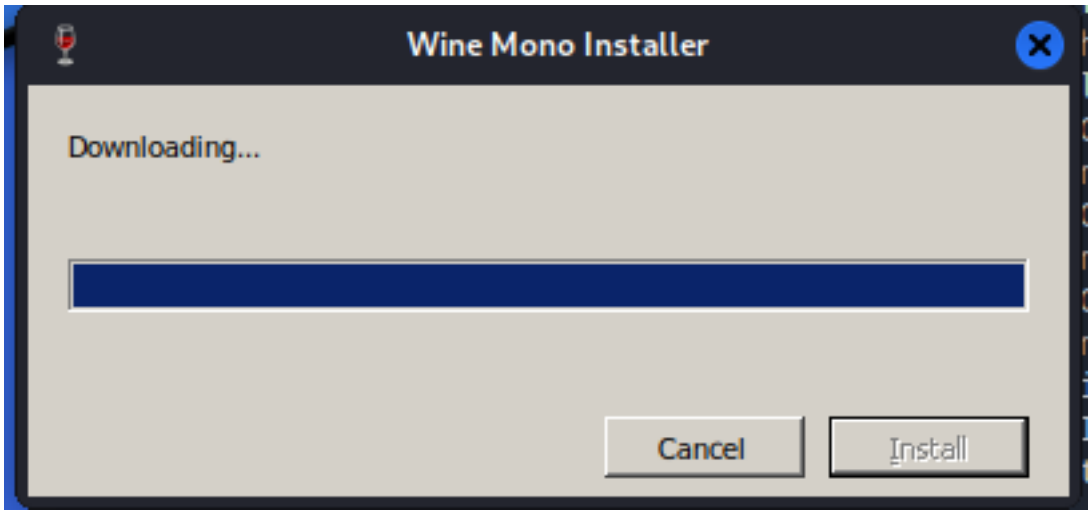
```
┌──(kali㉿kali)-[~]
└─$ sudo apt update
Get:1 http://ftp.us.debian.org/debian bullseye InRelease [116 kB]
Get:2 https://dl.winehq.org/wine-builds/debian bullseye InRelease [8,045 B]
Get:4 https://dl.winehq.org/wine-builds/debian bullseye/main all Packages [1,
280 B]
Get:5 https://dl.winehq.org/wine-builds/debian bullseye/main i386 Packages [5
44 kB]
Hit:3 http://kali.download/kali kali-rolling InRelease
Get:6 http://ftp.us.debian.org/debian bullseye/main i386 Packages [8,121 kB]
Get:7 https://dl.winehq.org/wine-builds/debian bullseye/main amd64 Packages [
533 kB]
Get:8 http://kali.download/kali kali-rolling/main i386 Packages [18.1 MB]
Get:9 http://ftp.us.debian.org/debian bullseye/main amd64 Packages [8,182 kB]
Get:10 http://kali.download/kali kali-rolling/main i386 Contents (deb) [41.3
MB]
Get:11 http://ftp.us.debian.org/debian bullseye/main Translation-en [6,243 kB
```

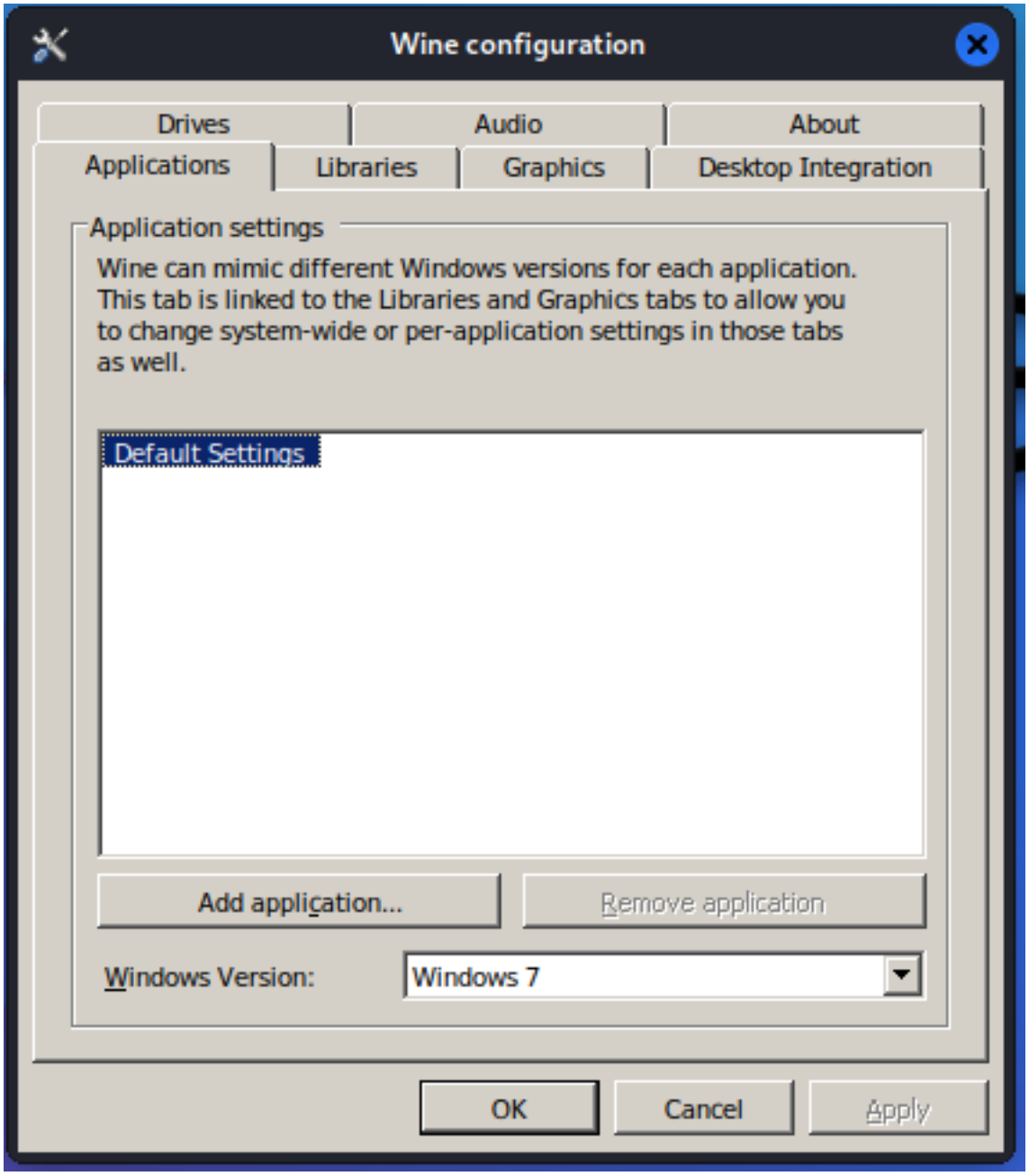
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install --install-recommends winehq-stable\
>
[sudo] password for kali:
```

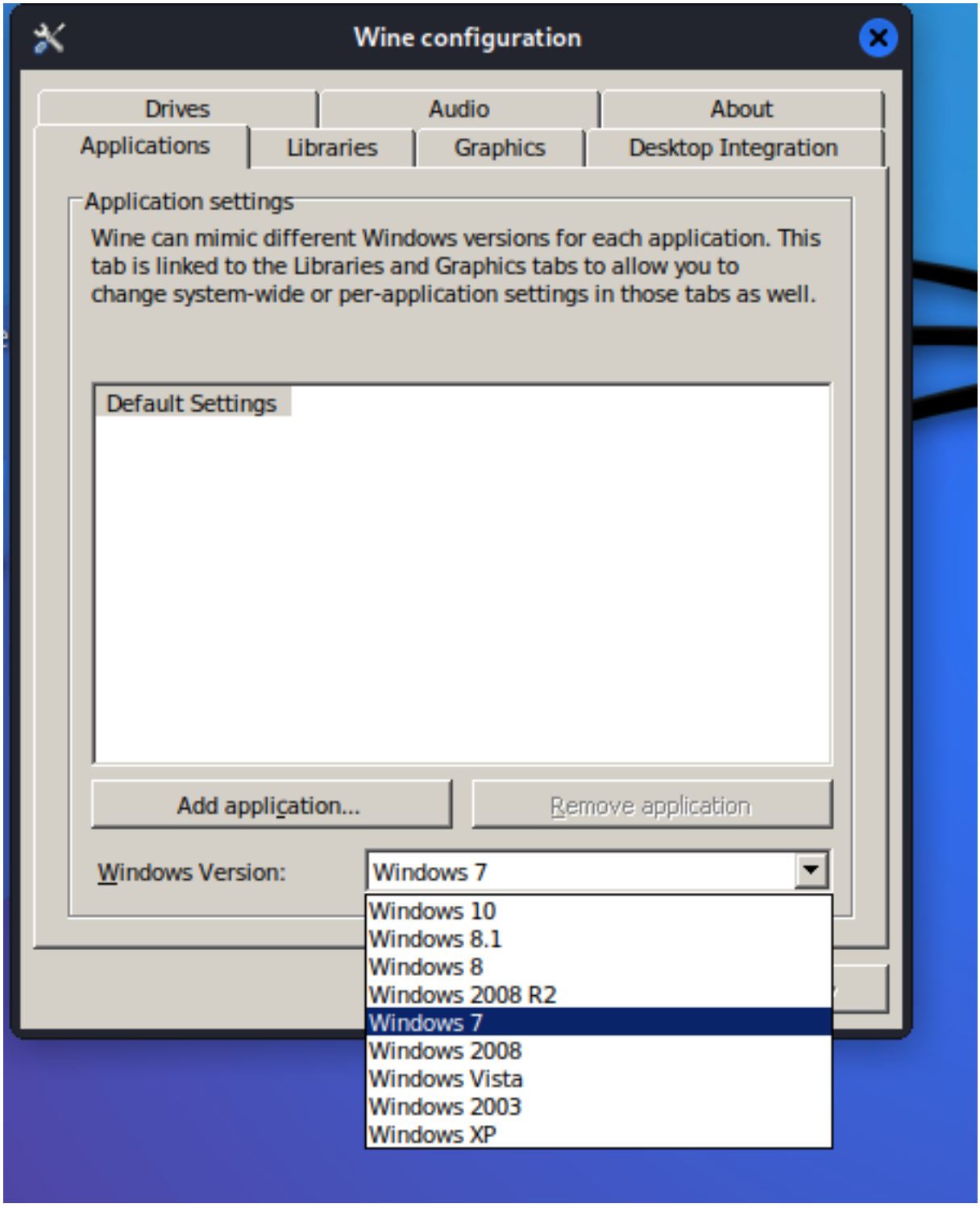
```
┌──(kali㉿kali)-[~]
└─$ wine --version
wine-7.0
```

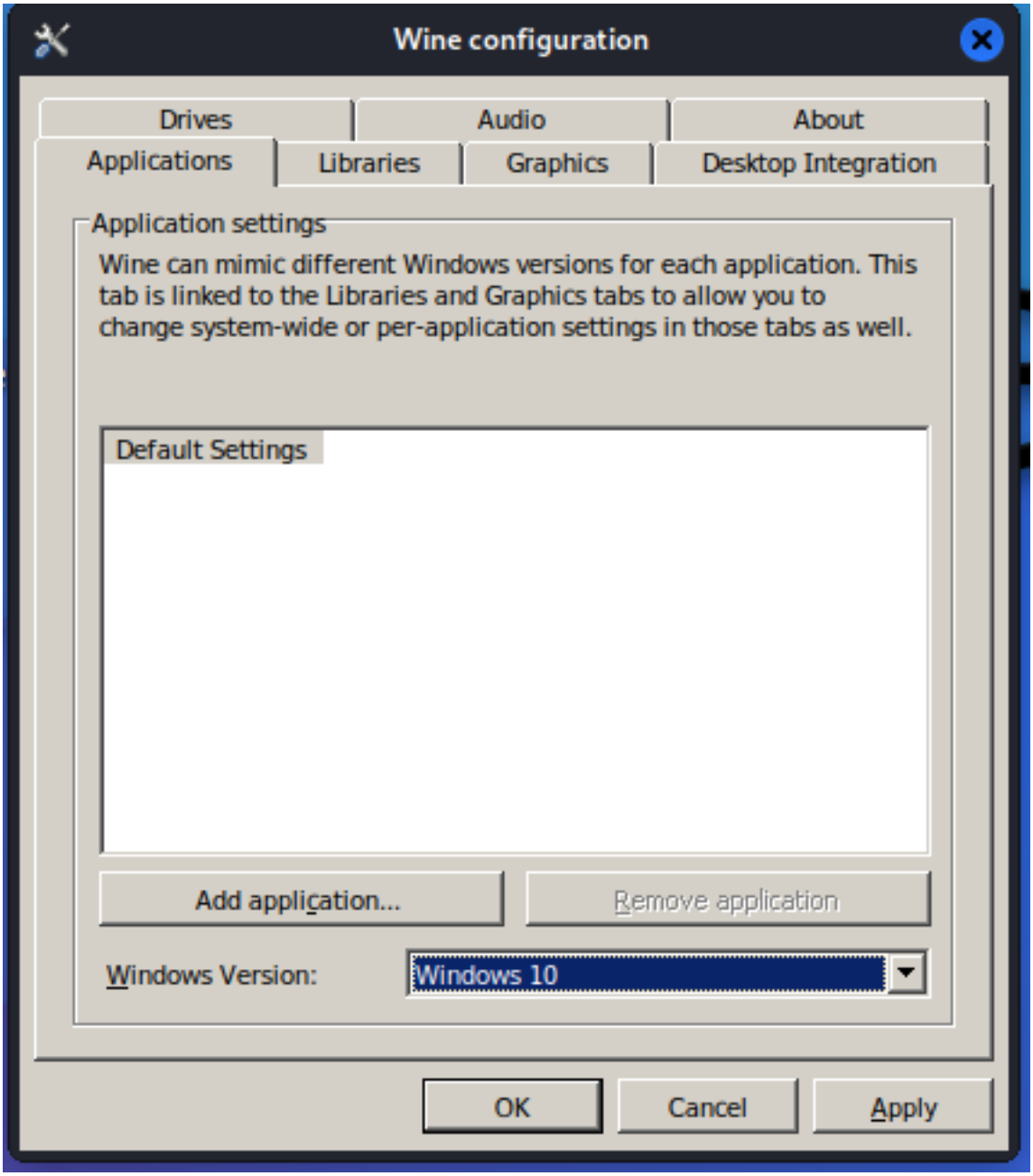
```
┌──(kali㉿kali)-[~]
└─$ winecfg
wine: created the configuration directory '/home/kali/.wine'
```

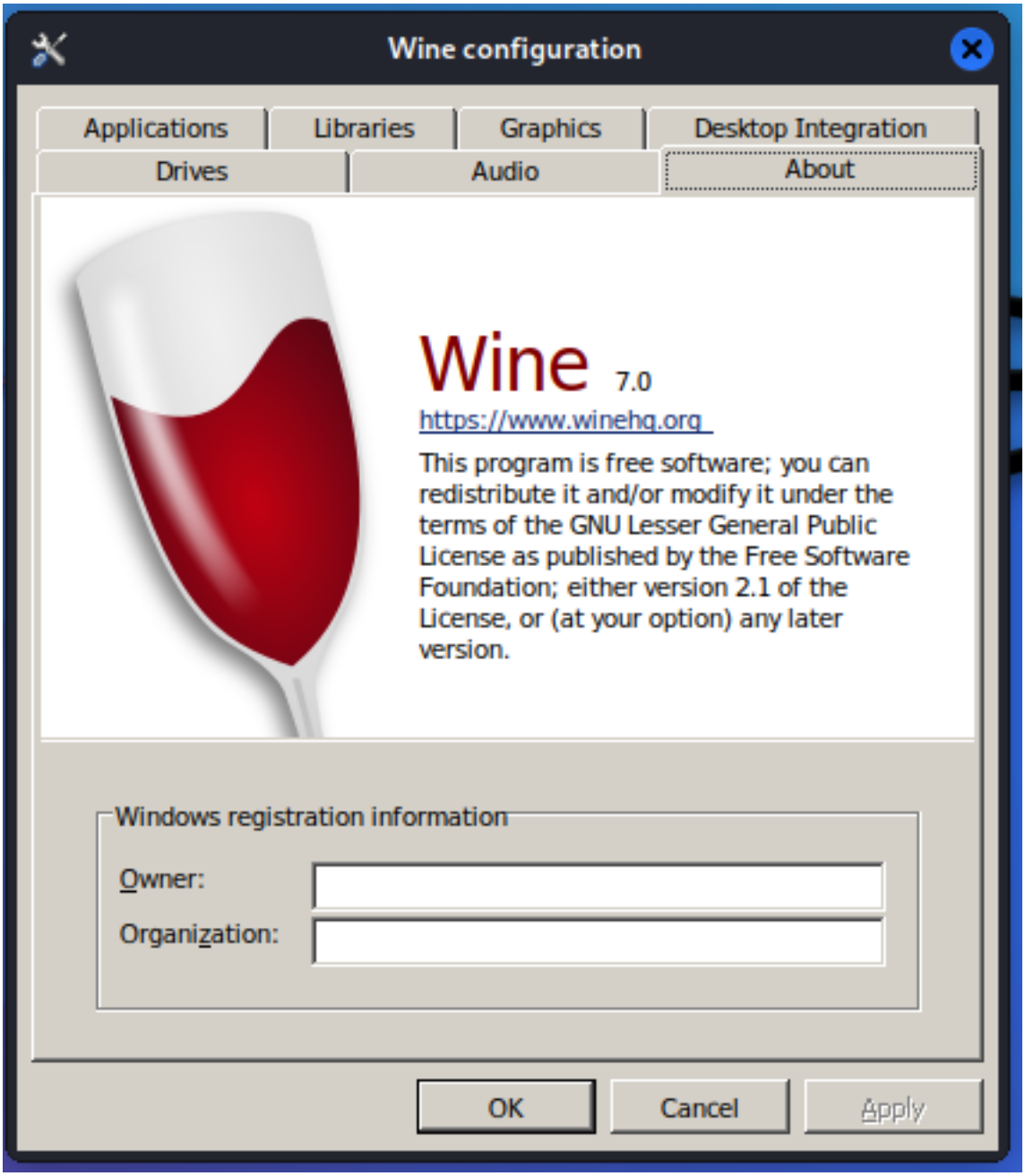




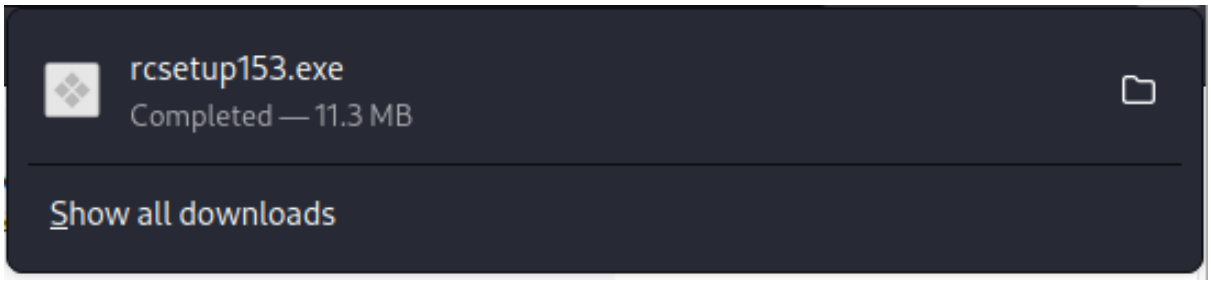

Wine configuration
Drives
Audio
About
Applications
Libraries
Graphics
Desktop Integration
Application settings
Wine can mimic different Windows versions for each application.
This tab is linked to the Libraries and Graphics tabs to allow you
to change system-wide or per-application settings in those tabs
as well.
Default Settings
Add application...
Remove application
Windows Version:
Windows 7
OK
Cancel
Apply

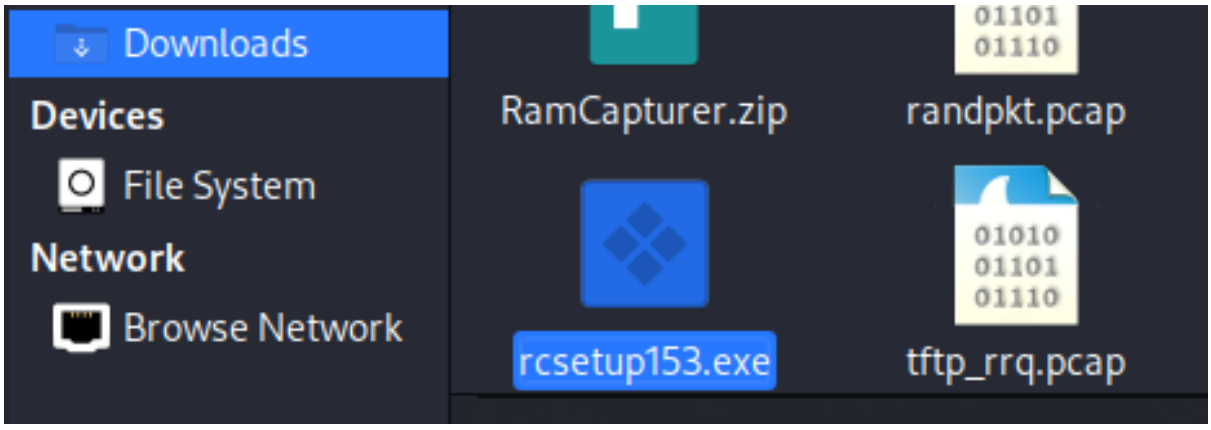

Wine configuration
Drives
Audio
About
Applications
Libraries
Graphics
Desktop Integration
Application settings
Wine can mimic different Windows versions for each application. This tab is linked to the Libraries and Graphics tabs to allow you to change system-wide or per-application settings in those tabs as well.
Default Settings
Add application...
Remove application
Windows Version:
Windows 7
Windows 10
Windows 8.1
Windows 8
Windows 2008 R2
Windows 7
Windows 2008
Windows Vista
Windows 2003
Windows XP

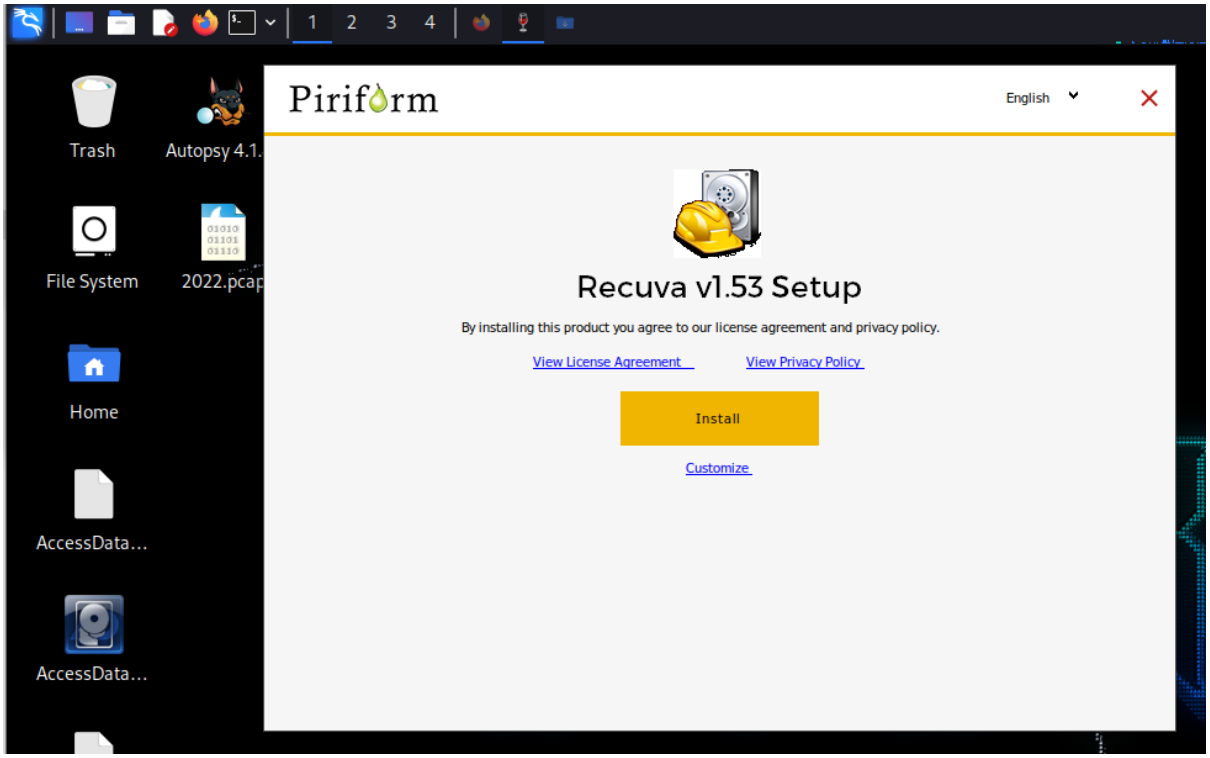

Wine configuration
Drives
Audio
About
Applications
Libraries
Graphics
Desktop Integration
Application settings
Wine can mimic different Windows versions for each application. This tab is linked to the Libraries and Graphics tabs to allow you to change system-wide or per-application settings in those tabs as well.
Default Settings
Add application...
Remove application
Windows Version:
Windows 10
OK
Cancel
Apply

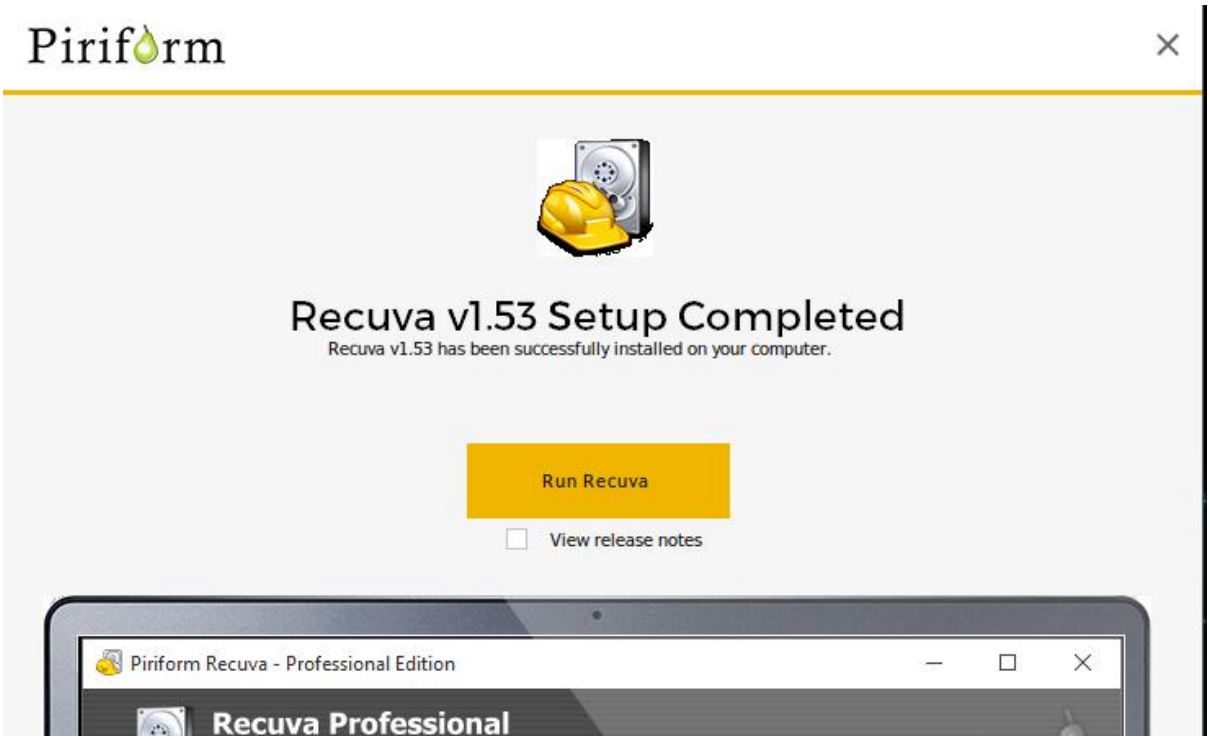

Wine configuration
Applications
Libraries
Graphics
Desktop Integration
Drives
Audio
About
Wine 7.0
https://www.winehq.org
This program is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.
Windows registration information
Owner:
Organization:
OK
Cancel
Apply

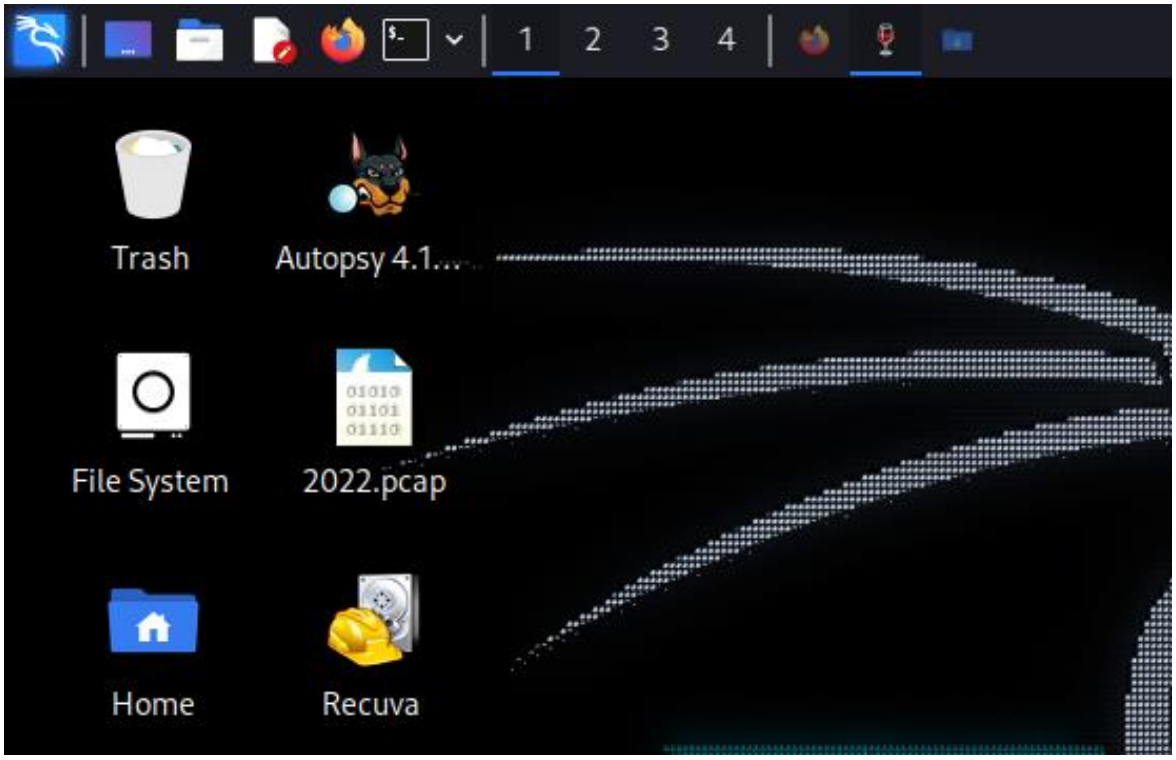
	FREE RECUVA	RECUVA PROFESSIONAL	CCLEANER PROFESSIONAL PLUS
Advanced file recovery	✓	✓	✓
Virtual hard drive support	✗	✓	✓
Automatic updates	✗	✓	✓
Premium support	✗	✓	✓
Complete cleaning	✗	✗	✓
CCleaner for Android Pro & Mac Pro	✗	✗	✓
	Download	Buy Now $19.95	Buy Now ~~$44.95~~ $39.95

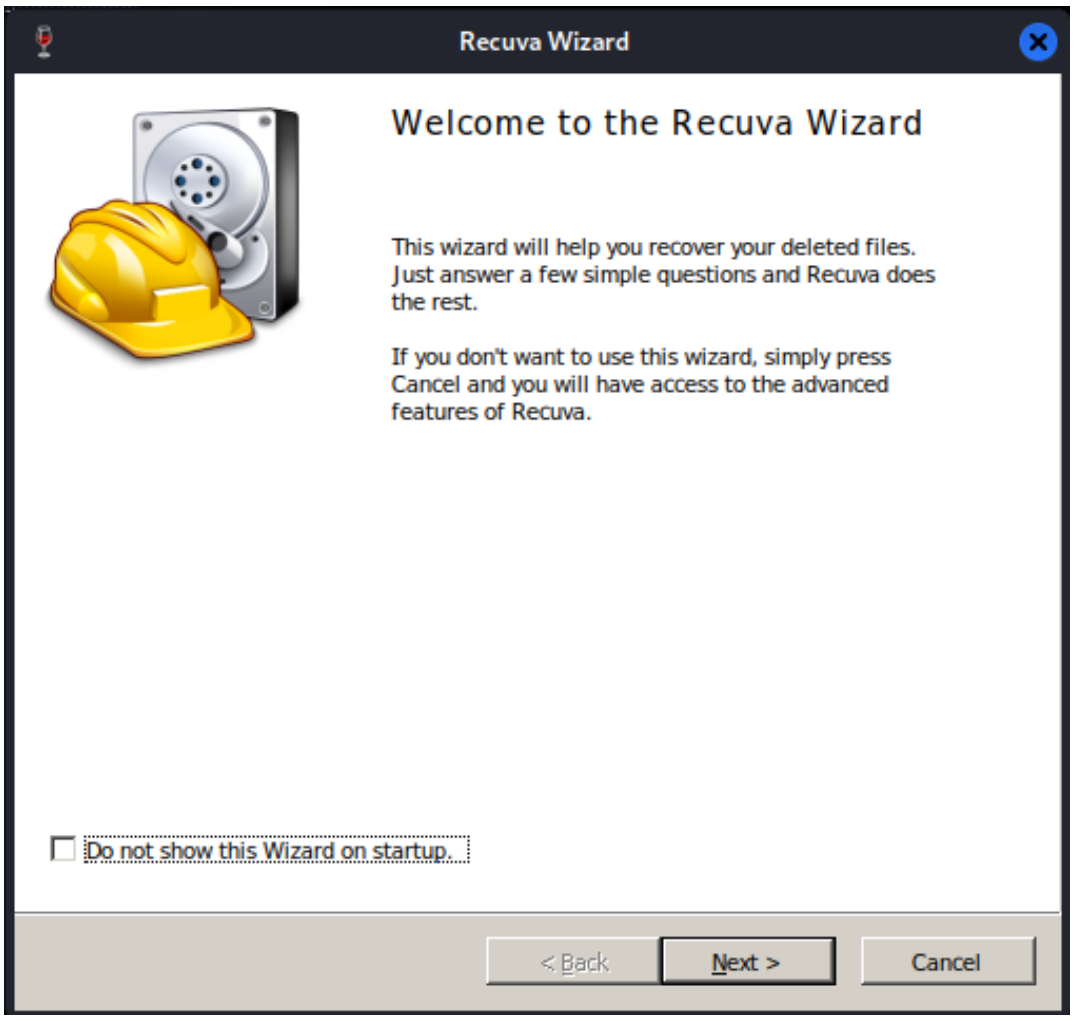




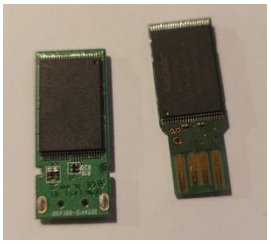

1 2 3 4
Trash
Autopsy 4.1.
File System
2022.pcap
Home
AccessData...
AccessData...
Piriform
English
Recuva v1.53 Setup
By installing this product you agree to our license agreement and privacy policy.
View License Agreement
View Privacy Policy
Install
Customize


Piriform
Recuva v1.53 Setup Completed
Recuva v1.53 has been successfully installed on your computer.
Run Recuva
View release notes
Piriform Recuva - Professional Edition
Recuva Professional


1
2
3
4
Trash
Autopsy 4.1...
File System
2022.pcap
Home
Recuva


Recuva Wizard
Welcome to the Recuva Wizard
This wizard will help you recover your deleted files. Just answer a few simple questions and Recuva does the rest.
If you don't want to use this wizard, simply press Cancel and you will have access to the advanced features of Recuva.
Do not show this Wizard on startup.
< Back
Next >
Cancel

Chapter 6: Understanding File Systems and Storage



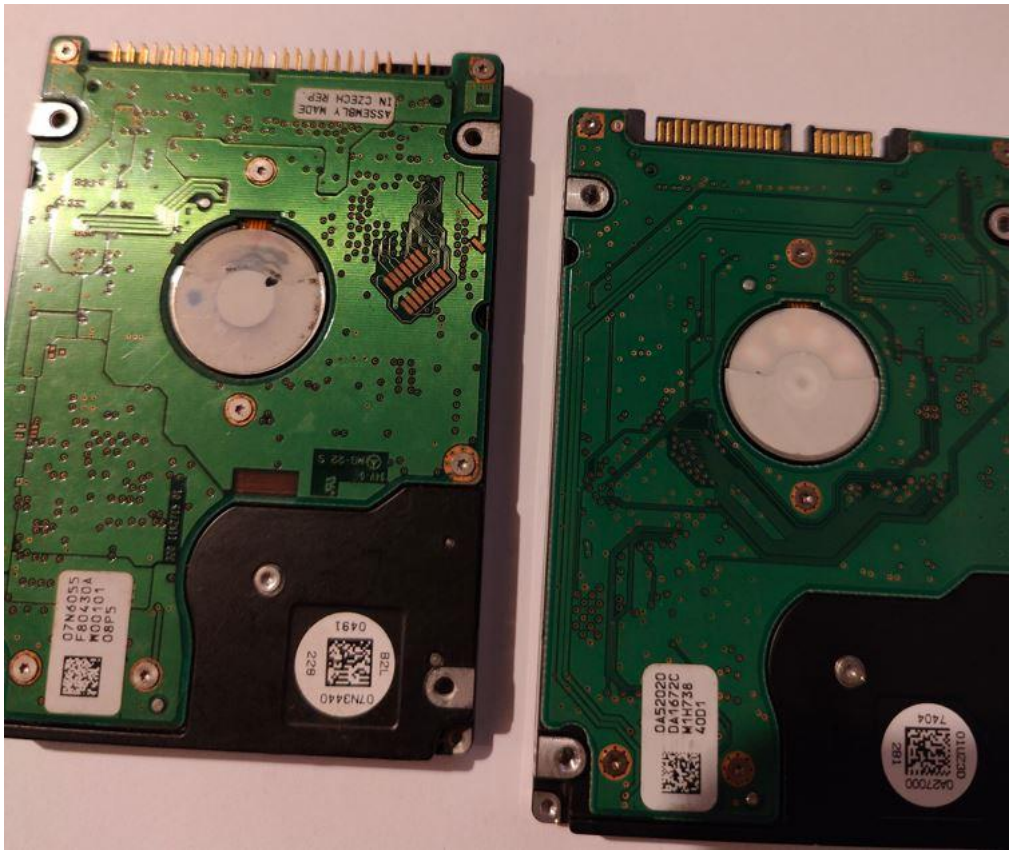

SAMSUNG
Made In China
LOT NO.20160503
DESIGNED BY SAMSUNG
SanDisk
MEMORY STICK PRO DUO
8GB
MAGICGATE
SONY
MEMORY STICK PRO DUO
2GB
MAGICGATE


Kingston
64GB
micro SD
XC I U
SAMSUNG
512
EVO
Select


CF MS
SD
SM

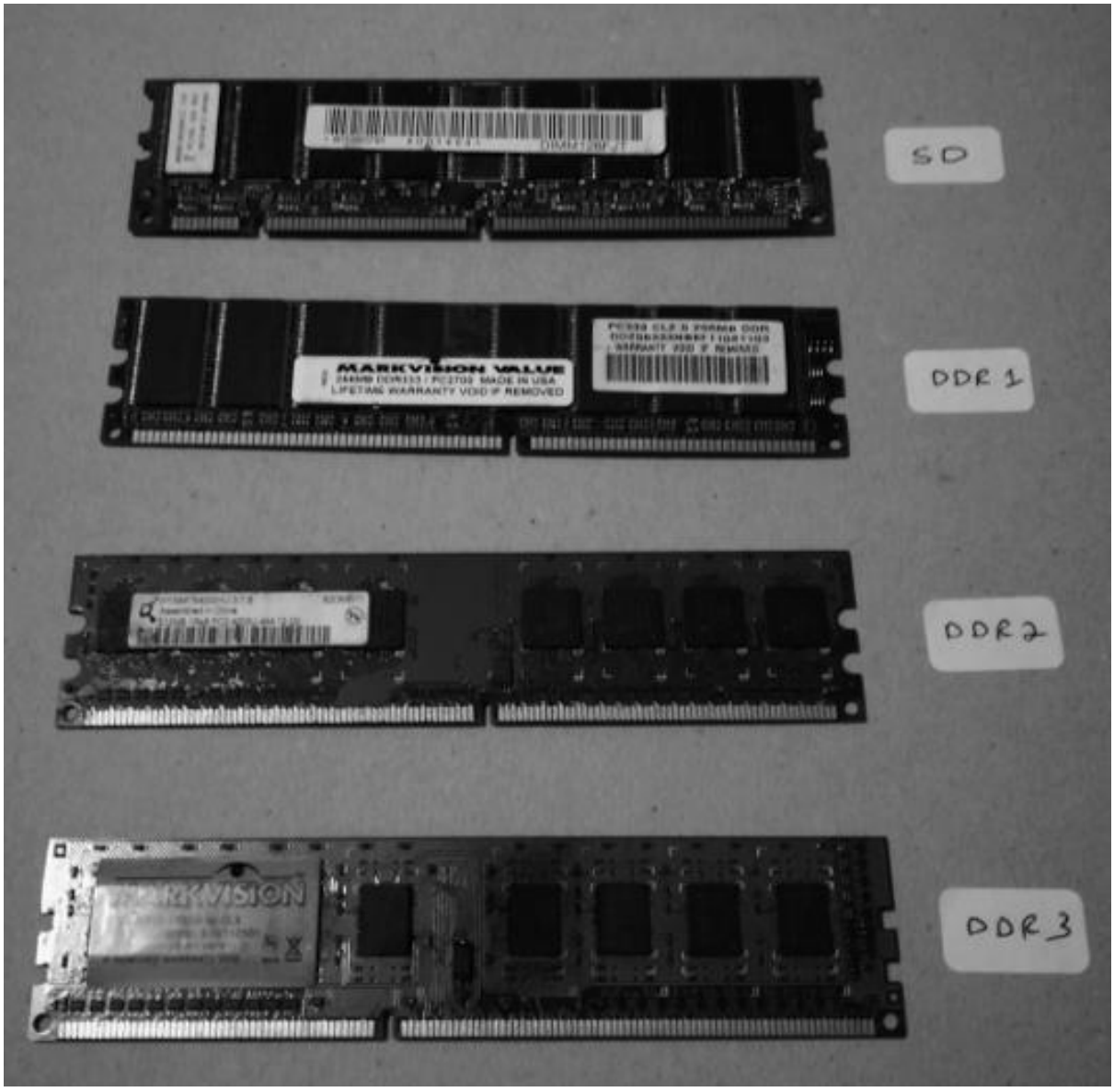

USB Type-C/OTG
Card Reader/Writer


82P1

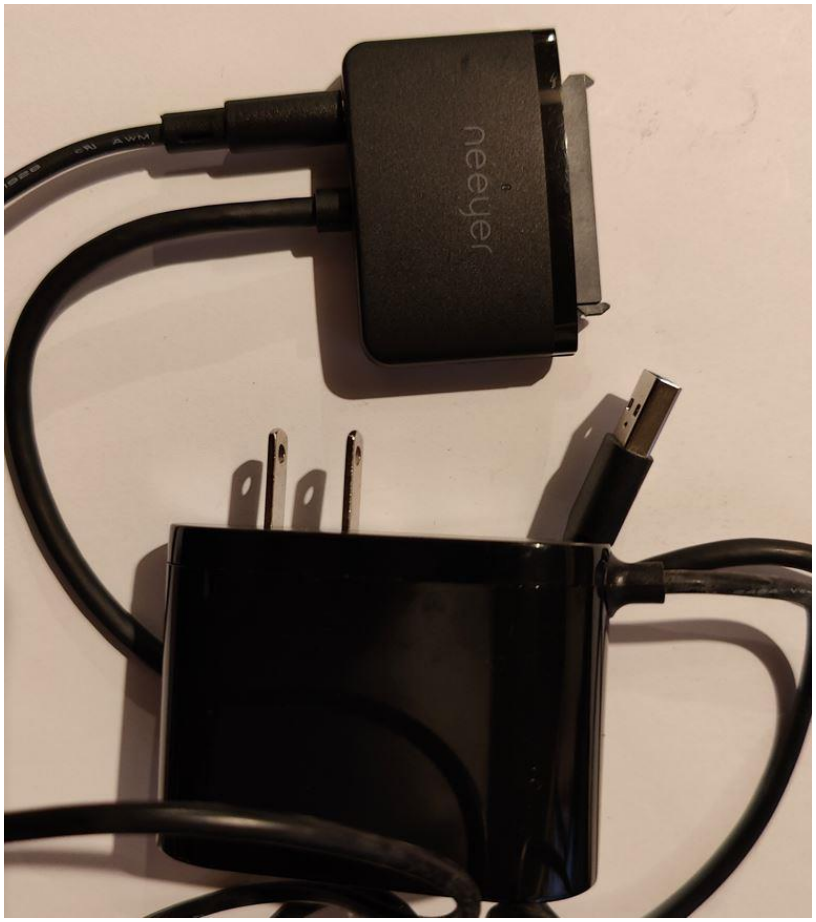

ASSEMBLY MADE IN CZECH REP
07N6055
F804304
M00101
08P5
0491
07N3440
228
828
DA52020
DA16720
M1H7738
4001
DA27000
7404
281
0822110

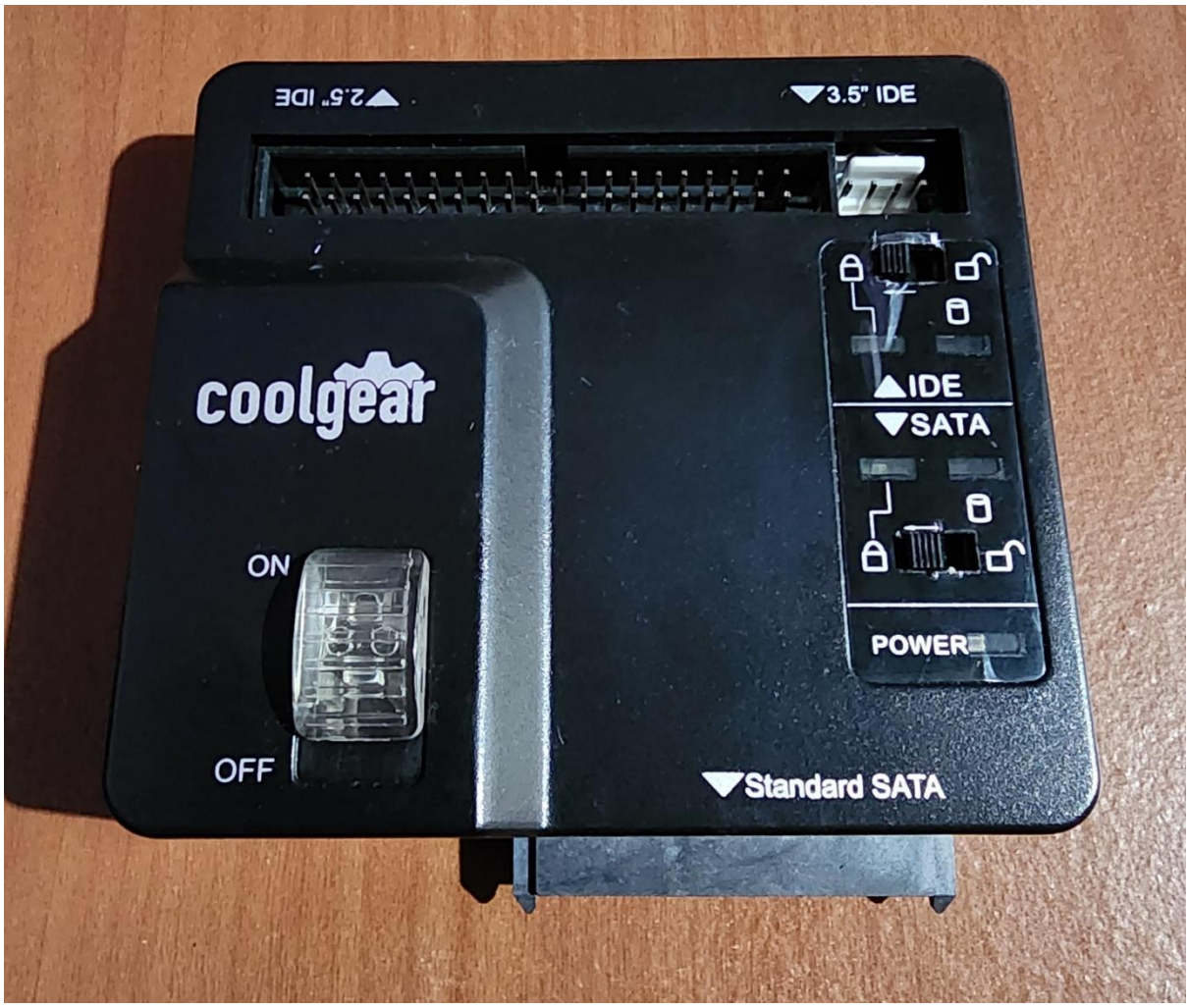

Seagate
Laptop SSHD
1000GB
CAUTION:
SATA
Capacity: 1000GB
5400 RPM
Firmware: DEM7
SN: W381DTV4
ST1000LM014
PN: 1EJ164-036
FW: DEM7
HDD Mfg by Seagate Technology LLC


SOLID STATE DRIVE


SD
MARKVISION VALUE
LIFETIME WARRANTY VOID IF REMOVED
DDR 1
DDR2
MARKVISION
DDR3

Chapter 7: Incident Response, Data Acquisitions, and DFIR Frameworks


neeyer


2.5" IDE
3.5" IDE
coolgear
IDE
SATA
ON
OFF
POWER
Standard SATA

Enter your text below:

Digital Forensics with Kali Linux

Generate | Clear All | SHA1 | SHA256 | SHA512 | Password Generator

☐ Treat each line as a separate string ☐ Lowercase hash(es)

MD5 Hash of your string: [Copy to clipboard]

`7E9506C4D9DD85220FB3DF671F09DA35`

Digital Forensics with ali Linux

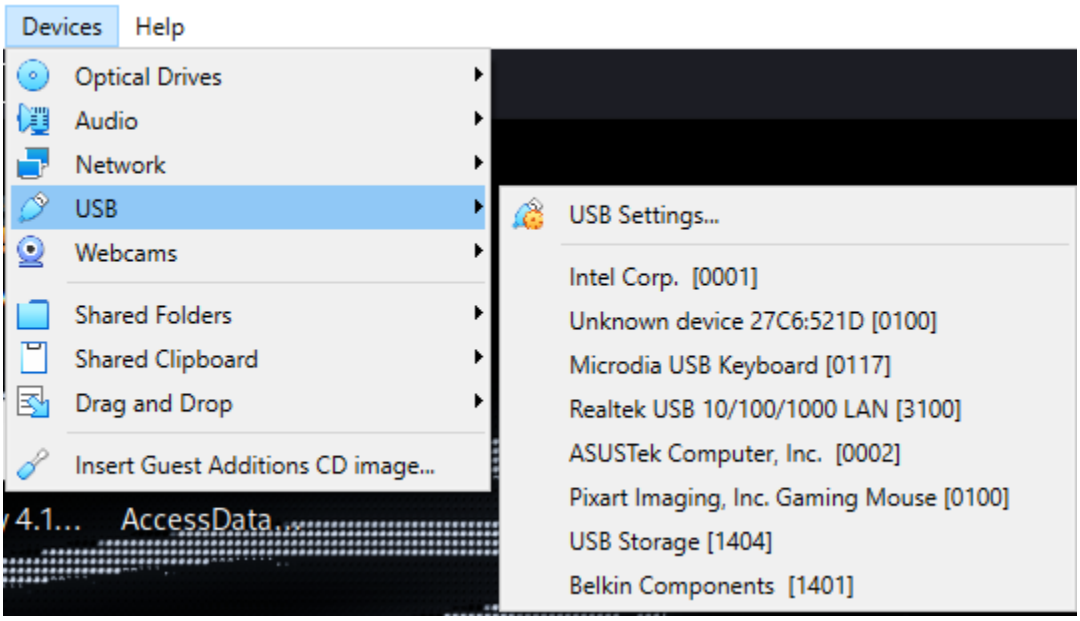
Generate | Clear All | SHA1 | SHA256 | SHA512 | Password Generator

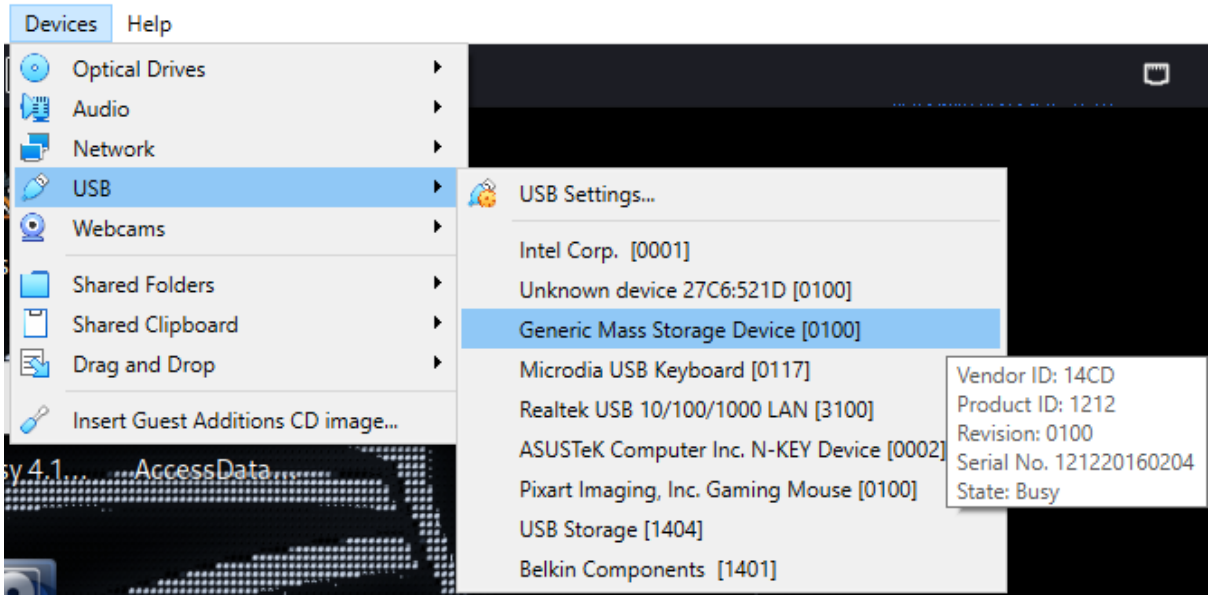
☐ Treat each line as a separate string ☐ Lowercase hash(es)

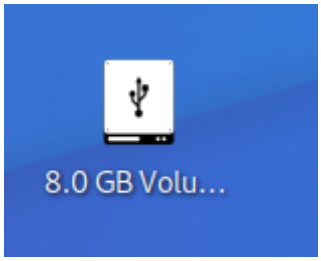
MD5 Hash of your string: [Copy to clipboard]

`7A4C7AA85B114E91F247779D6A0B3022`

Chapter 8: Evidence Acquisition Tools







```
┌──(cfsi㉿Research)-[~]
└─$ sudo fdisk -l
[sudo] password for cfsi:
Disk /dev/sda: 372.61 GiB, 400088457216 bytes, 781422768 sectors
Disk model: ST3400832NS
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0×ab60b093

Device     Boot     Start       End   Sectors   Size Id Type
/dev/sda1  *         2048 779421695 779419648 371.7G 83 Linux
/dev/sda2       779423742 781422591   1998850   976M  5 Extended
/dev/sda5       779423744 781422591   1998848   976M 82 Linux swap / Solaris


Disk /dev/sdb: 7.45 GiB, 8002732032 bytes, 15630336 sectors
Disk model: Multi-Card
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0×0fe98fd2

Device     Boot Start      End  Sectors  Size Id Type
/dev/sdb1  *     4476 15618427 15613952  7.4G  c W95 FAT32 (LBA)

┌──(cfsi㉿Research)-[~]
└─$
```

```
cfsi@Research: ~
File  Actions  Edit  View  Help
┌──(cfsi㉿Research)-[~]
└─$ sudo md5sum /dev/sdb
[sudo] password for cfsi:
54988d426a4a4b59ed1b4787cb75859a  /dev/sdb

┌──(cfsi㉿Research)-[~]
└─$ sudo sha1sum /dev/sdb
9f2bdb31da25693acb9acbe73d815996cd7e293b  /dev/sdb

┌──(cfsi㉿Research)-[~]
└─$ sudo sha256sum /dev/sdb
c5e037c4a16699409d18de9660bf0bd35753d746c4081d8b5c868a0a111578a4  /dev/sdb

┌──(cfsi㉿Research)-[~]
└─$
```

```
┌──(cfsi㉿Research)-[~]
└─$ sudo apt-get update
Get:1 http://kali.download/kali kali-rolling InRelease [30.6 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [18.7 MB]
Get:3 https://dl.google.com/linux/chrome/deb stable InRelease [1,811 B]
Get:4 https://dl.google.com/linux/chrome/deb stable/main amd64 Packages [1,095 B]
25% [2 Packages 7,005 kB/18.7 MB 37%]                                  187 kB/s 5min 3s
```

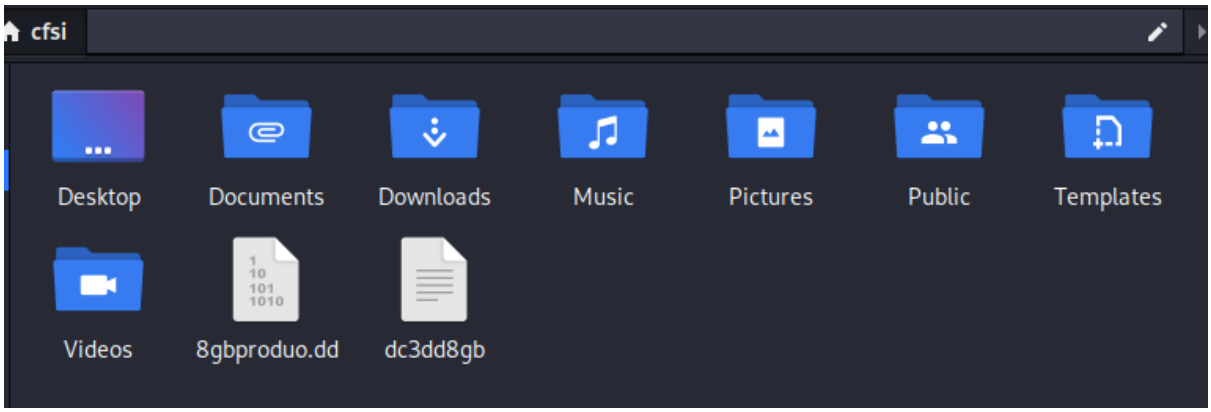
```
┌──(cfsi㉿Research)-[~]
└─$ sudo apt-get install dc3dd
[sudo] password for cfsi:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  dc3dd
0 upgraded, 1 newly installed, 0 to remove and 749 not upgraded.
Need to get 121 kB of archives.
After this operation, 501 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 dc3dd amd64 7.2.646-5
+b1 [121 kB]
Fetched 121 kB in 1s (151 kB/s)
Selecting previously unselected package dc3dd.
(Reading database ... 312296 files and directories currently installed.)
Preparing to unpack .../dc3dd_7.2.646-5+b1_amd64.deb ...
Unpacking dc3dd (7.2.646-5+b1) ...
Setting up dc3dd (7.2.646-5+b1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for kali-menu (2022.3.1) ...
```

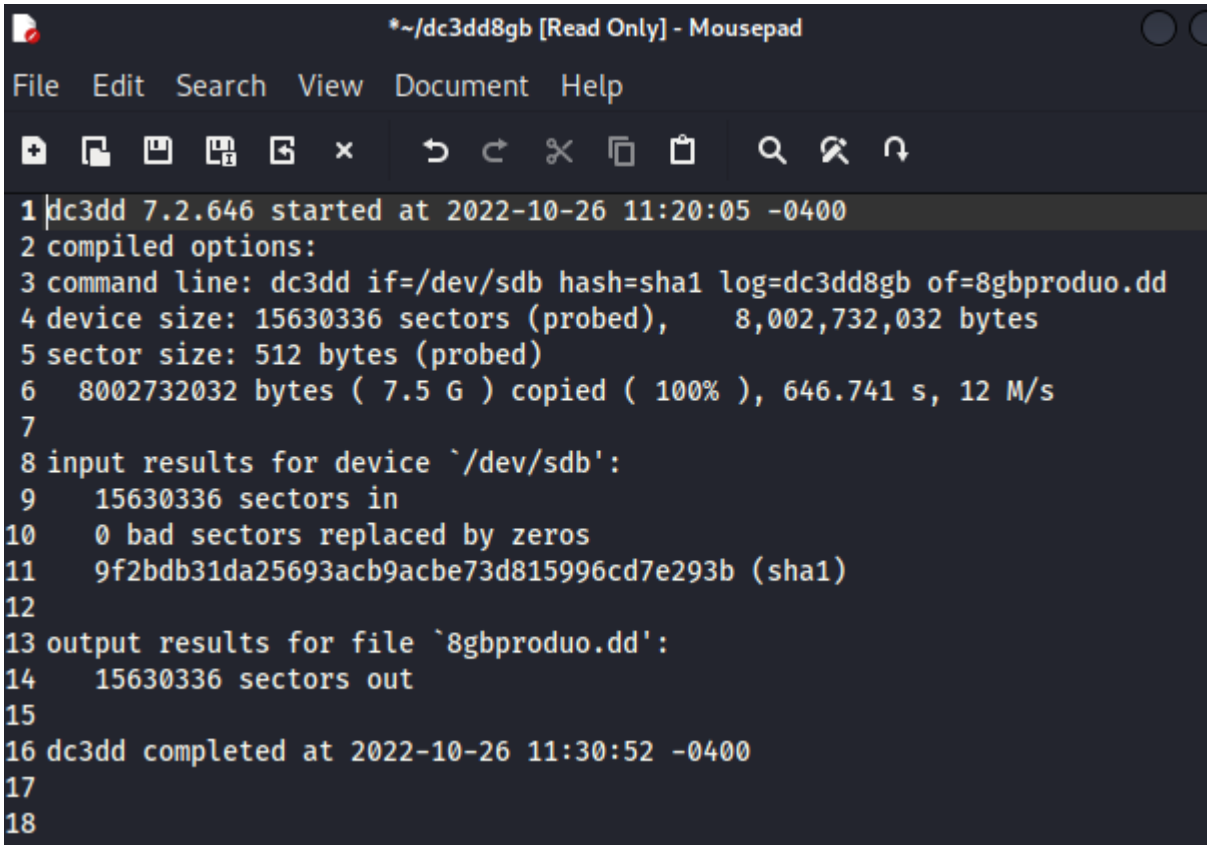
```
┌──(cfsi㉿Research)-[~]
└─$ dc3dd --help
─────
usage:
─────

        dc3dd [OPTION 1] [OPTION 2] ... [OPTION N]

                *or*

        dc3dd [HELP OPTION]

        where each OPTION is selected from the basic or advanced
        options listed below, or HELP OPTION is selected from the
        help options listed below.
```

```
┌──(cfsi㉿Research)-[~]
└─$ sudo dc3dd if=/dev/sdb hash=sha1 log=dc3dd8gb of=8gbproduo.dd

dc3dd 7.2.646 started at 2022-10-26 11:20:05 -0400
compiled options:
command line: dc3dd if=/dev/sdb hash=sha1 log=dc3dd8gb of=8gbproduo.dd
device size: 15630336 sectors (probed),    8,002,732,032 bytes
sector size: 512 bytes (probed)
^[[B^[[B^[[B^[[B^[[B^[[B
  349405184 bytes ( 333 M ) copied (  4% ),   28 s, 12 M/s
```

```
┌──(cfsi㉿Research)-[~]
└─$ sudo dc3dd if=/dev/sdb hash=sha1 log=dc3dd8gb of=8gbproduo.dd

dc3dd 7.2.646 started at 2022-10-26 11:20:05 -0400
compiled options:
command line: dc3dd if=/dev/sdb hash=sha1 log=dc3dd8gb of=8gbproduo.dd
device size: 15630336 sectors (probed),    8,002,732,032 bytes
sector size: 512 bytes (probed)
^[[B^[[B^[[B^[[B^[[B^[[B
  8002732032 bytes ( 7.5 G ) copied ( 100% ),  647 s, 12 M/s

input results for device `/dev/sdb':
   15630336 sectors in
   0 bad sectors replaced by zeros
   9f2bdb31da25693acb9acbe73d815996cd7e293b (sha1)

output results for file `8gbproduo.dd':
   15630336 sectors out

dc3dd completed at 2022-10-26 11:30:52 -0400
```

```
┌──(cfsi㉿Research)-[~]
└─$ ls
8gbproduo.dd  dc3dd8gb  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(cfsi㉿Research)-[~]
└─$
```






```
┌──(cfsi㉿Research)-[~]
└─$ sudo sha1sum /dev/sdb
[sudo] password for cfsi:
3b36efe65704c140b48df6dea3811c73b6091c0d  /dev/sdb
```

```
┌──(cfsi㉿Research)-[~]
└─$ cat 8gbproduo.dd | sha1sum
9f2bdb31da25693acb9acbe73d815996cd7e293b  -
```

```
┌──(cfsi㉿Research)-[~]
└─$ sudo dc3dd wipe=/dev/sdb
[sudo] password for cfsi:

dc3dd 7.2.646 started at 2022-10-27 10:09:33 -0400
compiled options:
command line: dc3dd wipe=/dev/sdb
device size: 15630336 sectors (probed),    8,002,732,032 bytes
sector size: 512 bytes (probed)
 4541087744 bytes ( 4.2 G ) copied ( 57% ),  122 s, 35 M/s
```

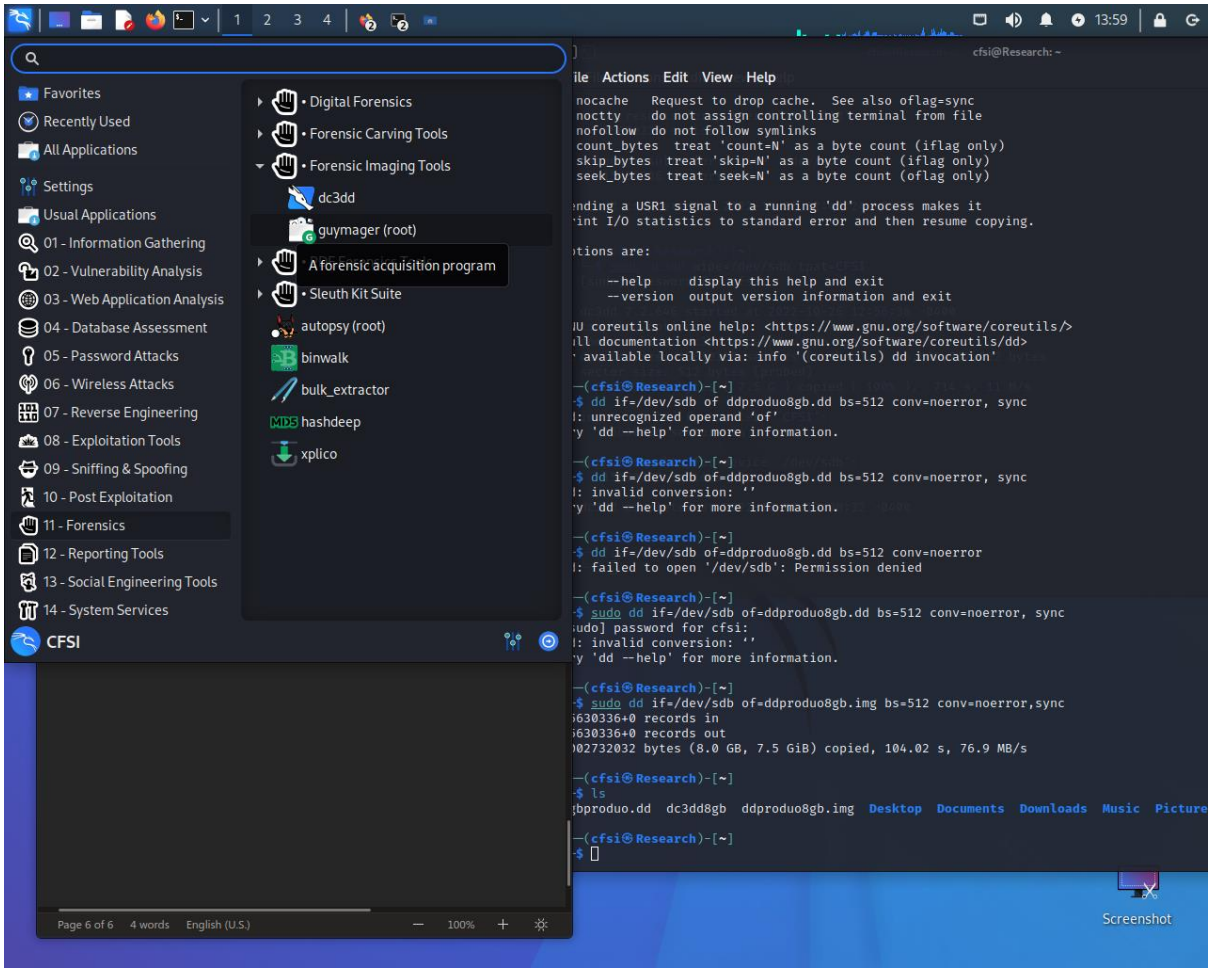
```
┌──(cfsi㉿Research)-[~]
└─$ sudo dc3dd wipe=/dev/sdb pat=10101010

dc3dd 7.2.646 started at 2022-10-26 12:33:29 -0400
compiled options:
command line: dc3dd wipe=/dev/sdb pat=10101010
device size: 15630336 sectors (probed),    8,002,732,032 bytes
sector size: 512 bytes (probed)
  8002732032 bytes ( 7.5 G ) copied ( 100% ),  715 s, 11 M/s

input results for pattern `10101010':
   15630336 sectors in

output results for device `/dev/sdb':
   15630336 sectors out

dc3dd completed at 2022-10-26 12:45:24 -0400
```

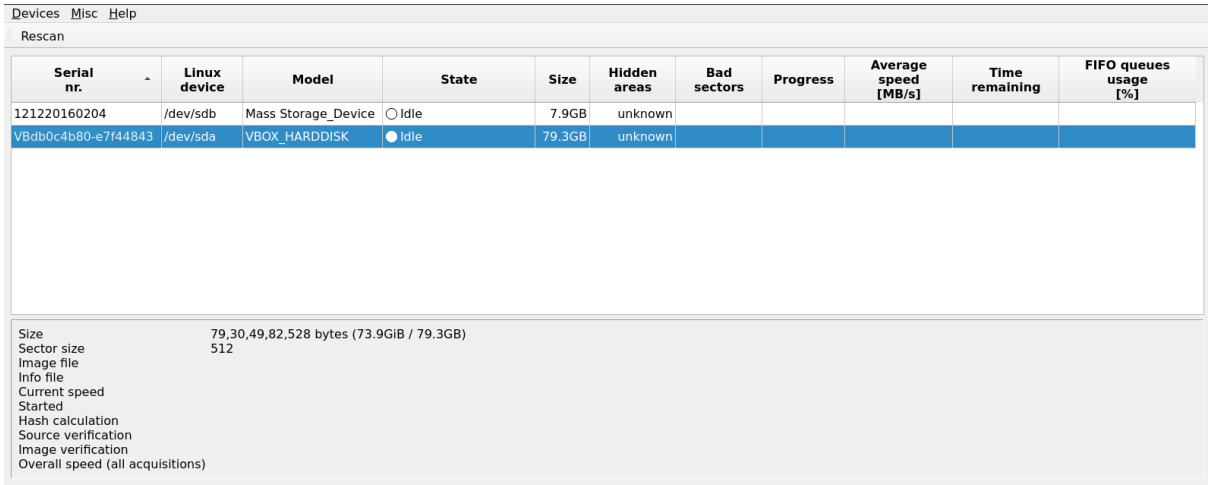
```
┌──(cfsi㉿Research)-[~]
└─$ sudo dc3dd wipe=/dev/sdb tpat=CFSI
[sudo] password for cfsi:
dc3dd 7.2.646 started at 2022-10-26 12:56:38 -0400
compiled options:
command line: dc3dd wipe=/dev/sdb tpat=CFSI
device size: 15630336 sectors (probed),    8,002,732,032 bytes
sector size: 512 bytes (probed)
  8002732032 bytes ( 7.5 G ) copied ( 100% ),  714 s, 11 M/s
input results for pattern `CFSI':
   15630336 sectors in

output results for device `/dev/sdb':
   15630336 sectors out

dc3dd completed at 2022-10-26 13:08:32 -0400
```

```
root@kali:~# dd --help
Usage: dd [OPERAND]...
  or:  dd OPTION
Copy a file, converting and formatting according to the operands.

  bs=BYTES        read and write up to BYTES bytes at a time (default: 512);
                  overrides ibs and obs
  cbs=BYTES       convert BYTES bytes at a time
  conv=CONVS      convert the file as per the comma separated symbol list
  count=N         copy only N input blocks
  ibs=BYTES       read up to BYTES bytes at a time (default: 512)
  if=FILE         read from FILE instead of stdin
  iflag=FLAGS     read as per the comma separated symbol list
  obs=BYTES       write BYTES bytes at a time (default: 512)
  of=FILE         write to FILE instead of stdout
  oflag=FLAGS     write as per the comma separated symbol list
  seek=N          skip N obs-sized blocks at start of output
  skip=N          skip N ibs-sized blocks at start of input
  status=LEVEL    The LEVEL of information to print to stderr;
                  'none' suppresses everything but error messages,
                  'noxfer' suppresses the final transfer statistics,
                  'progress' shows periodic transfer statistics

N and BYTES may be followed by the following multiplicative suffixes:
c =1, w =2, b =512, kB =1000, K =1024, MB =1000*1000, M =1024*1024, xM =M,
GB =1000*1000*1000, G =1024*1024*1024, and so on for T, P, E, Z, Y.

Each CONV symbol may be:

  ascii     from EBCDIC to ASCII
  ebcdic    from ASCII to EBCDIC
  ibm       from ASCII to alternate EBCDIC
  block     pad newline-terminated records with spaces to cbs-size
  unblock   replace trailing spaces in cbs-size records with newline
  lcase     change upper case to lower case
  ucase     change lower case to upper case
  sparse    try to seek rather than write the output for NUL input blocks
  swab      swap every pair of input bytes
```

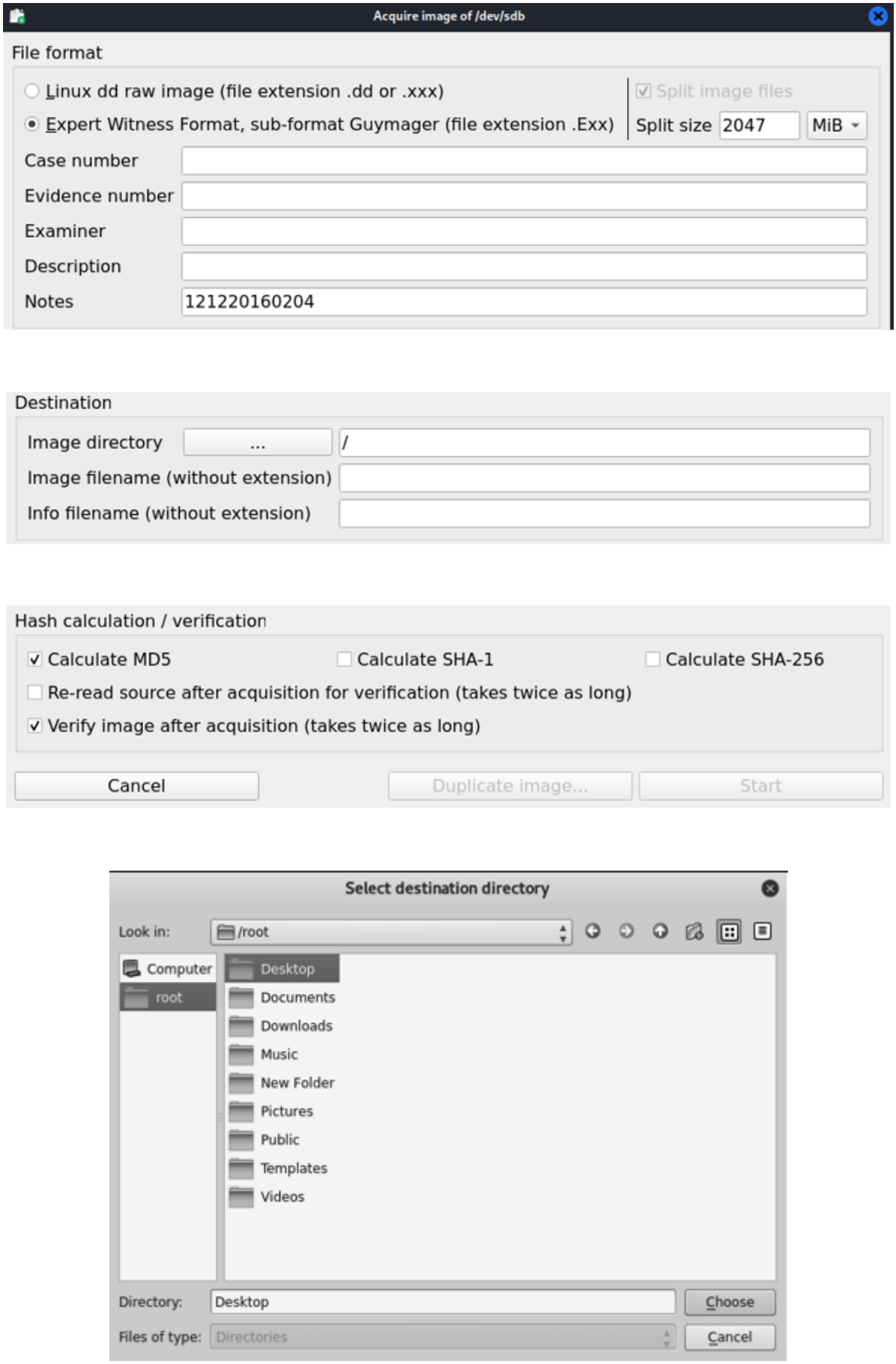
```
┌──(cfsi㉿Research)-[~]
└─$ sudo dd if=/dev/sdb of=ddproduo8gb.img bs=512 conv=noerror,sync
15630336+0 records in
15630336+0 records out
8002732032 bytes (8.0 GB, 7.5 GiB) copied, 104.02 s, 76.9 MB/s

┌──(cfsi㉿Research)-[~]
```

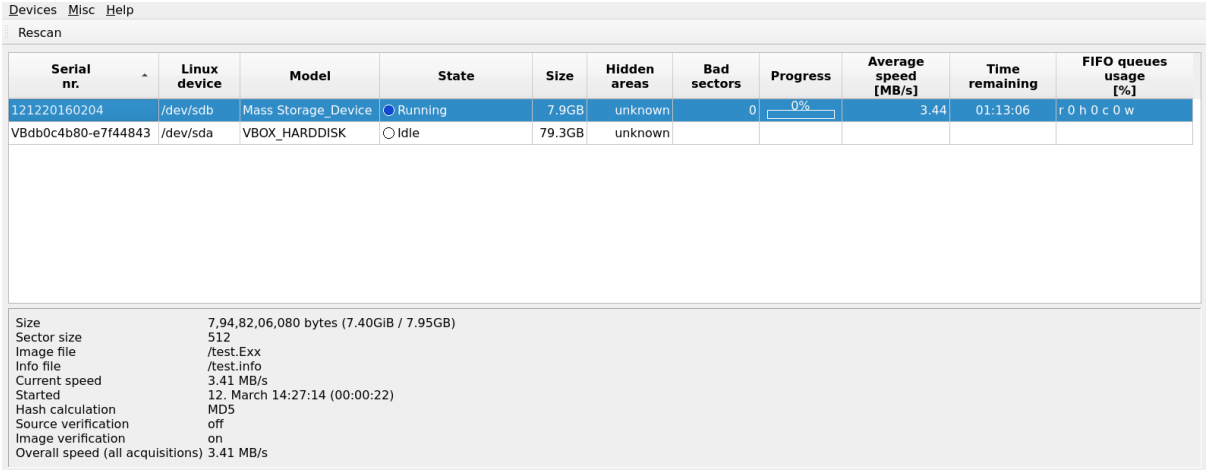
```
┌──(cfsi㉿Research)-[~]
└─$ ls
8gbproduo.dd  dc3dd8gb
```

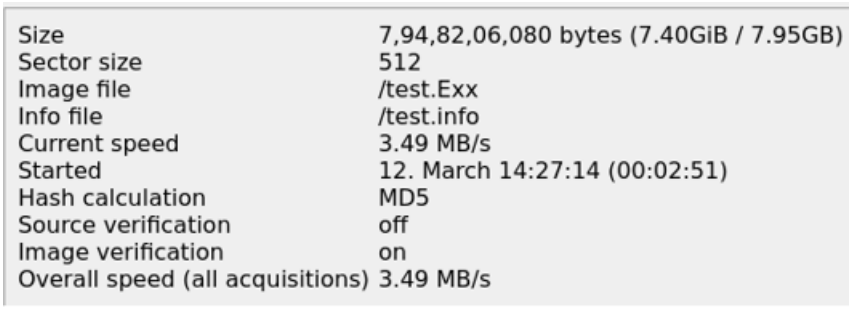

Favorites
Recently Used
All Applications
Settings
Usual Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
14 - System Services
CFSI
• Digital Forensics
• Forensic Carving Tools
• Forensic Imaging Tools
dc3dd
guymager (root)
A forensic acquisition program
• Sleuth Kit Suite
autopsy (root)
binwalk
bulk_extractor
hashdeep
xplico
Page 6 of 6
4 words
English (U.S.)
100%
Screenshot

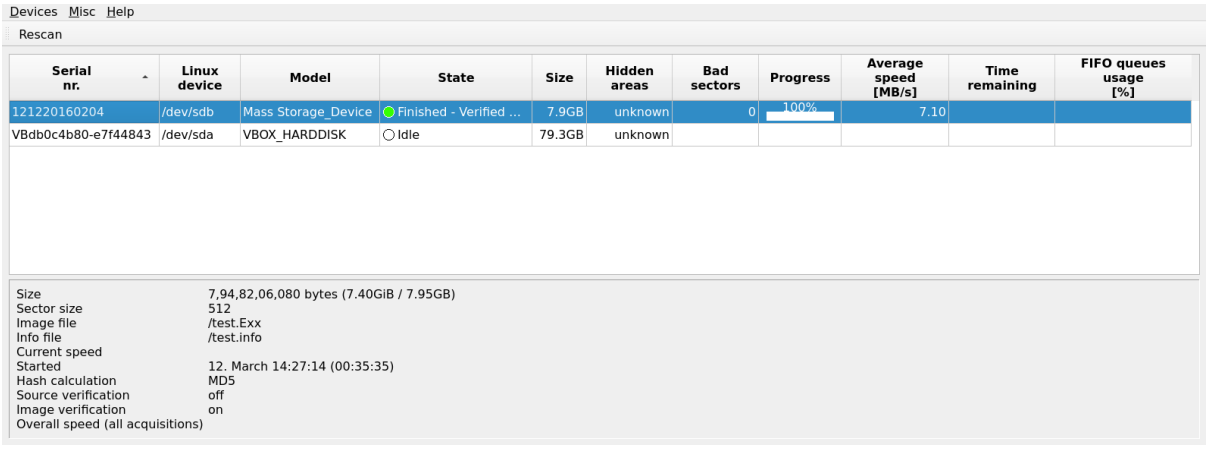

Devices Misc Help
Rescan
Serial nr.
Linux device
Model
State
Size
Hidden areas
Bad sectors
Progress
Average speed [MB/s]
Time remaining
FIFO queues usage [%]
121220160204 /dev/sdb Mass Storage_Device Idle 7.9GB unknown
VBdb0c4b80-e7f44843 /dev/sda VBOX_HARDDISK Idle 79.3GB unknown
Size 79,30,49,82,528 bytes (73.9GiB / 79.3GB)
Sector size 512
Image file
Info file
Current speed
Started
Hash calculation
Source verification
Image verification
Overall speed (all acquisitions)


Acquire image
Clone device
Abort
Info

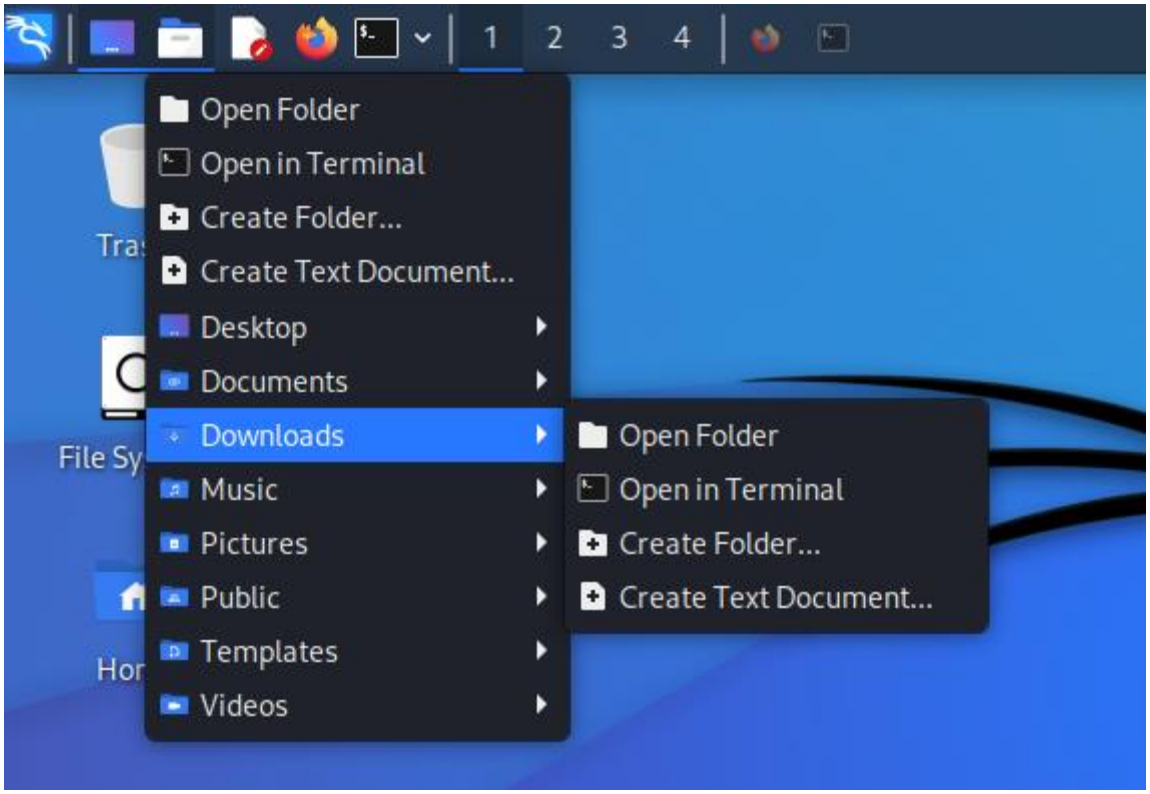

Acquire image of /dev/sdb
File format
Linux dd raw image (file extension .dd or .xxx)
Expert Witness Format, sub-format Guymager (file extension .Exx)
Split image files
Split size
2047
MiB
Case number
Evidence number
Examiner
Description
Notes
121220160204
Destination
Image directory
...
/
Image filename (without extension)
Info filename (without extension)
Hash calculation / verification
Calculate MD5
Calculate SHA-1
Calculate SHA-256
Re-read source after acquisition for verification (takes twice as long)
Verify image after acquisition (takes twice as long)
Cancel
Duplicate image...
Start
Select destination directory
Look in:
/root
Computer
root
Desktop
Documents
Downloads
Music
New Folder
Pictures
Public
Templates
Videos
Directory:
Desktop
Choose
Files of type:
Directories
Cancel

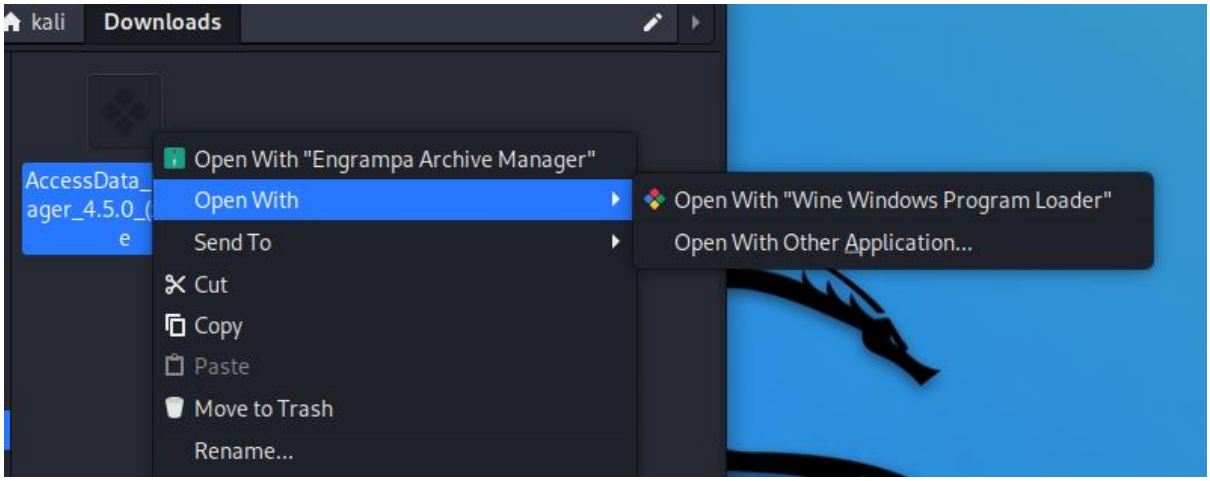

Devices Misc Help
Rescan
Serial nr. | Linux device | Model | State | Size | Hidden areas | Bad sectors | Progress | Average speed [MB/s] | Time remaining | FIFO queues usage [%]
121220160204 | /dev/sdb | Mass Storage_Device | Running | 7.9GB | unknown | 0 | 0% | 3.44 | 01:13:06 | r 0 h 0 c 0 w
VBdb0c4b80-e7f44843 | /dev/sda | VBOX_HARDDISK | Idle | 79.3GB | unknown
Size 7,94,82,06,080 bytes (7.40GiB / 7.95GB)
Sector size 512
Image file /test.Exx
Info file /test.info
Current speed 3.41 MB/s
Started 12. March 14:27:14 (00:00:22)
Hash calculation MD5
Source verification off
Image verification on
Overall speed (all acquisitions) 3.41 MB/s

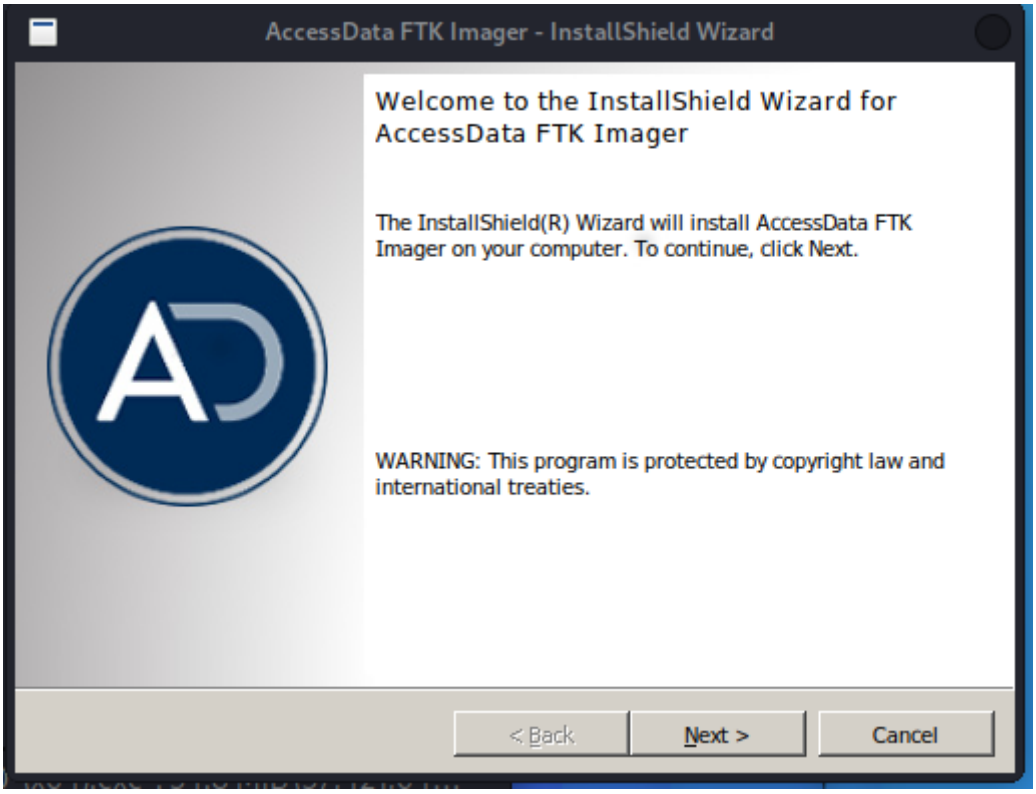

Size 7,94,82,06,080 bytes (7.40GiB / 7.95GB)
Sector size 512
Image file /test.Exx
Info file /test.info
Current speed 3.49 MB/s
Started 12. March 14:27:14 (00:02:51)
Hash calculation MD5
Source verification off
Image verification on
Overall speed (all acquisitions) 3.49 MB/s

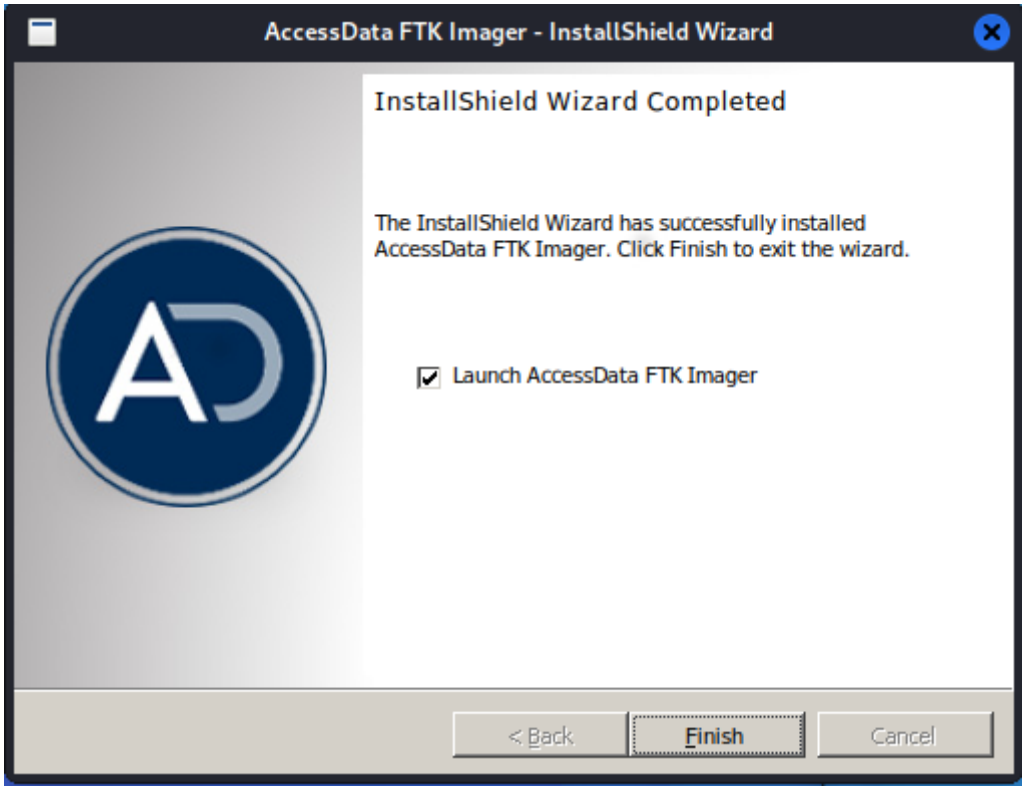

Devices Misc Help
Rescan
Serial nr. | Linux device | Model | State | Size | Hidden areas | Bad sectors | Progress | Average speed [MB/s] | Time remaining | FIFO queues usage [%]
121220160204 | /dev/sdb | Mass Storage_Device | Finished - Verified ... | 7.9GB | unknown | 0 | 100% | 7.10
VBdb0c4b80-e7f44843 | /dev/sda | VBOX_HARDDISK | Idle | 79.3GB | unknown
Size 7,94,82,06,080 bytes (7.40GiB / 7.95GB)
Sector size 512
Image file /test.Exx
Info file /test.info
Current speed
Started 12. March 14:27:14 (00:35:35)
Hash calculation MD5
Source verification off
Image verification on
Overall speed (all acquisitions)

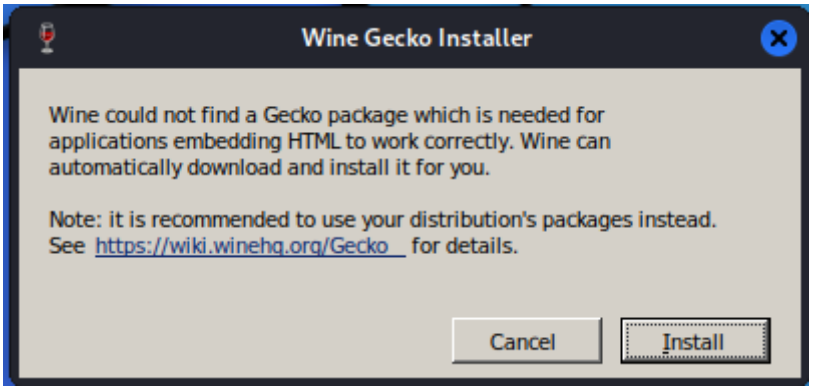

MD5 hash : 7d9171d9c5aabf743799ce4a323a9d45
MD5 hash verified source : --
MD5 hash verified image : 7d9171d9c5aabf743799ce4a323a9d45
SHA1 hash : --
SHA1 hash verified source : --
SHA1 hash verified image : --
SHA256 hash : --
SHA256 hash verified source: --
SHA256 hash verified image : --
Image verification OK. The image contains exactly the data that was written.

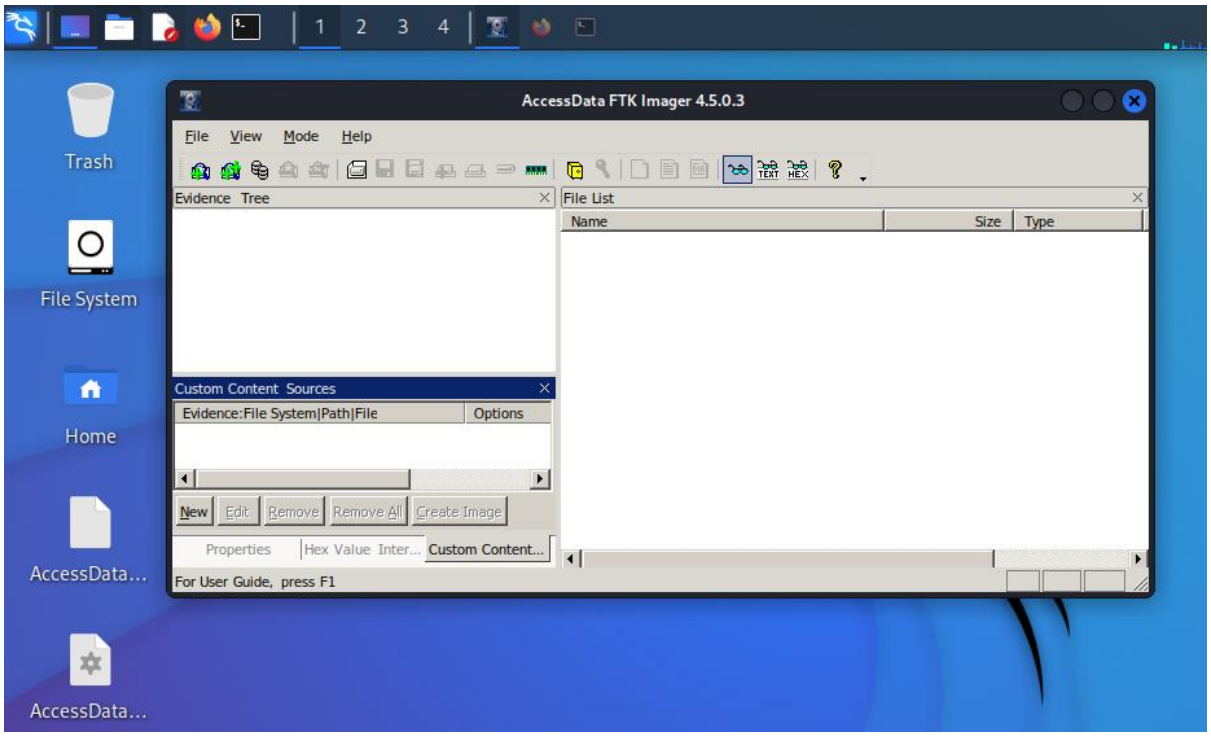

1
2
3
4
Open Folder
Open in Terminal
Create Folder...
Create Text Document...
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
Open Folder
Open in Terminal
Create Folder...
Create Text Document...

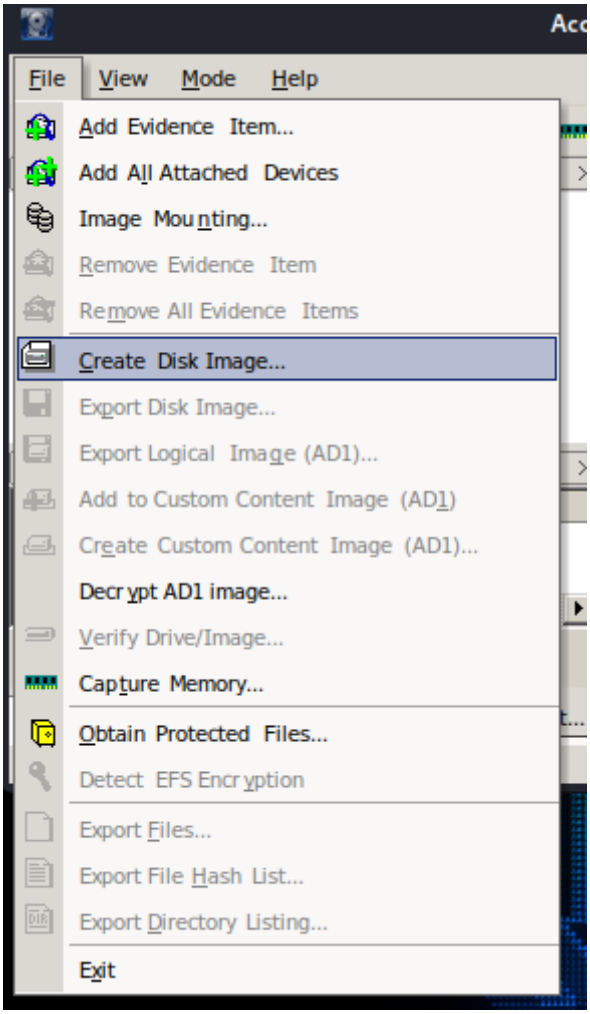

kali
Downloads
Open With "Engrampa Archive Manager"
Open With
Send To
Cut
Copy
Paste
Move to Trash
Rename...
Open With "Wine Windows Program Loader"
Open With Other Application...

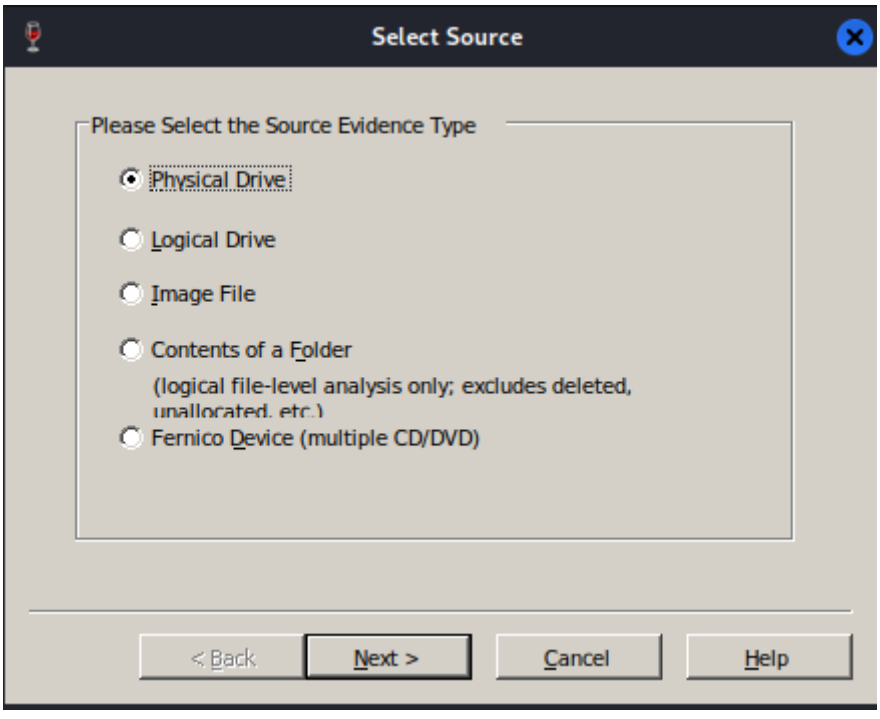

AccessData FTK Imager - InstallShield Wizard
Welcome to the InstallShield Wizard for AccessData FTK Imager
The InstallShield(R) Wizard will install AccessData FTK Imager on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

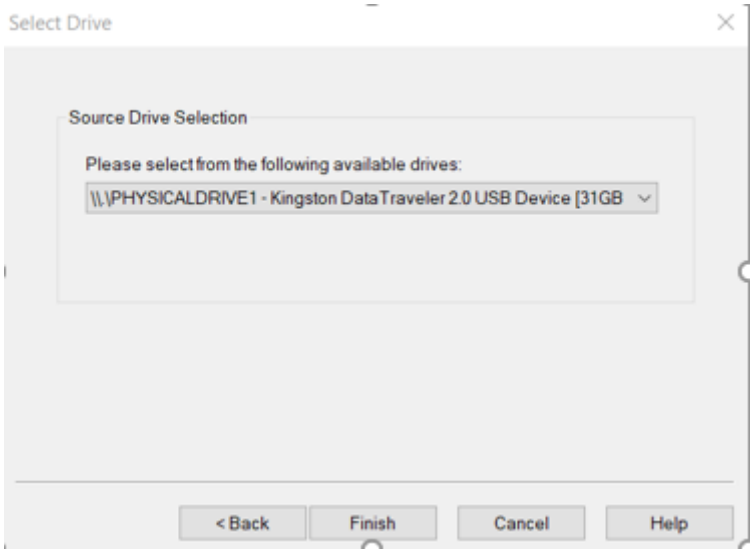

AccessData FTK Imager - InstallShield Wizard
InstallShield Wizard Completed
The InstallShield Wizard has successfully installed AccessData FTK Imager. Click Finish to exit the wizard.
Launch AccessData FTK Imager
< Back
Finish
Cancel

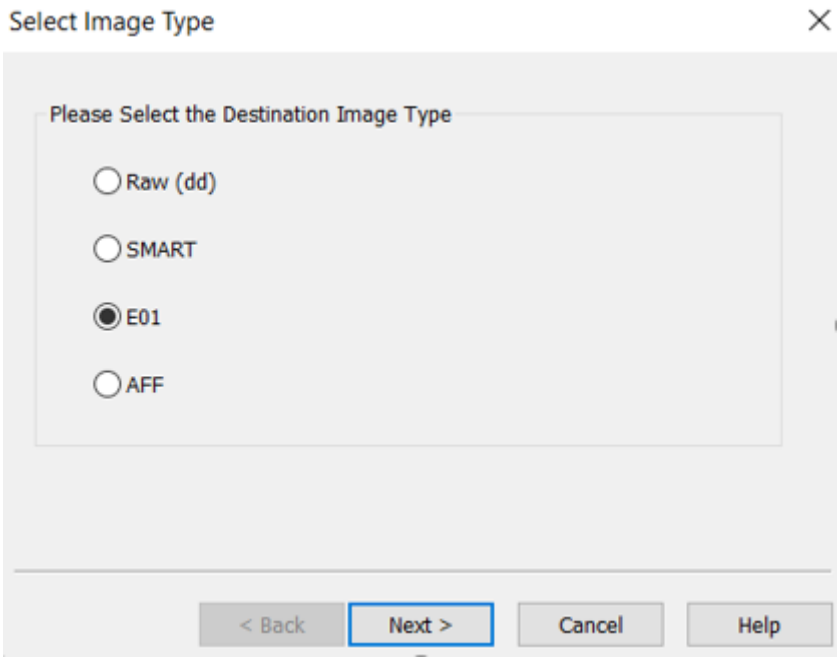

Wine Gecko Installer
Wine could not find a Gecko package which is needed for applications embedding HTML to work correctly. Wine can automatically download and install it for you.
Note: it is recommended to use your distribution's packages instead.
See https://wiki.winehq.org/Gecko for details.
Cancel
Install

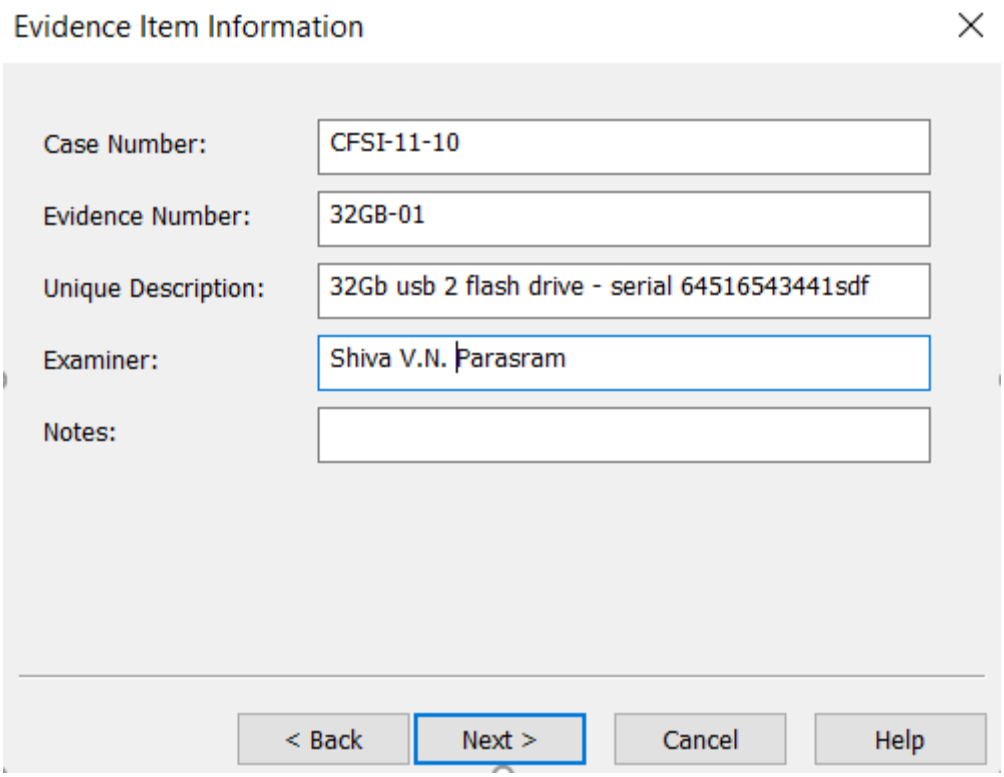

1 2 3 4
Trash
File System
Home
AccessData...
AccessData...
AccessData FTK Imager 4.5.0.3
File View Mode Help
Evidence Tree
File List
Name Size Type
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Content...
For User Guide, press F1

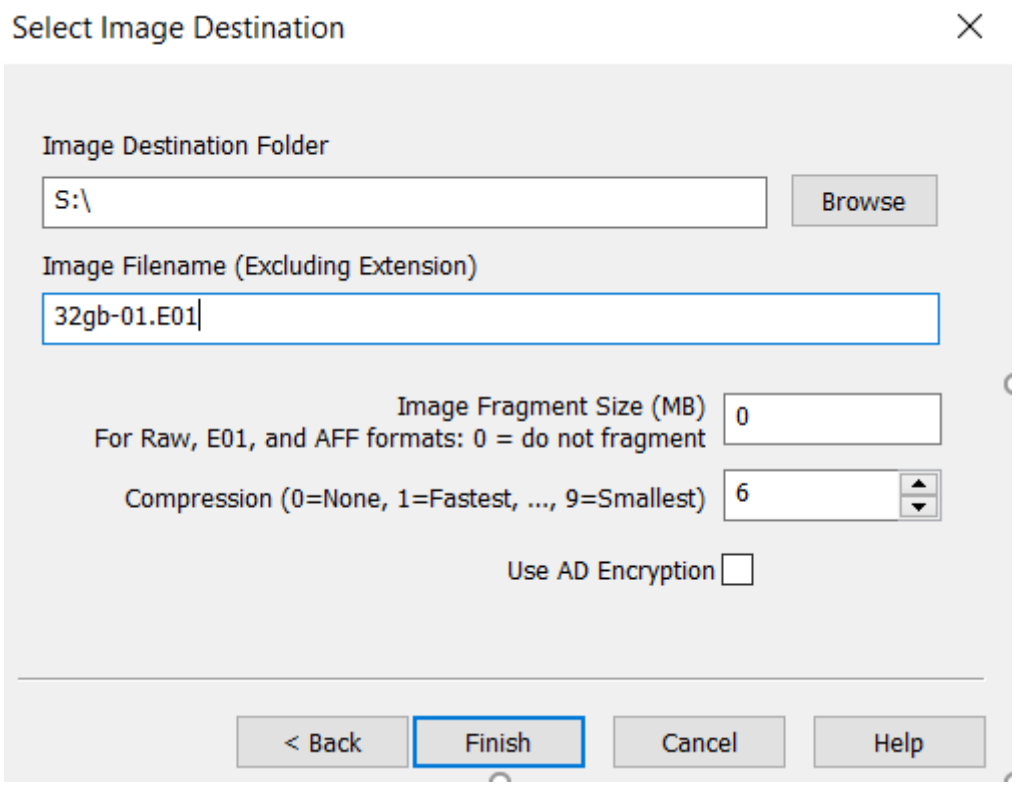

File
View
Mode
Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...
Decrypt AD1 image...
Verify Drive/Image...
Capture Memory...
Obtain Protected Files...
Detect EFS Encryption
Export Files...
Export File Hash List...
Export Directory Listing...
Exit

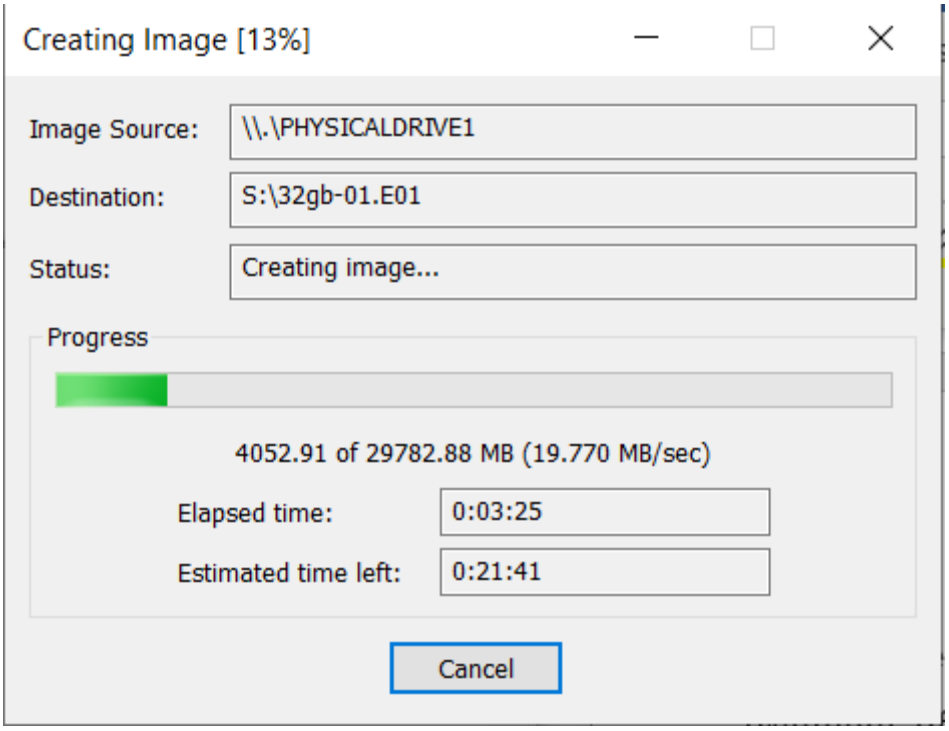

Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted,
unallocated, etc.)
Fernico Device (multiple CD/DVD)
< Back
Next >
Cancel
Help

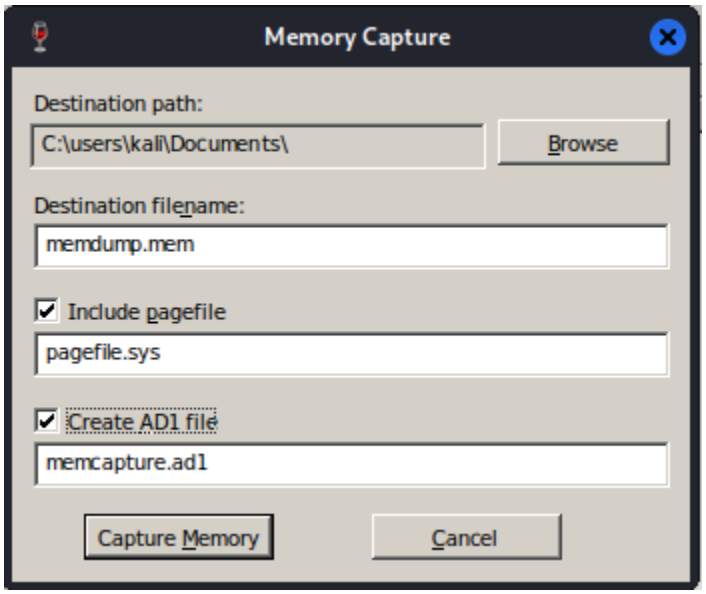

Select Drive
Source Drive Selection
Please select from the following available drives:
\\.\PHYSICALDRIVE1 - Kingston DataTraveler 2.0 USB Device [31GB
< Back
Finish
Cancel
Help

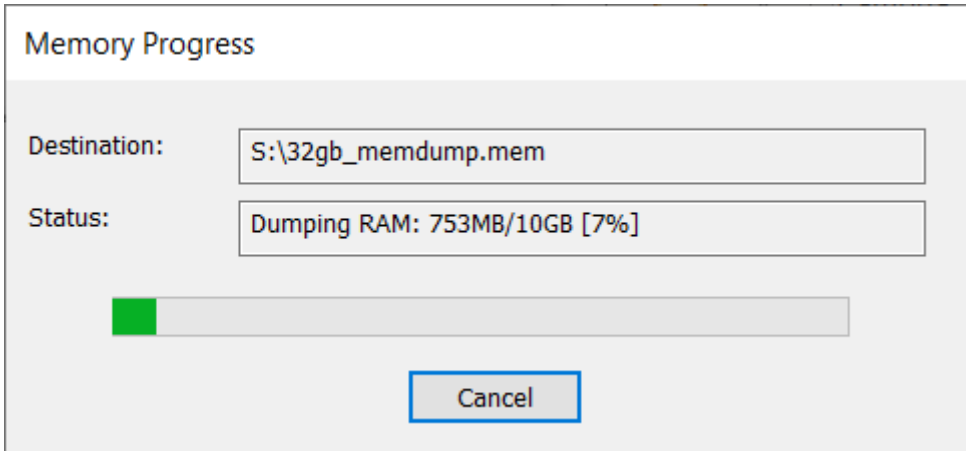

Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< Back
Next >
Cancel
Help

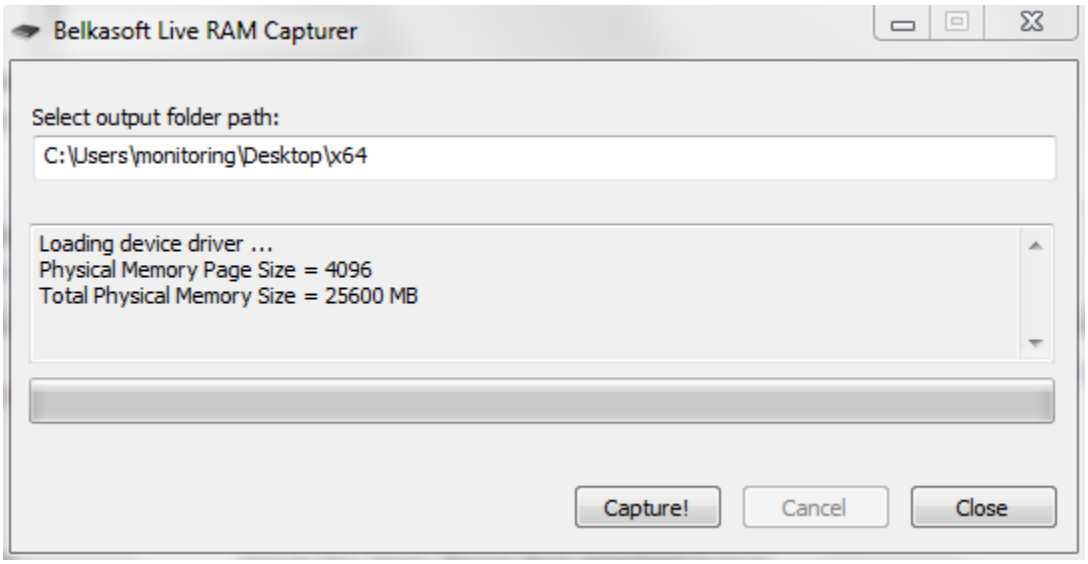

Evidence Item Information
Case Number:
CFSI-11-10
Evidence Number:
32GB-01
Unique Description:
32Gb usb 2 flash drive - serial 64516543441sdf
Examiner:
Shiva V.N. Parasram
Notes:
< Back
Next >
Cancel
Help


Select Image Destination
Image Destination Folder
S:\
Browse
Image Filename (Excluding Extension)
32gb-01.E01
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment
0
Compression (0=None, 1=Fastest, ..., 9=Smallest)
6
Use AD Encryption
< Back
Finish
Cancel
Help

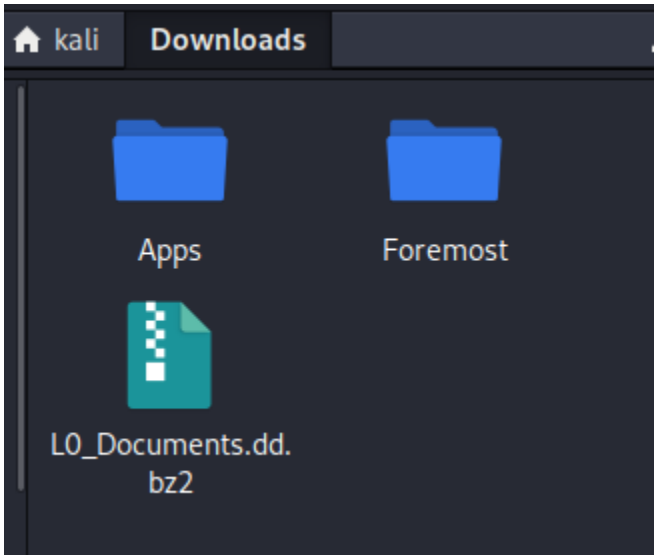

Creating Image [13%]
Image Source:
\\.\PHYSICALDRIVE1
Destination:
S:\32gb-01.E01
Status:
Creating image...
Progress
4052.91 of 29782.88 MB (19.770 MB/sec)
Elapsed time:
0:03:25
Estimated time left:
0:21:41
Cancel

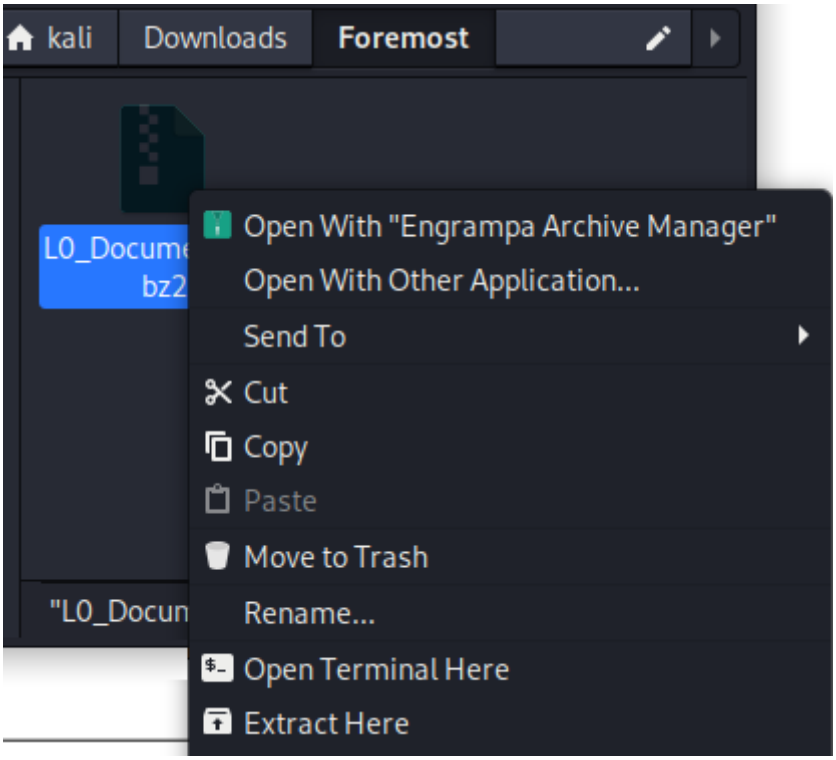

Memory Capture
Destination path:
C:\users\kali\Documents\
Browse
Destination filename:
memdump.mem
Include pagefile
pagefile.sys
Create AD1 file
memcapture.ad1
Capture Memory
Cancel

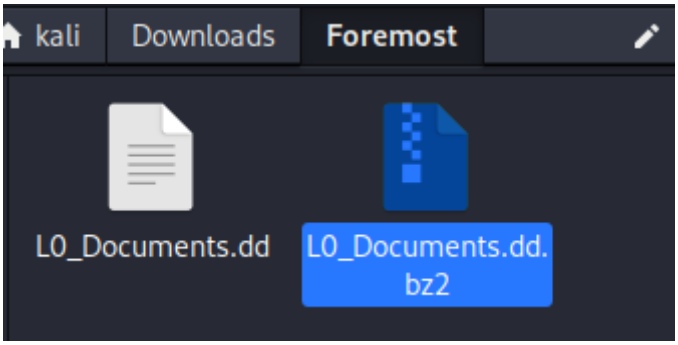

Memory Progress
Destination:
S:\32gb_memdump.mem
Status:
Dumping RAM: 753MB/10GB [7%]
Cancel


Belkasoft Live RAM Capturer
Select output folder path:
C:\Users\monitoring\Desktop\x64
Loading device driver ...
Physical Memory Page Size = 4096
Total Physical Memory Size = 25600 MB
Capture!
Cancel
Close

Chapter 9: File Recovery and Data Carving Tools



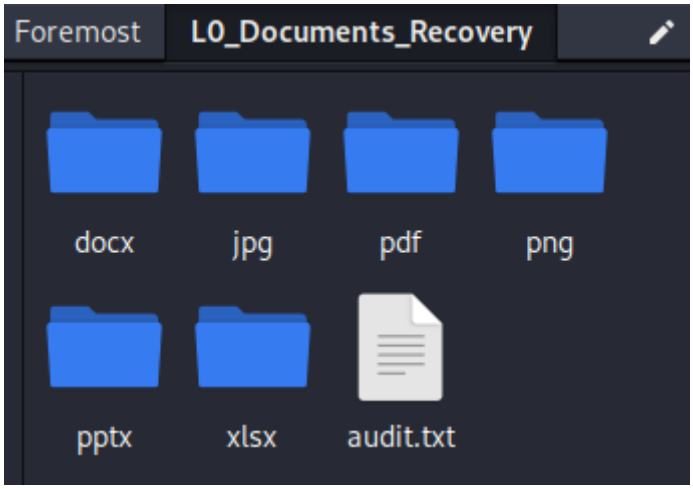




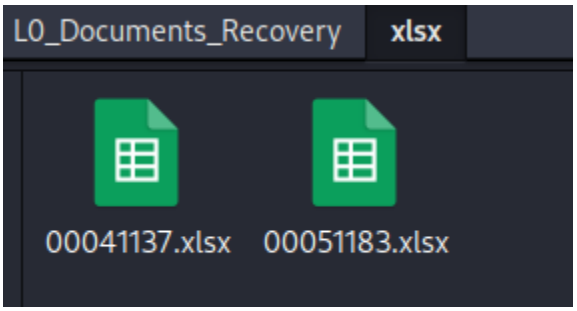

```
┌──(kali㉿kali)-[~]
└─$ cd Downloads/Foremost

┌──(kali㉿kali)-[~/Downloads/Foremost]
└─$ ls
L0_Documents.dd  L0_Documents.dd.bz2
```

```
FOREMOST(8)                System Manager's Manual                FOREMOST(8)

NAME
       foremost - Recover files using their headers, footers, and data structures

SYNOPSIS
       foremost [-h] [-V] [-d] [-vqwQT] [-b <blocksize>] [-o <dir>] [-t <type>] [-s
       <num>] [-i <file>]

BUILTIN FORMATS
       Recover files from a disk image based on file types specified  by  the  user
       using the -t switch.

       jpg    Support  for the JFIF and Exif formats including implementations used
              in modern digital cameras.

       gif

       png

       bmp    Support for windows bmp format.

       avi

       exe    Support for Windows PE binaries, will extract DLL and EXE files along
              with their compile times.

       mpg    Support for most MPEG files (must begin with 0×000001BA)

       wav

 Manual page foremost(8) line 1 (press h for help or q to quit)
```

```
┌──(kali㉿kali)-[~/Downloads/Foremost]
└─$ foremost -i L0_Documents.dd -o L0_Documents_Recovery
Processing: L0_Documents.dd
|foundat=_rels/.rels ◆◆(◆
foundat=xl/_rels/workbook.xml.rels ◆(◆
foundat=_rels/.rels ◆◆(◆
foundat=xl/_rels/workbook.xml.rels ◆(◆
foundat=_rels/.rels◆◆◆J1
                        ◆◆>E◆}'◆+◆◆v◆"◆◆Dmf◆8◆◆◆◆◆◆VPt`]◆◆◆i◆◆K◆vw◆◆z◆\\
                                                                    ▒◆M
                                                                       ◆◆◆oQ◆s◆◆◆U
◆◆◆9◆p◆◆◆j◆◆3I◆)◆KEUH(▒&◆t◆X◆ĞJ◆◆3◆◆I◆3◆◆ɾ◆⍝i◆◆-◆jo5伙◆_◆◆
x◆hs◆◆◆Ӣg!KBhb◆◆>◆◆◆◆◆◆◆◆e∂◆{◆◆W◆◆W◆}                        ◆G◆◆9ï◆◆`_R◆◆Y\F◆◆G
foundat=word/_rels/document.xml.rels◆◆MK1
W◆'^I[◆◆K◆◆ARu0◆◆;◆◆g◆T◆dN-◆D◆6◆&χ◆◆[0U)3◆W◆▒7]w◆◆7◆3◆◆ez0◆S灘 e◆◆□◆^8◆◆XU◆K\◆◆◆◆Z
                                                                                ◆◆◆8◆
◆mP◆◆.◆◆t◆◆◆◆◆◆k◆;◆◆PK
foundat=_rels/.rels◆◆◆J1
                        ◆◆>E◆}'◆+◆◆v◆"◆◆Dmf◆8◆◆◆◆◆◆VPt`]◆◆◆i◆◆K◆vw◆◆z◆\\
                                                                    ▒◆M
                                                                       ◆◆◆oQ◆s◆◆◆U
◆◆◆9◆p◆◆◆j◆◆3I◆)◆KEUH(▒&◆t◆X◆ĞJ◆◆3◆◆I◆3◆◆ɾ◆⍝i◆◆-◆jo5伙◆_◆◆
x◆hs◆◆◆Ӣg!KBhb◆◆>◆◆◆◆◆◆◆◆e∂◆{◆◆W◆◆W◆}                        ◆G◆◆9ï◆◆`_R◆◆Y\F◆◆G
foundat=word/_rels/document.xml.rels◆◆MK1
W◆'^I[◆◆K◆◆ARu0◆◆;◆◆g◆T◆dN-◆D◆6◆&χ◆◆[0U)3◆W◆▒7]w◆◆7◆3◆◆ez0◆S灘 e◆◆□◆^8◆◆XU◆K\◆◆◆◆Z
                                                                                ◆◆◆8◆
◆mP◆◆.◆◆t◆◆◆◆◆◆k◆;◆◆PK
foundat=_rels/.rels ◆(◆
*|
```

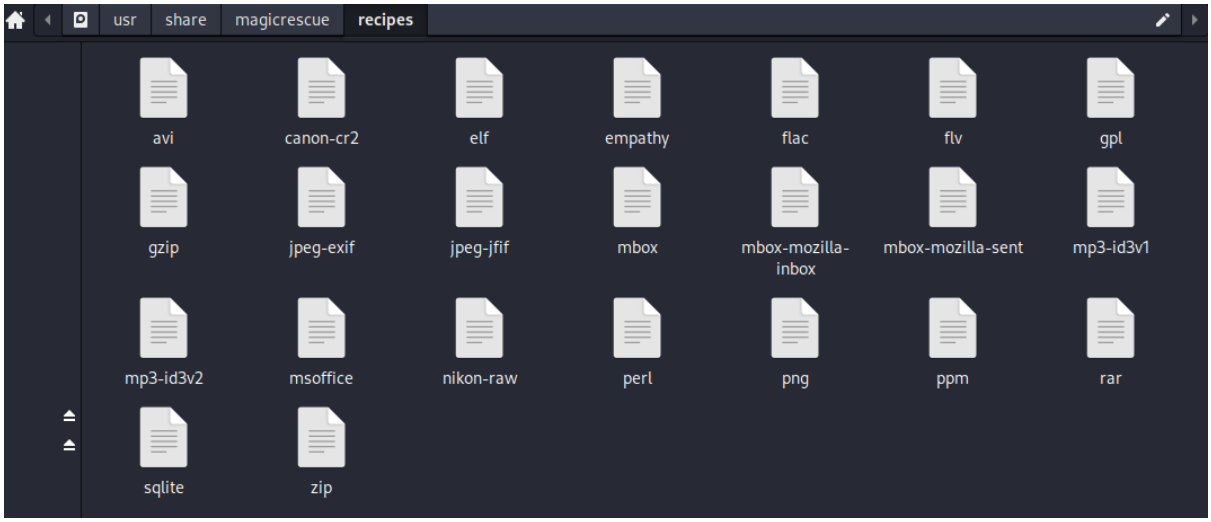


```
File: L0_Documents.dd
Start: Fri Oct 28 10:58:48 2022
Length: 40 MB (42490880 bytes)

Num        Name (bs=512)       Size      File Offset          Comment

0:         00081300.jpg        27 KB     41625792
1:         00041137.xlsx       22 KB     21062144
2:         00051183.xlsx       13 KB     26205696
3:         00061210.docx       4 KB      31339520
4:         00071219.docx       3 KB      36464128
5:         00081227.pptx       881 KB    41588224
6:         00081364.png        15 KB     41658610          (256 x 256)
7:         00010000.pdf        3 MB      5120000  (PDF is Linearized)
8:         00026204.pdf        2 MB      13416448          (PDF is Linearized)
Finish: Fri Oct 28 10:58:48 2022

9 FILES EXTRACTED

jpg:= 1
zip:= 5
png:= 1
pdf:= 2
------------------------------------------------

Foremost finished at Fri Oct 28 10:58:48 2022
```



```
┌──(kali㉿kali)-[~]
└─$ sudo fdisk -l
[sudo] password for kali:
Disk /dev/sda: 80.09 GiB, 86000000000 bytes, 167968750 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x1a92f870

Device     Boot Start       End   Sectors  Size Id Type
/dev/sda1  *     2048 167968749 167966702 80.1G 83 Linux


Disk /dev/sdc: 7.5 GiB, 8053063680 bytes, 15728640 sectors
Disk model: Flash Disk
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x7ace7177

Device     Boot Start      End  Sectors  Size Id Type
/dev/sdc1        2048 15728639 15726592  7.5G  c W95 FAT32 (LBA)
```

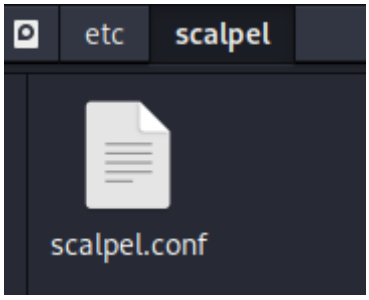
```
MAGICRESCUE(1)                    Magic Rescue                    MAGICRESCUE(1)

NAME
       magicrescue - Scans a block device and extracts known file types by looking
       at magic bytes.

SYNOPSIS
       magicrescue [ options ] devices

DESCRIPTION
       Magic Rescue opens devices for reading, scans them for file types it knows
       how to recover and calls an external program to extract them.  It looks at
       "magic bytes" in file contents, so it can be used both as an undelete
       utility and for recovering a corrupted drive or partition.  It works on any
       file system, but on very fragmented file systems it can only recover the
       first chunk of each file.  These chunks are sometimes as big as 50MB,
       however.

       To invoke magicrescue, you must specify at least one device and the -d and
       -r options.  See the "USAGE" section in this manual for getting started.

OPTIONS
       -b blocksize
              Default: 1.  This will direct magicrescue to only consider files that
              start at a multiple of the blocksize argument.  The option applies
              only to the recipes following it, so by specifying it multiple times
              it can be used to get different behavior for different recipes.

              Using this option you can usually get better performance, but fewer
              files will be found.  In particular, files with leading garbage (e.g.
              many mp3 files) and files contained inside other files are likely to
 Manual page magicrescue(1) line 1 (press h for help or q to quit)
```




```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ mkdir Rescue

┌──(kali㉿kali)-[~/Desktop]
└─$ cd Rescue

┌──(kali㉿kali)-[~/Desktop/Rescue]
└─$
```

```
┌──(kali㉿kali)-[~/Desktop/Rescue]
└─$ sudo magicrescue -r png -r jpeg-jfif -r jpeg-exif -d recovered -M io /dev/sdc > logs
Found jpeg-jfif at 0×1004000
Found png at 0×103BD54
Successfully extracted png file
Found png at 0×103DB67
Successfully extracted png file
Found png at 0×103FADF
Successfully extracted png file
Found png at 0×1042609
Successfully extracted png file
Found png at 0×1046370
Successfully extracted png file
Found png at 0×106C1E9
Successfully extracted png file
Found png at 0×1080354
Successfully extracted png file
Found png at 0×1087643
Successfully extracted png file
```


kali
Desktop
Rescue
recovered
000001DFFE8C-0.png
000001E1FDF6-0.png
000001FF09F5-0.png
000002ADC7A8-0.png
000002AFC712-0.png
000002C94FB1-0.png
000002C96CBA-0.png
000002E2F559-0.png
000002E30B8F-0.png
000002E32194-0.png
000003B5D5CA-0.png
000003B6F67D-0.png
000003B7AD55-0.png
000003B8F790-0.png
000003B61A4F-0.png
000003B63FA5-0.png
000003B510DC-0.png
000003B572F2-0.png
000003B5984A-0.png
000003B53004-0.png
000003BA41CB-0.png
000003BA88C5-0.png
000003BA6548-0.png
000003BAA2EF-0.png
000003BABD19-0.png
000003BADA96-0.png
000003BAF813-0.png
000003BB1D06-0.png
000003BB41F9-0.png
000003BB87A8-0.png


etc
scalpel
scalpel.conf

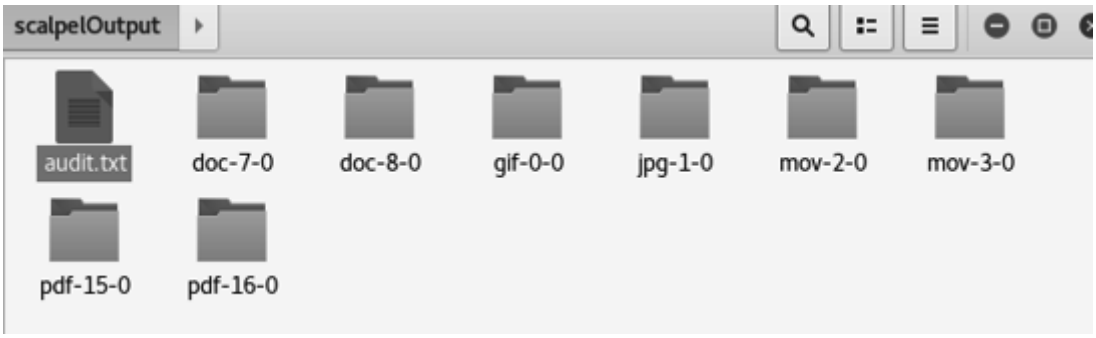
```
GIF and JPG files (very common)
#       gif     y       5000000         \x47\x49\x46\x38\x37\x61    \x00\x3b
#       gif     y       5000000         \x47\x49\x46\x38\x39\x61    \x00\x3b
#       jpg     y       5242880         \xff\xd8\xff???Exif         \xff\xd9   REVERSE
#       jpg     y       5242880         \xff\xd8\xff???JFIF         \xff\xd9   REVERSE
#
#
PNG
#       png     y       20000000        \x50\x4e\x47?       \xff\xfc\xfd\xfe
#
#
BMP     (used by MSWindows, use only if you have reason to think there are
#       BMP files worth digging for. This often kicks back a lot of false
#       positives
#
#       bmp     y       100000   BM??\x00\x00\x00
#
TIFF
#       tif     y       200000000       \x49\x49\x2a\x00
TIFF
#       tif     y       200000000       \x4D\x4D\x00\x2A
#
#-------------------------------------------
# ANIMATION FILES
#-------------------------------------------
#
AVI (Windows animation and DiVX/MPEG-4 movies)
#       avi     y       50000000 RIFF????AVI
#
```

```
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.
Carves files from a disk image based on file headers and footers.

Usage: scalpel [-b] [-c <config file>] [-d] [-h|V] [-i <file>]
               [-m blocksize] [-n] [-o <outputdir>] [-O num] [-q clustersize]
               [-r] [-s num] [-t <blockmap file>] [-u] [-v]
               <imgfile> [<imgfile>] ...

-b  Carve files even if defined footers aren't discovered within
    maximum carve size for file type [foremost 0.69 compat mode].
-c  Choose configuration file.
-d  Generate header/footer database; will bypass certain optimizations
    and discover all footers, so performance suffers.  Doesn't affect
    the set of files carved.  **EXPERIMENTAL**
-h  Print this help message and exit.
-i  Read names of disk images from specified file.
-m  Generate/update carve coverage blockmap file.  The first 32bit
    unsigned int in the file identifies the block size. Thereafter
    each 32bit unsigned int entry in the blockmap file corresponds
    to one block in the image file.  Each entry counts how many
    carved files contain this block. Requires more memory and
    disk.  **EXPERIMENTAL**
-n  Don't add extensions to extracted files.
-o  Set output directory for carved files.
-O  Don't organize carved files by type. Default is to organize carved files
    into subdirectories.
-p  Perform image file preview; audit log indicates which files
    would have been carved, but no files are actually carved.
-q  Carve only when header is cluster-aligned.
-r  Find only first of overlapping headers/footers [foremost 0.69 compat mode].
-s  Skip n bytes in each disk image before carving.
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ scalpel -o scalpelOutput/ 11-carve-fat.dd
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/home/kali/Downloads/11-carve-fat.dd"
```

```
Image file pass 1/2.
11-carve-fat.dd: 100.0% |******************************|   62.0 MB    00:00 ETAAllocating work queues...
Work queues allocation complete. Building carve lists...
Carve lists built.  Workload:
gif with header "\x47\x49\x46\x38\x39\x61" and footer "\x00\x3b" --> 1 files
jpg with header "\xff\xd8\xff\xe0\x00\x10" and footer "\xff\xd9" --> 5 files
mov with header "\x3f\x3f\x3f\x3f\x6d\x6f\x6f\x76" and footer "" --> 1 files
mov with header "\x3f\x3f\x3f\x3f\x6d\x64\x61\x74" and footer "" --> 2 files
mov with header "\x3f\x3f\x3f\x3f\x77\x69\x64\x65\x76" and footer "" --> 0 files
mpg with header "\x00\x00\x01\xba" and footer "\x00\x00\x01\xb9" --> 0 files
mpg with header "\x00\x00\x01\xb3" and footer "\x00\x00\x01\xb7" --> 0 files
doc with header "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00" and footer "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00" --> 3 files
doc with header "\xd0\xcf\x11\xe0\xa1\xb1" and footer "" --> 3 files
pst with header "\x21\x42\x4e\xa5\x6f\xb5\xa6" and footer "" --> 0 files
ost with header "\x21\x42\x44\x4e" and footer "" --> 0 files
dbx with header "\xcf\xad\x12\xfe\xc5\xfd\x74\x6f" and footer "" --> 0 files
idx with header "\x4a\x4d\x46\x39" and footer "" --> 0 files
mbx with header "\x4a\x4d\x46\x36" and footer "" --> 0 files
htm with header "\x3c\x68\x74\x6d\x6c" and footer "\x3c\x2f\x68\x74\x6d\x6c\x3e" --> 0 files
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0d" --> 1 files
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0a" --> 2 files
zip with header "\x50\x4b\x03\x04" and footer "\x3c\xac" --> 0 files
Carving files from image.
Image file pass 2/2.
11-carve-fat.dd: 100.0% |******************************|   62.0 MB    00:00 ETAProcessing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 18, elapsed = 2 seconds.
```

```
11-carve-fat.dd: 100.0% |******************************|   62.0 MB    00:00 ETA
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 18, elapsed = 2 seconds.
```

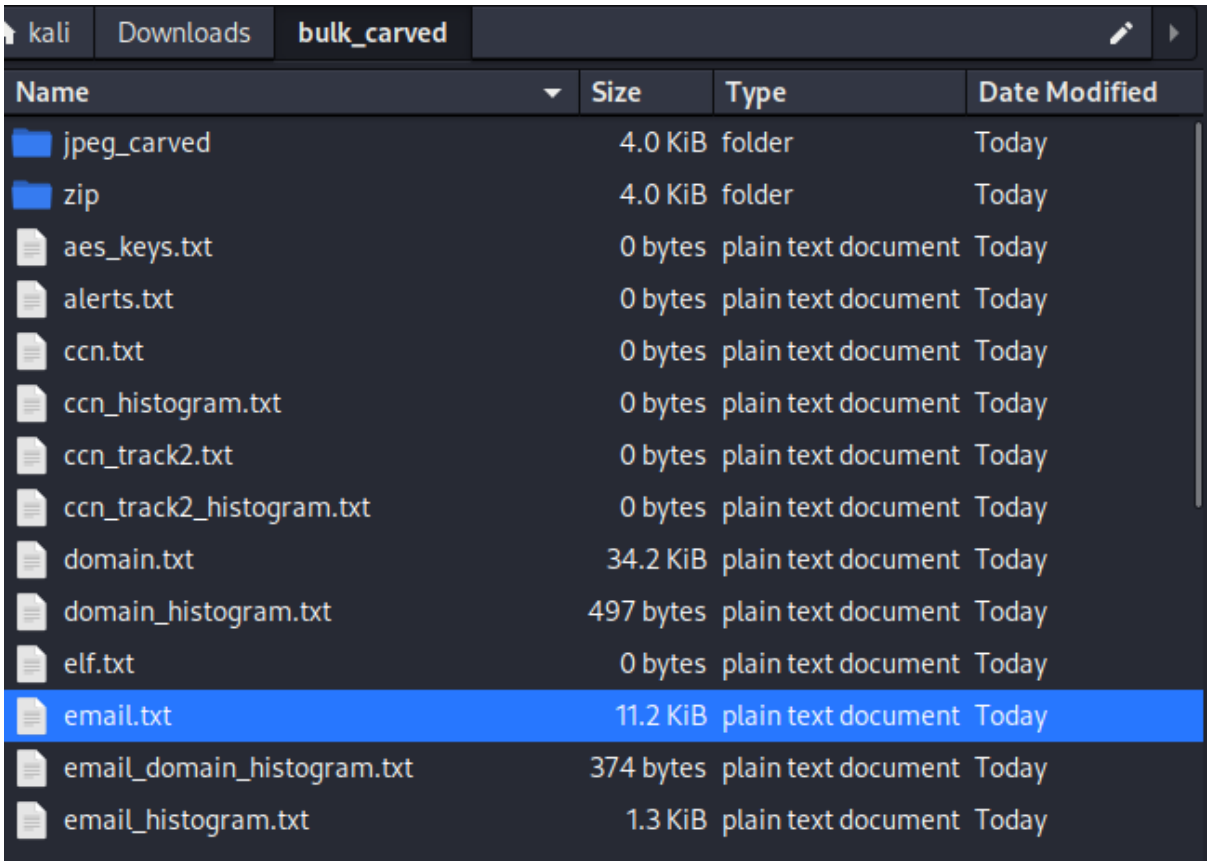


```
┌──(kali㉿kali)-[~/Downloads]
└─$ bulk_extractor -h
bulk_extractor version 2.0.0: A high-performance flexible digital forensics program.
Usage:
  bulk_extractor [OPTION ... ] image_name

  -A, --offset_add arg          Offset added (in bytes) to feature locations
                                (default: 0)
  -b, --banner_file arg         Path of file whose contents are prepended to top of
                                all feature files
  -C, --context_window arg      Size of context window reported in bytes (default:
                                16)
  -d, --debug arg               enable debugging (default: 1)
  -D, --debug_help              help on debugging
  -E, --enable_exclusive arg    disable all scanners except the one specified. Same
                                as -x all -E scanner.
  -e, --enable arg              enable a scanner (can be repeated)
  -x, --disable arg             disable a scanner (can be repeated)
  -f, --find arg                search for a pattern (can be repeated)
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ bulk_extractor -o bulk_carved nps-2010-emails.E01
opening nps-2010-emails.E01

bulk_extractor version: 2.0.0
Input file: "nps-2010-emails.E01"
Output directory: "bulk_carved"
Disk Size: 10485760
Scanners: aes base64 elf evtx exif facebook find gzip httplogs json kml_carved msxml n
et ntfsindx ntfslogfile ntfsmft ntfsusn pdf rar sqlite utmp vcard_carved windirs winln
k winpe winprefetch zip accts email gps
Threads: 2
going multi-threaded ... ( 2 )
bulk_extractor      Fri Oct 28 14:22:21 2022

available_memory: 6097850368
bytes_queued: 0
depth0_bytes_queued: 0
depth0_sbufs_queued: 0
elapsed_time:  0:00:00
estimated_date_completion: 2022-10-28 14:22:20
estimated_time_remaining: n/a
fraction_read: 0.000000 %
max_offset: 0
```

```
Phase 2. Shutting down scanners
Computing final histograms and shutting down ...
Phase 3. Generating stats and printing final usage information
All Threads Finished!
Elapsed time: 2.006 sec.
Total MB processed: 10
Overall performance: 5.228 MBytes/sec 2.614 (MBytes/sec/thread)
sbufs created:   62785
sbufs unaccounted: 0
Time producer spent waiting for scanners to process data:         0:00:00 (0.00 second
s)
Time consumer scanners spent waiting for data from producer:      0:00:00 (0.04 second
s)
Average time each consumer spent waiting for data from producer:  0:00:00 (0.00 second
s)
*** More time spent waiting for reader. You need faster I/O for improved performance.
Total email features found: 67
```

```
┌──(kali㉿kali)-[~/Downloads/bulk_carved]
└─$ ls -l
total 280
-rw-r--r-- 1 kali kali      0 Oct 28 14:22 aes_keys.txt
-rw-r--r-- 1 kali kali      0 Oct 28 14:22 alerts.txt
-rw-r--r-- 1 kali kali      0 Oct 28 14:22 ccn_histogram.txt
-rw-r--r-- 1 kali kali      0 Oct 28 14:22 ccn_track2_histogram.txt
-rw-r--r-- 1 kali kali      0 Oct 28 14:22 ccn_track2.txt
-rw-r--r-- 1 kali kali      0 Oct 28 14:22 ccn.txt
-rw-r--r-- 1 kali kali    497 Oct 28 14:22 domain_histogram.txt
-rw-r--r-- 1 kali kali  35044 Oct 28 14:22 domain.txt
-rw-r--r-- 1 kali kali      0 Oct 28 14:22 elf.txt
-rw-r--r-- 1 kali kali    374 Oct 28 14:22 email_domain_histogram.txt
-rw-r--r-- 1 kali kali   1320 Oct 28 14:22 email_histogram.txt
-rw-r--r-- 1 kali kali  11462 Oct 28 14:22 email.txt
-rw-r--r-- 1 kali kali      0 Oct 28 14:22 ether_histogram_1.txt
-rw-r--r-- 1 kali kali      0 Oct 28 14:22 ether_histogram.txt
-rw-r--r-- 1 kali kali      0 Oct 28 14:22 ether.txt
-rw-r--r-- 1 kali kali      0 Oct 28 14:22 evtx_carved.txt
-rw-r--r-- 1 kali kali   3998 Oct 28 14:22 exif.txt
-rw-r--r-- 1 kali kali      0 Oct 28 14:22 facebook.txt
-rw-r--r-- 1 kali kali      0 Oct 28 14:22 find_histogram.txt
-rw-r--r-- 1 kali kali      0 Oct 28 14:22 find.txt
-rw-r--r-- 1 kali kali      0 Oct 28 14:22 gps.txt
```



email.txt - Notepad

File Edit Search Help

```
\000\000\000\000\000\037\000\000\000\001\000\000\000\000\000\000\000
848896-GZIP-0       email_in_gzip@gzipfile.com  email_in_gzip@gzipfile.com\012
70727-PDF-0         plain_text_pdf@textedit.com  plain_text_pdf@textedit.com
81991-PDF-0         rtf_text_pdf@textedit.com      rtf_text_pdf@textedit.com
92231-PDF-0         plain_utf16_pdf@textedit.com            plain_utf16_pdf@textedit.com
130119-PDF-20       user_doc_pdf@microsoftword.com       is a test —
user_doc_pdf@microsoftword.com   Really.
181319-PDF-20       user_docx_pdf@microsoftword.com      is a test —
user_docx_pdf@microsoftword.com   Really.
155371-ZIP-402      user_docx@microsoftword.com
Target="mailto:user_docx@microsoftword.com" TargetMode="Ex
155996-ZIP-1012     user_docx@microsoftword.com          "/><!
w:rPr><w:t>user_docx@microsoftword.com</w:t></w:r></w:
227991-ZIP-161      xlsx_cell@microsoft_excel.com
ount="1"><si><t>xlsx_cell@microsoft_excel.com</t></si></sst>
228216-ZIP-265      xlsx_cell@microsoft_excel.com
Target="mailto:xlsx_cell@microsoft_excel.com" TargetMode="Ex
232443-ZIP-433      xlsx_comment@microsoft_excel.com   ce="preserve">
\015\012xlsx_comment@microsoft_excel.com\015\012</t></r></text
665889-ZIP-1380     docx_within_docx@document.com       \000\000\000\000\236\007\000\000>
\001\000\000\210\000\000\000d\000o\000c\000x\000_\000w\000i\000t\000h\000i\000n\000_\000d\000o
\000c\000x\000@\000d\000o\000c\000u\000m\000e\000n\000t\000.\000c\000o\000m
\000\377\274\030\000\000\000\030\000\000\000\023\000\000\000\024\000
740698-ZIP-265      ppt_within_doc@document.com
Target="mailto:ppt_within_doc@document.com" TargetMode="Ex
754980-ZIP-4640     pptx_within_docx@document.com
\000\000\000\000\377\377\377\377\377\377\377\377\210\000\000\000p\000p\000t\000x\000_\000w\000i
\000t\000h\000i\000n\000_\000d\000o\000c\000x\000@\000d\000o\000c\000u\000m\000e\000n\000t
```

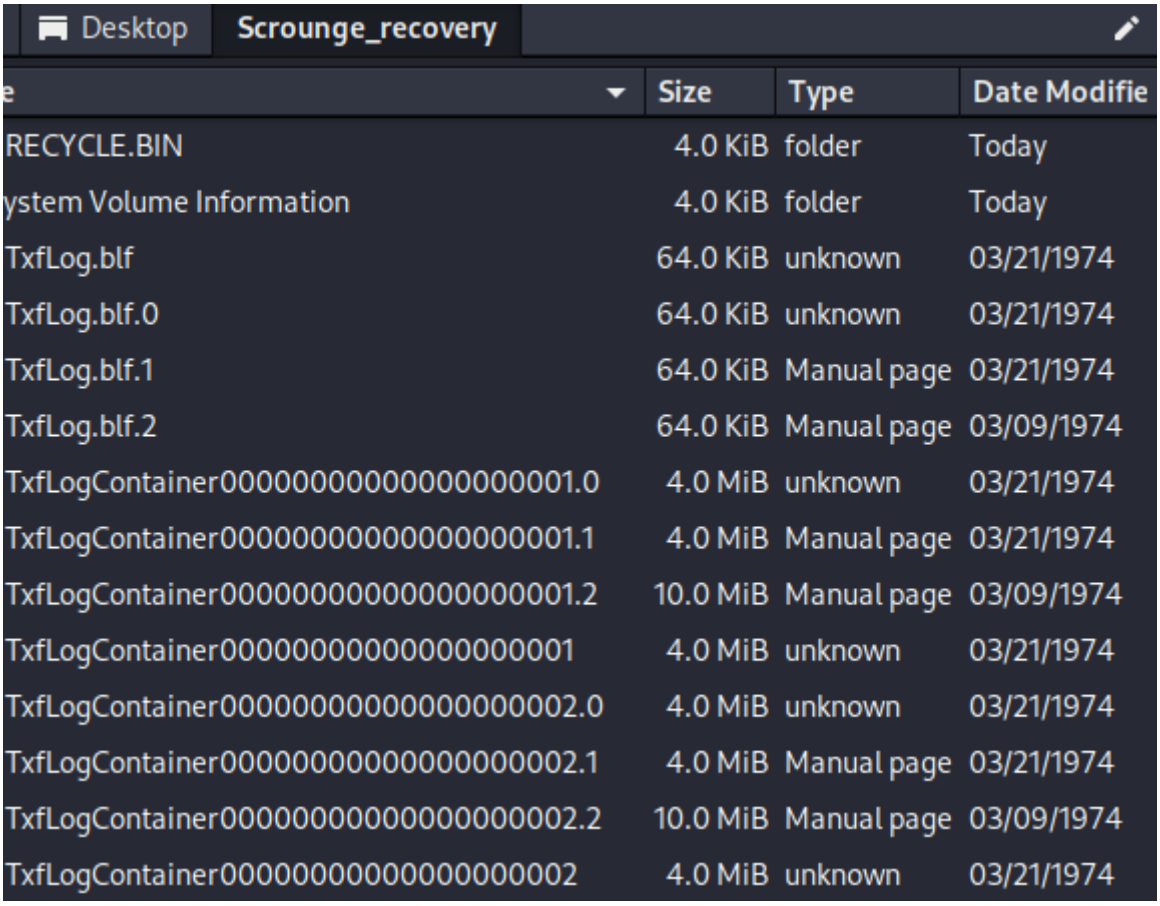
```
Disk /dev/sdb: 465.76 GiB, 500107862016 bytes, 976773168 sectors
Disk model: 2115
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disklabel type: dos
Disk identifier: 0x01ea53d4

Device     Boot Start       End   Sectors   Size Id Type
/dev/sdb1        16065 976768064 976752000 465.8G  f W95 Ext'd (LBA)
/dev/sdb5        16128 976768064 976751937 465.8G  7 HPFS/NTFS/exFAT
```

```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ mkdir Scrounge_recovery

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
'AccessData FTK Imager.desktop'  'Brute Shark.lnk'    testpdf.pdf
'AccessData FTK Imager.lnk'       Recuva.desktop      xfce4-screenshooter.desktop
'Autopsy 4.19.3.desktop'          Rescue
'Autopsy 4.19.3.lnk'              Scrounge_recovery
```

```
┌──(kali㉿kali)-[~/Desktop/Scrounge_recovery]
└─$ scrounge-ntfs -h
usage: scrounge-ntfs -l disk
  List all drive partition information.

usage: scrounge-ntfs -s disk
  Search drive for NTFS partitions.

usage: scrounge-ntfs [-m mftoffset] [-c clustersize] [-o outdir] disk start end
  Scrounge data from a partition
  -m          Offset to mft (in sectors)
  -c          Cluster size (in sectors, default of 8)
  -o          Directory to put scrounged files in
  disk        The raw disk partitios (ie: /dev/hda)
  start       First sector of partition
  end         Last sector of partition
```

```
┌──(kali㉿kali)-[~/Desktop/Scrounge_recovery]
└─$ sudo scrounge-ntfs -l /dev/sdb
    Start Sector    End Sector      Cluster Size    MFT Offset
═══════════════════════════════════════════════════════════════

Drive: /dev/sdb
    16128           976768002       8               24
```

```
┌──(kali㉿kali)-[~/Desktop/Scrounge_recovery]
└─$ sudo scrounge-ntfs -m 24 -c 8 /dev/sdb 16128 976768002
[Scrounging via MFT ... ]
[Processing MFT ... ]
\$TxfLog.blf
\$TxfLogContainer00000000000000000001
\$TxfLogContainer00000000000000000002
\$RECYCLE.BIN
\$RECYCLE.BIN\S-1-5-21-1054828521-904020205-1243921375-24603
\$RECYCLE.BIN\S-1-5-21-1054828521-904020205-1243921375-24603\desktop.ini
\System Volume Information
\System Volume Information\WPSettings.dat
\System Volume Information\IndexerVolumeGuid
\$RECYCLE.BIN\S-1-5-21-2653766897-1606394338-1728658101-500\$R10G6QE\ISOs
\$RECYCLE.BIN\S-1-5-21-2653766897-1606394338-1728658101-500\$R10G6QE
\.Trash-1000\files\Microsoft SQL Server 2016 13.0.4001.0 (Service Pack 1)
```


Desktop
Scrounge_recovery
Size
Type
Date Modifie
RECYCLE.BIN 4.0 KiB folder Today
ystem Volume Information 4.0 KiB folder Today
TxfLog.blf 64.0 KiB unknown 03/21/1974
TxfLog.blf.0 64.0 KiB unknown 03/21/1974
TxfLog.blf.1 64.0 KiB Manual page 03/21/1974
TxfLog.blf.2 64.0 KiB Manual page 03/09/1974
TxfLogContainer00000000000000000001.0 4.0 MiB unknown 03/21/1974
TxfLogContainer00000000000000000001.1 4.0 MiB Manual page 03/21/1974
TxfLogContainer00000000000000000001.2 10.0 MiB Manual page 03/09/1974
TxfLogContainer00000000000000000001 4.0 MiB unknown 03/21/1974
TxfLogContainer00000000000000000002.0 4.0 MiB unknown 03/21/1974
TxfLogContainer00000000000000000002.1 4.0 MiB Manual page 03/21/1974
TxfLogContainer00000000000000000002.2 10.0 MiB Manual page 03/09/1974
TxfLogContainer00000000000000000002 4.0 MiB unknown 03/21/1974


(cfsi㉿Research)-[~]
$ cd Desktop
(cfsi㉿Research)-[~/Desktop]
$ mkdir Recoverjpeg

```
┌──(cfsi㉿Research)-[~/Desktop]
└─$ sudo apt-get install recoverjpeg
[sudo] password for cfsi:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  exif fonts-urw-base35 ghostscript graphicsmagick graphicsmagick-ima
  libgraphicsmagick-q16-3 libwmflite-0.2-7
Suggested packages:
  fonts-texgyre ghostscript-x graphicsmagick-dbg
The following NEW packages will be installed:
  exif ghostscript graphicsmagick graphicsmagick-imagemagick-compat g
  libwmflite-0.2-7 recoverjpeg
The following packages will be upgraded:
  fonts-urw-base35
1 upgraded, 8 newly installed, 0 to remove and 1090 not upgraded.
Need to get 8,913 kB of archives.
After this operation, 9,965 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

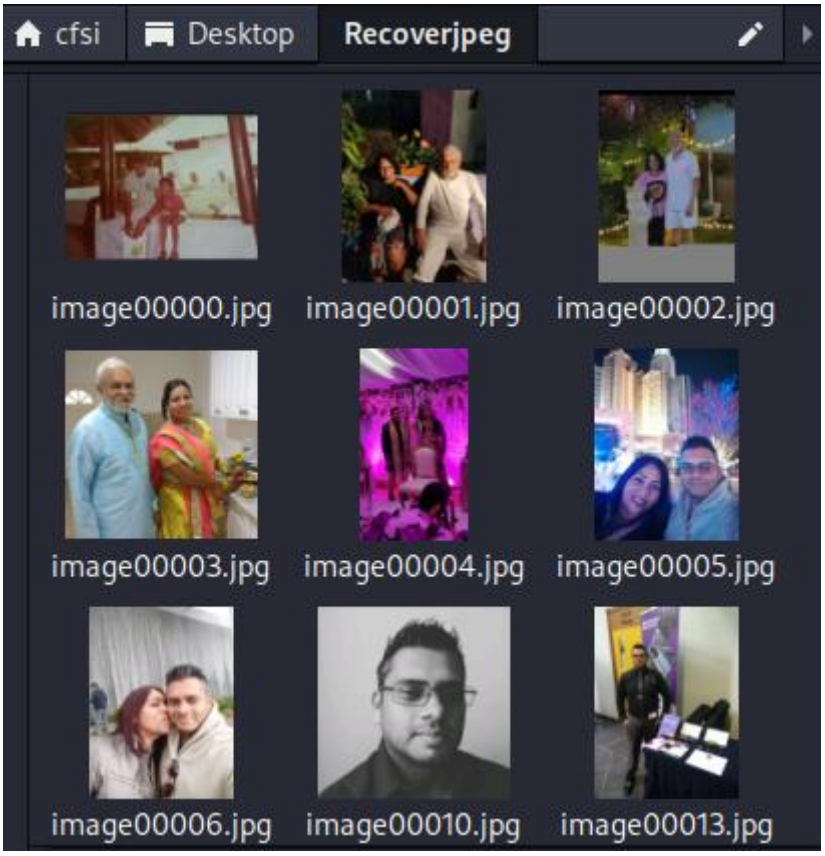
```
┌──(cfsi㉿Research)-[~/Desktop]
└─$ sudo fdisk -l
Disk /dev/sda: 372.61 GiB, 400088457216 bytes, 781422768 sectors
Disk model: ST3400832NS
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0×ab60b093

Device     Boot     Start       End   Sectors   Size Id Type
/dev/sda1  *         2048 779421695 779419648 371.7G 83 Linux
/dev/sda2       779423742 781422591   1998850   976M  5 Extended
/dev/sda5       779423744 781422591   1998848   976M 82 Linux swap / Solaris


Disk /dev/sdb: 29.32 GiB, 31482445824 bytes, 61489152 sectors
Disk model: Cruzer Blade
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0×1ace7ba7

Device     Boot    Start      End  Sectors  Size Id Type
/dev/sdb1  *        2048 57294814 57292767 27.3G  c W95 FAT32 (LBA)
/dev/sdb2       57294815 61489102  4194288    2G 83 Linux
```

```
┌──(cfsi㉿Research)-[~/Desktop]
└─$ cd Recoverjpeg
```

```
┌──(cfsi㉿Research)-[~/Desktop]
└─$ recoverjpeg
Usage: recoverjpeg [options] file|device
Options:
   -b blocksize   Block size in bytes (default: 512)
   -d format      Directory format string in printf syntax
   -f format      File format string in printf syntax
   -h             This help message
   -i index       Initial picture index
   -m maxsize     Max jpeg file size in bytes (default: 6m)
   -o directory   Restore jpeg files into this directory
   -q             Be quiet
   -r readsize    Size of disk reads in bytes (default: 128m)
   -s cutoff      Minimal file size in bytes to restore
   -S skipsize    Size to skip at the beginning
   -v             Be verbose
   -V             Display version and exit
```

```
┌──(cfsi㉿Research)-[~/Desktop/Recoverjpeg]
└─$ sudo recoverjpeg /dev/sdb
```

```
└─$ sudo recoverjpeg /dev/sdb
Restored 2021 pictures
```



Chapter 10: Memory Forensics and Analysis with Volatility 3

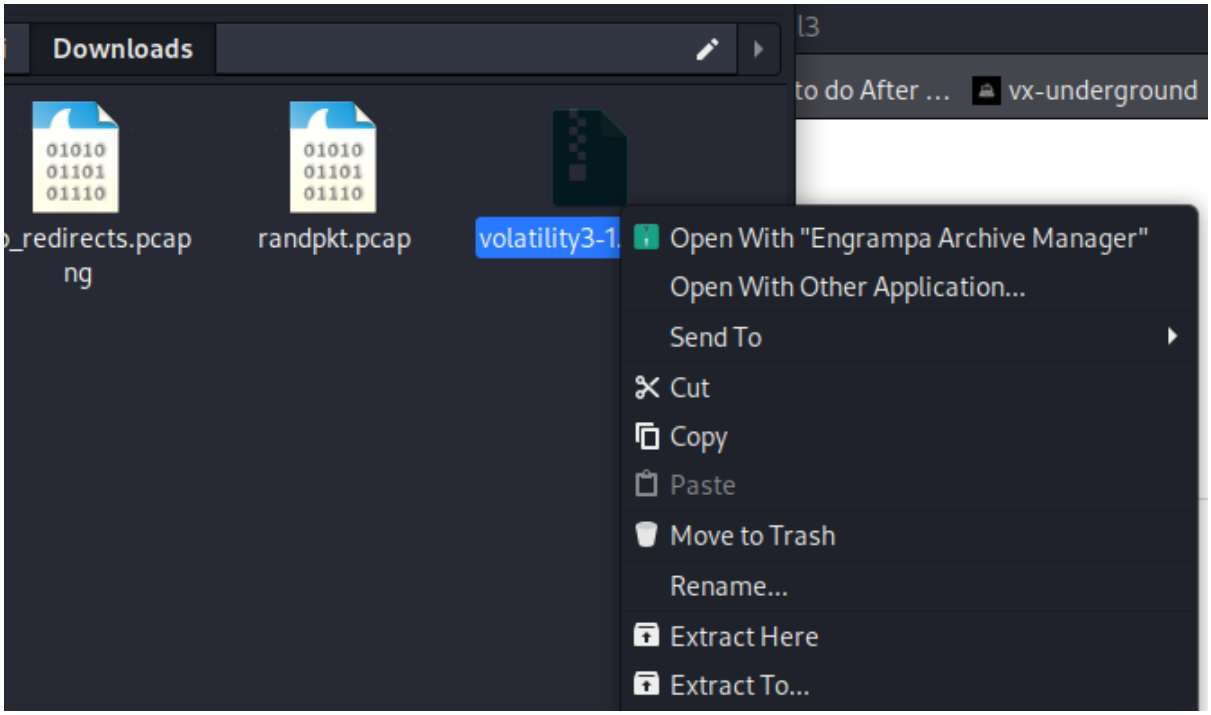
Volatility 2 | Volatility 3

Volatility 3 v1.0.0 (Python 3 Rewrite)

In 2020, the Volatility Foundation publicly released a complete rewrite of the framework, Volatility 3. The project was intended to address many of the technical and performance challenges associated with the original code base that became apparent since its original release in 2007. Another benefit of the rewrite is that Volatility 3 could be released under a custom license that was more aligned with the goals of the Volatility community, the Volatility Software License (VSL). Details about the rewrite of Volatility 3 can be found in this presentation: Volatility 3 Public Beta: Insider's Preview.

Released: February 2020

- Download the Volatility 3 v1.0.0 Source Code (.zip)
- Download the Volatility 3 v1.0.0 Source Code (tar.gz)
- View Volatility 3 documentation on Read the Docs
- GitHub release page for Volatility 3 v1.0.0



```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get update
Get:1 http://kali.download/kali kali-rolling InRelease [30.6 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [18.7 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [43.0 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [111 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [161 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [235 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [897 kB
]
Fetched 63.2 MB in 27s (2,341 kB/s)
Reading package lists... Done
```

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install python3
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libpython3.9-dev libtbb2 python3-llvmlite python3.9-dev
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  blueman gcc-12-base gobject-introspection libc-bin libc-dev-bin libc-l10n
  libc6 libc6-dev libc6-i386 libgirepository-1.0-1 libglib2.0-0 libglib2.0-bin
  libgmp-dev libgmp10 libgmpxx4ldbl libgnutls30 libicu71 libjansson4
  libldap-2.5-0 libldb2 libpython3-dev libpython3-stdlib libpython3.10
  libpython3.10-dev libpython3.10-minimal libpython3.10-stdlib libsasl2-2
  libsasl2-modules-db libsmbclient libstdc++6 libtalloc2 libtdb1 libwbclient0
  locales python3-dev python3-distutils python3-donut python3-jq python3-ldb
  python3-lib2to3 python3-minimal python3-nassl python3-samba python3-talloc
  python3-tdb python3.10 python3.10-dev python3.10-minimal samba samba-common
  samba-common-bin samba-dsdb-modules samba-libs samba-vfs-modules smbclient
```

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install python3-pip python-setuptools build-essential
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
build-essential is already the newest version (12.9).
python-setuptools is already the newest version (44.1.1-1.2).
The following packages were automatically installed and are no longer required:
  libpython3.9-dev libtbb2 python3-llvmlite python3.9-dev
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  python3-wheel
The following packages will be REMOVED:
  python-pip
The following NEW packages will be installed:
  python3-pip python3-wheel
0 upgraded, 2 newly installed, 1 to remove and 1600 not upgraded.
Need to get 1,353 kB of archives.
After this operation, 2,052 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

```
┌──(kali㉿kali)-[~]
└─$ cd Downloads/volatility3
```

```
┌──(kali㉿kali)-[~/Downloads/volatility3]
└─$ ls
development  LICENSE.txt  mypy.ini   setup.py     vol.py       volshell.spec
doc          MANIFEST.in  README.md  volatility3  volshell.py  vol.spec
```

```
┌──(kali㉿kali)-[~/Downloads/volatility3]
└─$ sudo python3 setup.py install
running install
/usr/lib/python3/dist-packages/setuptools/command/install.py:34: SetuptoolsDeprecationWarning: setup.py install is deprecated. Use build and pip and other standards-based tools.
  warnings.warn(
/usr/lib/python3/dist-packages/setuptools/command/easy_install.py:158: EasyInstallDeprecationWarning: easy_install command is deprecated. Use build and pip and other standards-based tools.
  warnings.warn(
/usr/lib/python3/dist-packages/pkg_resources/__init__.py:116: PkgResourcesDeprecationWarning: 1.16.0-unknown is an invalid version and will not be supported in a future release
  warnings.warn(
/usr/lib/python3/dist-packages/pkg_resources/__init__.py:116: PkgResourcesDeprecationWarning: 1.12.1-git20200711.33e2d80-dfsg1-0.6 is an invalid version and will not be supported in a future release
  warnings.warn(
running bdist_egg
```

```
┌──(kali㉿kali)-[~/Downloads/volatility3]
└─$ python3 vol.py
Volatility 3 Framework 1.0.0
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]]
                  [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG]
                  [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config]
                  [--clear-cache] [--single-location SINGLE_LOCATION]
                  [--stackers [STACKERS ...]]
                  [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
                  plugin ...
volatility: error: Please select a plugin to run
```

```
┌──(kali㉿kali)-[~/Downloads/volatility3]
└─$ python3 vol.py -h
Volatility 3 Framework 1.0.0
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND]
                  [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR] [-q]
                  [-r RENDERER] [-f FILE] [--write-config] [--clear-cache]
                  [--single-location SINGLE_LOCATION] [--stackers [STACKERS ...]]
                  [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
                  plugin ...

An open-source memory forensics framework

options:
  -h, --help            Show this help message and exit, for specific plugin options use
                        'volatility <pluginname> --help'
  -c CONFIG, --config CONFIG
                        Load the configuration from a json file
  --parallelism [{processes,threads,off}]
                        Enables parallelism (defaults to off if no argument given)
  -e EXTEND, --extend EXTEND
                        Extend the configuration with a new (or changed) setting
  -p PLUGIN_DIRS, --plugin-dirs PLUGIN_DIRS
                        Semi-colon separated list of paths to find plugins
```

```
  mac.psaux.Psaux     Recovers program command line arguments.
  mac.pslist.PsList   Lists the processes present in a particular mac memory image.
  mac.pstree.PsTree   Plugin for listing processes in a tree based on their parent
                      process ID.
  mac.socket_filters.Socket_filters
                      Enumerates kernel socket filters.
  mac.timers.Timers   Check for malicious kernel timers.
  mac.trustedbsd.Trustedbsd
                      Checks for malicious trustedbsd modules
  mac.vfsevents.VFSevents
                      Lists processes that are filtering file system events
  timeliner.Timeliner
                      Runs all relevant plugins that provide time related information
                      and orders the results by time.
  windows.bigpools.BigPools
                      List big page pools.
  windows.callbacks.Callbacks
                      Lists kernel callbacks and notification routines.
  windows.cmdline.CmdLine
                      Lists process command line arguments.
```

```
┌──(kali㉿kali)-[~/Downloads/volatility3]
└─$ ls
build                MANIFEST.in          volshell.py
cridex_memdump.zip   mypy.ini             volshell.spec
cridex.vmem          README.md            vol.spec
development          setup.py             'wannacry pw- infected'
dist                 volatility3          'wannacry pw- infected.7z'
doc                  volatility3.egg-info wcry.raw
LICENSE.txt          vol.py
```

```
┌──(kali㉿kali)-[~/Downloads/volatility3]
└─$ python3 vol.py -f cridex.vmem windows.info
Volatility 3 Framework 1.0.0
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0×804d7000
DTB     0×2fe000
Symbols file:///home/kali/Downloads/volatility3/volatility3/
B31AE7E4ACAABA750AA241FF331-1.json.xz
Is64Bit False
IsPAE   True
primary 0 WindowsIntelPAE
memory_layer    1 FileLayer
KdDebuggerDataBlock     0×80545ae0
NTBuildLab      2600.xpsp.080413-2111
CSDVersion      3
KdVersionBlock  0×80545ab8
Major/Minor     15.2600
MachineType     332
KeNumberProcessors      1
SystemTime      2012-07-22 02:45:08
NtSystemRoot    C:\WINDOWS
NtProductType   NtProductWinNt
NtMajorVersion  5
NtMinorVersion  1
PE MajorOperatingSystemVersion  5
PE MinorOperatingSystemVersion  1
PE Machine      332
```

```
NTBuildLab              2600.xpsp_sp3_qfe.130704-0421
CSDVersion              3
KdVersionBlock          0x8054cf38
Major/Minor             15.2600
MachineType             332
KeNumberProcessors      1
SystemTime              2017-05-12 21:26:32
NtSystemRoot            C:\WINDOWS
NtProductType           NtProductWinNt
NtMajorVersion          5
NtMinorVersion          1
PE MajorOperatingSystemVersion  5
PE MinorOperatingSystemVersion  1
PE Machine              332
PE TimeDateStamp        Thu Jul  4 02:58:58 2013
```

```
┌──(kali㉿kali)-[~/Downloads/volatility3]
└─$ python3 vol.py -f cridex.vmem windows.pslist
Volatility 3 Framework 1.0.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0x823c89c8      53      240     N/A     False   N/A     N/A     Disabled
368     4       smss.exe        0x822f1020      3       19      N/A     False   2012-07-22 02:42:31.000000      N/A     Disabled
584     368     csrss.exe       0x822a0598      9       326     0       False   2012-07-22 02:42:32.000000      N/A     Disabled
608     368     winlogon.exe    0x82298700      23      519     0       False   2012-07-22 02:42:32.000000      N/A     Disabled
652     608     services.exe    0x81e2ab28      16      243     0       False   2012-07-22 02:42:32.000000      N/A     Disabled
664     608     lsass.exe       0x81e2a3b8      24      330     0       False   2012-07-22 02:42:32.000000      N/A     Disabled
824     652     svchost.exe     0x82311360      20      194     0       False   2012-07-22 02:42:33.000000      N/A     Disabled
908     652     svchost.exe     0x81e29ab8      9       226     0       False   2012-07-22 02:42:33.000000      N/A     Disabled
1004    652     svchost.exe     0x823001d0      64      1118    0       False   2012-07-22 02:42:33.000000      N/A     Disabled
1056    652     svchost.exe     0x821dfda0      5       60      0       False   2012-07-22 02:42:33.000000      N/A     Disabled
1220    652     svchost.exe     0x82295650      15      197     0       False   2012-07-22 02:42:35.000000      N/A     Disabled
1484    1464    explorer.exe    0x821dea70      17      415     0       False   2012-07-22 02:42:36.000000      N/A     Disabled
1512    652     spoolsv.exe     0x81eb17b8      14      113     0       False   2012-07-22 02:42:36.000000      N/A     Disabled
1640    1484    reader_sl.exe   0x81e7bda0      5       39      0       False   2012-07-22 02:42:36.000000      N/A     Disabled
788     652     alg.exe 0x820e8da0      7       104     0       False   2012-07-22 02:43:01.000000      N/A     Disabled
1136    1004    wuauclt.exe     0x821fcda0      8       173     0       False   2012-07-22 02:43:46.000000      N/A     Disabled
1588    1004    wuauclt.exe     0x8205bda0      5       132     0       False   2012-07-22 02:44:01.000000      N/A     Disabled

┌──(kali㉿kali)-[~/Downloads/volatility3]
└─$
```

```
└─$ python3 vol.py -f cridex.vmem windows.pstree
Volatility 3 Framework 1.0.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime

4       0       System  0x8205bda0      53      240     N/A     False   N/A     N/A
* 368   4       smss.exe        0x8205bda0      3       19      N/A     False   2012-07-22 02:42:31.000000      N/A
** 584  368     csrss.exe       0x8205bda0      9       326     0       False   2012-07-22 02:42:32.000000      N/A
** 608  368     winlogon.exe    0x8205bda0      23      519     0       False   2012-07-22 02:42:32.000000      N/A
*** 664 608     lsass.exe       0x8205bda0      24      330     0       False   2012-07-22 02:42:32.000000      N/A
*** 652 608     services.exe    0x8205bda0      16      243     0       False   2012-07-22 02:42:32.000000      N/A
**** 1056       652     svchost.exe     0x8205bda0      5       60      0       False   2012-07-22 02:42:33.000000      N/A
**** 1220       652     svchost.exe     0x8205bda0      15      197     0       False   2012-07-22 02:42:35.000000      N/A
**** 1512       652     spoolsv.exe     0x8205bda0      14      113     0       False   2012-07-22 02:42:36.000000      N/A
**** 908        652     svchost.exe     0x8205bda0      9       226     0       False   2012-07-22 02:42:33.000000      N/A
**** 1004       652     svchost.exe     0x8205bda0      64      1118    0       False   2012-07-22 02:42:33.000000      N/A
***** 1136      1004    wuauclt.exe     0x8205bda0      8       173     0       False   2012-07-22 02:43:46.000000      N/A
***** 1588      1004    wuauclt.exe     0x8205bda0      5       132     0       False   2012-07-22 02:44:01.000000      N/A
**** 788        652     alg.exe 0x8205bda0      7       104     0       False   2012-07-22 02:43:01.000000      N/A
**** 824        652     svchost.exe     0x8205bda0      20      194     0       False   2012-07-22 02:42:33.000000      N/A
1484    1464    explorer.exe    0x8205bda0      17      415     0       False   2012-07-22 02:42:36.000000      N/A
* 1640  1484    reader_sl.exe   0x8205bda0      5       39      0       False   2012-07-22 02:42:36.000000      N/A
```

```
└─$ python3 vol.py -f cridex.vmem windows.psscan
Volatility 3 Framework 1.0.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset  Threads Handles SessionId       Wow64   CreateTime      ExitTime

908     652     svchost.exe     0x2029ab8       9       226     0       False   2012-07-22 02:42:33.000000
664     608     lsass.exe       0x202a3b8       24      330     0       False   2012-07-22 02:42:32.000000
652     608     services.exe    0x202ab28       16      243     0       False   2012-07-22 02:42:32.000000
1640    1484    reader_sl.exe   0x207bda0       5       39      0       False   2012-07-22 02:42:36.000000
1512    652     spoolsv.exe     0x20b17b8       14      113     0       False   2012-07-22 02:42:36.000000
1588    1004    wuauclt.exe     0x225bda0       5       132     0       False   2012-07-22 02:44:01.000000
788     652     alg.exe 0x22e8da0       7       104     0       False   2012-07-22 02:43:01.000000      N/A
1484    1464    explorer.exe    0x23dea70       17      415     0       False   2012-07-22 02:42:36.000000
1056    652     svchost.exe     0x23dfda0       5       60      0       False   2012-07-22 02:42:33.000000
1136    1004    wuauclt.exe     0x23fcda0       8       173     0       False   2012-07-22 02:43:46.000000
1220    652     svchost.exe     0x2495650       15      197     0       False   2012-07-22 02:42:35.000000
608     368     winlogon.exe    0x2498700       23      519     0       False   2012-07-22 02:42:32.000000
584     368     csrss.exe       0x24a0598       9       326     0       False   2012-07-22 02:42:32.000000
368     4       smss.exe        0x24f1020       3       19      N/A     False   2012-07-22 02:42:31.000000
1004    652     svchost.exe     0x25001d0       64      1118    0       False   2012-07-22 02:42:33.000000
824     652     svchost.exe     0x2511360       20      194     0       False   2012-07-22 02:42:33.000000
4       0       System  0x25c89c8       53      240     N/A     False   N/A     N/A     Disabled
```

```
└─$ python3 vol.py -f cridex.vmem windows.modscan
Volatility 3 Framework 1.0.0
Progress:  100.00               PDB scanning finished
Offset  Base    Size    Name    Path    File output

0x59ca40        0x89607b8d      0x89662c46                      Disabled
0x5a3890        0x6600000c      0x8d50a045                      Disabled
0x5a3e06        0x400   0x66000010                      Disabled
0x20296b8       0xf7c6f000      0x4000  ndisuio.sys     \SystemRoot\system32\DRIVERS\ndisuio.sys
d
0x202fe80       0xf8b46000      0x3000  ndistapi.sys    \SystemRoot\system32\DRIVERS\ndistapi.sys
d
0x20350c8       0xf89b2000      0x7000  HIDPARSE.SYS    \SystemRoot\system32\DRIVERS\HIDPARSE.SYS
d
0x2078108       0xf8982000      0x5000  flpydisk.sys    \SystemRoot\system32\DRIVERS\flpydisk.sys
d
0x2085008       0xbff50000      0x3000  framebuf.dll    \SystemRoot\System32\framebuf.dll       Di
0x20858d8       0xf877a000      0xf000  redbook.sys     \SystemRoot\system32\DRIVERS\redbook.sys
```

```
└─$ python3 vol.py -f cridex.vmem windows.getsids
Volatility 3 Framework 1.0.0
Progress:  100.00               PDB scanning finished
PID     Process SID     Name

4       System  S-1-5-18        Local System
4       System  S-1-5-32-544    Administrators
4       System  S-1-1-0 Everyone
4       System  S-1-5-11        Authenticated Users
368     smss.exe        S-1-5-18        Local System
368     smss.exe        S-1-5-32-544    Administrators
368     smss.exe        S-1-1-0 Everyone
368     smss.exe        S-1-5-11        Authenticated Users
584     csrss.exe       S-1-5-18        Local System
584     csrss.exe       S-1-5-32-544    Administrators
584     csrss.exe       S-1-1-0 Everyone
584     csrss.exe       S-1-5-11        Authenticated Users
608     winlogon.exe    S-1-5-18        Local System
608     winlogon.exe    S-1-5-32-544    Administrators
608     winlogon.exe    S-1-1-0 Everyone
```

```
1640    reader_sl.exe   S-1-5-21-789336058-261478967-1417001333-1003    Robert
1640    reader_sl.exe   S-1-5-21-789336058-261478967-1417001333-513     Domain Users
1640    reader_sl.exe   S-1-1-0 Everyone
1640    reader_sl.exe   S-1-5-32-544    Administrators
1640    reader_sl.exe   S-1-5-32-545    Users
1640    reader_sl.exe   S-1-5-4 Interactive
1640    reader_sl.exe   S-1-5-11        Authenticated Users
1640    reader_sl.exe   S-1-5-5-0-53426 Logon Session
1640    reader_sl.exe   S-1-2-0 Local (Users with the ability to log in locally)
```

```
└─$ python3 vol.py -f cridex.vmem windows.envars
Volatility 3 Framework 1.0.0
Progress:  100.00               PDB scanning finished
PID     Process Block   Variable        Value

368     smss.exe        0x110048        Path    C:\WINDOWS\System32
368     smss.exe        0x110048        SystemDrive     C:
368     smss.exe        0x110048        SystemRoot      C:\WINDOWS
368     smss.exe        0x110048        ve      C:
368     smss.exe        0x110048        SystemRoot      C:\WINDOWS
368     smss.exe        0x110048        oot     C:\WINDOWS
584     csrss.exe       0x110048        ComSpec C:\WINDOWS\system32\cmd.exe
584     csrss.exe       0x110048        FP_NO_HOST_CHECK        NO
584     csrss.exe       0x110048        NUMBER_OF_PROCESSORS    1
584     csrss.exe       0x110048        OS      Windows_NT
584     csrss.exe       0x110048        Path    C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
584     csrss.exe       0x110048        PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
584     csrss.exe       0x110048        PROCESSOR_ARCHITECTURE  x86
584     csrss.exe       0x110048        PROCESSOR_IDENTIFIER    x86 Family 6 Model 23 Stepping 6, GenuineIntel
584     csrss.exe       0x110048        PROCESSOR_LEVEL 6
584     csrss.exe       0x110048        PROCESSOR_REVISION      1706
584     csrss.exe       0x110048        SystemDrive     C:
584     csrss.exe       0x110048        SystemRoot      C:\WINDOWS
584     csrss.exe       0x110048        TEMP    C:\WINDOWS\TEMP
584     csrss.exe       0x110048        TMP     C:\WINDOWS\TEMP
584     csrss.exe       0x110048        windir  C:\WINDOWS
```

```
1640    reader_sl.exe   0x20048 ALLUSERSPROFILE C:\Documents and Settings\All Users
1640    reader_sl.exe   0x20048 APPDATA C:\Documents and Settings\Robert\Application Data
1640    reader_sl.exe   0x20048 CLIENTNAME      Console
1640    reader_sl.exe   0x20048 CommonProgramFiles      C:\Program Files\Common Files
1640    reader_sl.exe   0x20048 COMPUTERNAME    ACCOUNTING12
1640    reader_sl.exe   0x20048 ComSpec C:\WINDOWS\system32\cmd.exe
1640    reader_sl.exe   0x20048 FP_NO_HOST_CHECK        NO
1640    reader_sl.exe   0x20048 HOMEDRIVE       C:
1640    reader_sl.exe   0x20048 HOMEPATH        \Documents and Settings\Robert
1640    reader_sl.exe   0x20048 LOGONSERVER     \\ACCOUNTING12
1640    reader_sl.exe   0x20048 NUMBER_OF_PROCESSORS    1
1640    reader_sl.exe   0x20048 OS      Windows_NT
1640    reader_sl.exe   0x20048 Path    C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
1640    reader_sl.exe   0x20048 PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
1640    reader_sl.exe   0x20048 PROCESSOR_ARCHITECTURE  x86
1640    reader_sl.exe   0x20048 PROCESSOR_IDENTIFIER    x86 Family 6 Model 23 Stepping 6, GenuineIntel
1640    reader_sl.exe   0x20048 PROCESSOR_LEVEL 6
1640    reader_sl.exe   0x20048 PROCESSOR_REVISION      1706
1640    reader_sl.exe   0x20048 ProgramFiles    C:\Program Files
1640    reader_sl.exe   0x20048 SESSIONNAME     Console
1640    reader_sl.exe   0x20048 SystemDrive     C:
1640    reader_sl.exe   0x20048 SystemRoot      C:\WINDOWS
1640    reader_sl.exe   0x20048 TEMP    C:\DOCUME~1\Robert\LOCALS~1\Temp
1640    reader_sl.exe   0x20048 TMP     C:\DOCUME~1\Robert\LOCALS~1\Temp
1640    reader_sl.exe   0x20048 USERDOMAIN      ACCOUNTING12
1640    reader_sl.exe   0x20048 USERNAME        Robert
1640    reader_sl.exe   0x20048 USERPROFILE     C:\Documents and Settings\Robert
1640    reader_sl.exe   0x20048 windir  C:\WINDOWS
```

```
└─$ python3 vol.py -f cridex.vmem windows.registry.hivelist
Volatility 3 Framework 1.0.0
Progress:  100.00               PDB scanning finished
Offset  FileFullPath    File output

0xe18e5b60      \Device\HarddiskVolume1\Documents and Settings\Robert\Local Settings\Application Data\Microsoft
\Windows\UsrClass.dat   Disabled
0xe1a19b60      \Device\HarddiskVolume1\Documents and Settings\Robert\NTUSER.DAT        Disabled
0xe18398d0      \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Mic
rosoft\Windows\UsrClass.dat     Disabled
0xe18614d0      \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT  Disabled
0xe183bb60      \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\M
icrosoft\Windows\UsrClass.dat   Disabled
0xe17f2b60      \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT        Disabled
0xe1570510      \Device\HarddiskVolume1\WINDOWS\system32\config\software        Disabled
0xe1571008      \Device\HarddiskVolume1\WINDOWS\system32\config\default Disabled
0xe15709b8      \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY        Disabled
0xe15719e8      \Device\HarddiskVolume1\WINDOWS\system32\config\SAM     Disabled
0xe13ba008              Disabled
0xe1035b60      \Device\HarddiskVolume1\WINDOWS\system32\config\system  Disabled
0xe102e008              Disabled
```

```
0xe15719e8      \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
```

```
└─$ python3 vol.py -f cridex.vmem windows.registry.userassist
Volatility 3 Framework 1.0.0
Progress:  100.00               PDB scanning finished
Hive Offset     Hive Name       Path    Last Write Time Type    Name    ID      Count   Focus Count     Time Fo
cused   Last Updated    Raw Data

0×e1a19b60      \Device\HarddiskVolume1\Documents and Settings\Robert\NTUSER.DAT        NTUSER.DAT\Software\Mic
rosoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count  2012-07-22 02:2
6:25.000000     Key     N/A     N/A     N/A     N/A     N/A     N/A     N/A
* 0×e1a19b60    \Device\HarddiskVolume1\Documents and Settings\Robert\NTUSER.DAT        NTUSER.DAT\Software\Mic
rosoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count  2012-07-22 02:2
6:25.000000     Value   UEME_CTLSESSION -       -       -       -       -
8b 3d 6b 0e 03 00 00 00 .=k.....
* 0×e1a19b60    \Device\HarddiskVolume1\Documents and Settings\Robert\NTUSER.DAT        NTUSER.DAT\Software\Mic
rosoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count  2012-07-22 02:2
6:25.000000     Value   UEME_CTLCUACount:ctor   1       2       N/A     N/A     N/A
01 00 00 00 02 00 00 00 ........
00 00 00 00 00 00 00 00 ........
* 0×e1a19b60    \Device\HarddiskVolume1\Documents and Settings\Robert\NTUSER.DAT        NTUSER.DAT\Software\Mic
rosoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count  2012-07-22 02:2
6:25.000000     Value   UEME_UITOOLBAR  1       1       N/A     N/A     2011-04-13 00:56:58.000000
01 00 00 00 06 00 00 00 ........
30 35 b2 b0 75 f9 cb 01 05..u...
* 0×e1a19b60    \Device\HarddiskVolume1\Documents and Settings\Robert\NTUSER.DAT        NTUSER.DAT\Software\Mic
rosoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count  2012-07-22 02:2
6:25.000000     Value   UEME_UITOOLBAR:0×4,7031 1       1       N/A     N/A     2011-04-13 00:56:58.000000
```

```
└─$ python3 vol.py -f cridex.vmem windows.malfind
Volatility 3 Framework 1.0.0
Progress:  100.00               PDB scanning finished
PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output   H
exdump  Disasm

584     csrss.exe       0×7f6f0000      0×7f7effff      Vad     PAGE_EXECUTE_READWRITE  0       0       Disable
d
c8 00 00 00 91 01 00 00 ........
ff ee ff ee 08 70 00 00 .....p..
08 00 00 00 00 fe 00 00 ........
00 00 10 00 00 20 00 00 ........
00 02 00 00 00 20 00 00 ........
8d 01 00 00 ff ef fd 7f ........
03 00 08 06 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........        c8 00 00 00 91 01 00 00 ff ee ff ee 08 70 00 00 08 00 00 00 00 fe 00 00
 00 00 10 00 00 20 00 00 00 02 00 00 00 20 00 00 8d 01 00 00 ff ef fd 7f 03 00 08 06 00 00 00 00 00 00 00 00 00
 00 00 00
```

```
1640    reader_sl.exe   0×3d0000        0×3f0fff        VadS    PAGE_EXECUTE_READWRITE  33      1       Disable
d
4d 5a 90 00 03 00 00 00 MZ......
04 00 00 00 ff ff 00 00 ........
b8 00 00 00 00 00 00 00 ........
40 00 00 00 00 00 00 00 @.......
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 e0 00 00 00 ........        4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00
 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0
 00 00 00
```

Chapter 11: Artifact, Malware, and Ransomware Analysis

```
┌──(kali㉿kali)-[~]
└─$ p0f -h
Command 'p0f' not found, but can be installed with:
sudo apt install p0f
Do you want to install it? (N/y)y
sudo apt install p0f
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
```

```
┌──(kali㉿kali)-[~]
└─$ p0f -h
── p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ──

p0f: invalid option -- 'h'
Usage: p0f [ ... options ... ] [ 'filter rule' ]

Network interface options:

  -i iface  - listen on the specified network interface
  -r file   - read offline pcap data from a given file
  -p        - put the listening interface in promiscuous mode
  -L        - list all available interfaces
```

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.77.159  netmask 255.255.0.0  broadcast 172.16.255.255
        inet6 fe80::a00:27ff:fe42:e90  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:42:0e:90  txqueuelen 1000  (Ethernet)
        RX packets 228  bytes 18623 (18.1 KiB)
        RX errors 0  dropped 4  overruns 0  frame 0
        TX packets 269  bytes 44562 (43.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1572  bytes 130588 (127.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1572  bytes 130588 (127.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
┌──(kali㉿kali)-[~]
└─$ sudo p0f -i eth0
--- p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ---

[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on interface 'eth0'.
[+] Default packet filtering configured [+VLAN].
[+] Entered main event loop.
```

```
[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on interface 'eth0'.
[+] Default packet filtering configured [+VLAN].
[+] Entered main event loop.

.-[ 172.16.77.161/33364 -> 172.16.77.159/7 (syn) ]-
|
| client   = 172.16.77.161/33364
| os       = Linux 2.2.x-3.x
| dist     = 0
| params   = generic
| raw_sig  = 4:64+0:0:1460:65535,7:mss,sok,ts,nop,ws:df,id+:0
|
`----

.-[ 172.16.77.161/33364 -> 172.16.77.159/7 (mtu) ]-
|
| client   = 172.16.77.161/33364
| link     = Ethernet or modem
| raw_mtu  = 1500
|
`----
```

```
.-[ 172.16.77.159/53382 -> 185.230.60.211/80 (syn) ]-
|
| client   = 172.16.77.159/53382
| os       = Linux 2.2.x-3.x
| dist     = 0
| params   = generic
| raw_sig  = 4:64+0:0:1460:mss*44,7:mss,sok,ts,nop,ws:df,id+:0
|
`----

.-[ 172.16.77.159/53382 -> 185.230.60.211/80 (mtu) ]-
|
| client   = 172.16.77.159/53382
| link     = Ethernet or modem
| raw_mtu  = 1500
|
```

```
inetnum:        185.230.60.0 - 185.230.60.255
netname:        wix_com_inc
country:        US
admin-c:        SP17239-RIPE
tech-c:         SP17239-RIPE
status:         LIR-PARTITIONED PA
mnt-by:         il-wixcom-sys-mnt
mnt-by:         il-wixcom-1-mnt
created:        2018-05-21T15:00:58Z
last-modified:  2019-10-10T07:20:09Z
source:         RIPE

person:         Stanislav Panich
address:        Namal Tel Aviv 40
phone:          +972 3 5454900
nic-hdl:        SP17239-RIPE
mnt-by:         il-wixcom-sys-mnt
created:        2018-05-09T15:30:17Z
last-modified:  2018-05-09T15:30:17Z
source:         RIPE
```

```
.-[ 172.16.77.159/47460 -> 185.230.60.211/443 (uptime) ]-
|
| server   = 185.230.60.211/443
| uptime   = 33 days 15 hrs 14 min (modulo 49 days)
| raw_freq = 1003.42 Hz
|
`----

.-[ 172.16.77.159/52308 -> 35.241.16.116/443 (syn) ]-
|
| client   = 172.16.77.159/52308
| os       = Linux 2.2.x-3.x
| dist     = 0
| params   = generic
| raw_sig  = 4:64+0:0:1460:mss*44,7:mss,sok,ts,nop,ws:df,id+:0
|
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ git clone https://github.com/sevagas/swap_digger.git
Cloning into 'swap_digger' ...
remote: Enumerating objects: 147, done.
remote: Counting objects: 100% (30/30), done.
remote: Compressing objects: 100% (19/19), done.
remote: Total 147 (delta 15), reused 21 (delta 11), pack-reused 117
Receiving objects: 100% (147/147), 357.52 KiB | 1.21 MiB/s, done.
Resolving deltas: 100% (69/69), done.
```

```
┌──(kali㉿kali)-[~/Desktop/swap_digger]
└─$ sudo ./swap_digger.sh -h
Searches for valuable and sensitive data in Linux SWAP memory.
Usage: ./swap_digger.sh [ OPTIONS ]

Options :
  -p, --passwd                Search for system passwords
  -g, --guessing              Try to guess potential passwords based on observations and stats.
                              hundreds false positives. (Warning: This option is not reliable,
                              it may dig more passwords as well as
  -a, --app-data              Run extended tests on the target swap to retrieve other interesting
data
                              (web passwords, emails, wifi creds, most accessed URLs, hashes etc)
  -v, --verbose               Verbose mode.
  -l, --log                   Log all outputs in a log file (protected inside the generated workin
g directory).
  -c, --clean                 Automatically erase the generated working directory at end of script
 (will also remove log file)
  -r PATH, --root-path PATH   Location of the target file-system root (default value is /)
                              Change this value for forensic analysis when target is a mounted fil
e system.
                              This option has to  be used along the -s option to indicate path to
swap device.
  -s PATH, --swap-path PATH   Location of swap device or swap dump to analyse
                              Use this option for forensic/remote analysis of a swap dump or a mou
nted external swap partition.
                              This option should be used with the -r option where at least /<root-
path>/etc/shadow exists.
  -S, --swap-search           Search for all available swap devices.
  -h, --help                  Display this help.

  For more details see the README.md file at https://github.com/sevagas/swap_digger
```

```
┌──(kali㉿kali)-[~/Desktop/swap_digger]
└─$ sudo ./swap_digger.sh -p

  - SWAP Digger -

 [+] Looking for swap partition
     → Found swap at /swapfile
 [+] Dumping swap strings in /tmp/swap_dig/swap_dump.txt  ... (this may take some time)


   ═══ Linux system accounts ═══

 [+] Digging linux accounts credentials ... (pattern attack)
 Passwords not found. Attempt dictionary based attack? (Can last from 5 minutes to several hours d
epending on swap usage) [y/n] y

 [+] Digging linux accounts credentials method 2  ... (dictionary attack)
   [-] Generating wordlist file ...
   [-] Digging passwords in wordlist ... (This may take 5min to few hours!)
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ git clone https://github.com/huntergregal/mimipenguin
Cloning into 'mimipenguin' ...
remote: Enumerating objects: 533, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (8/8), done.
remote: Total 533 (delta 1), reused 1 (delta 0), pack-reused 525
Receiving objects: 100% (533/533), 185.62 KiB | 795.00 KiB/s, done.
Resolving deltas: 100% (242/242), done.
```

```
┌──(kali㉿kali)-[~/Desktop/mimipenguin]
└─$ ls
include  LICENSE  Makefile  mimipenguin.py  mimipenguin.sh  README.md  src
```

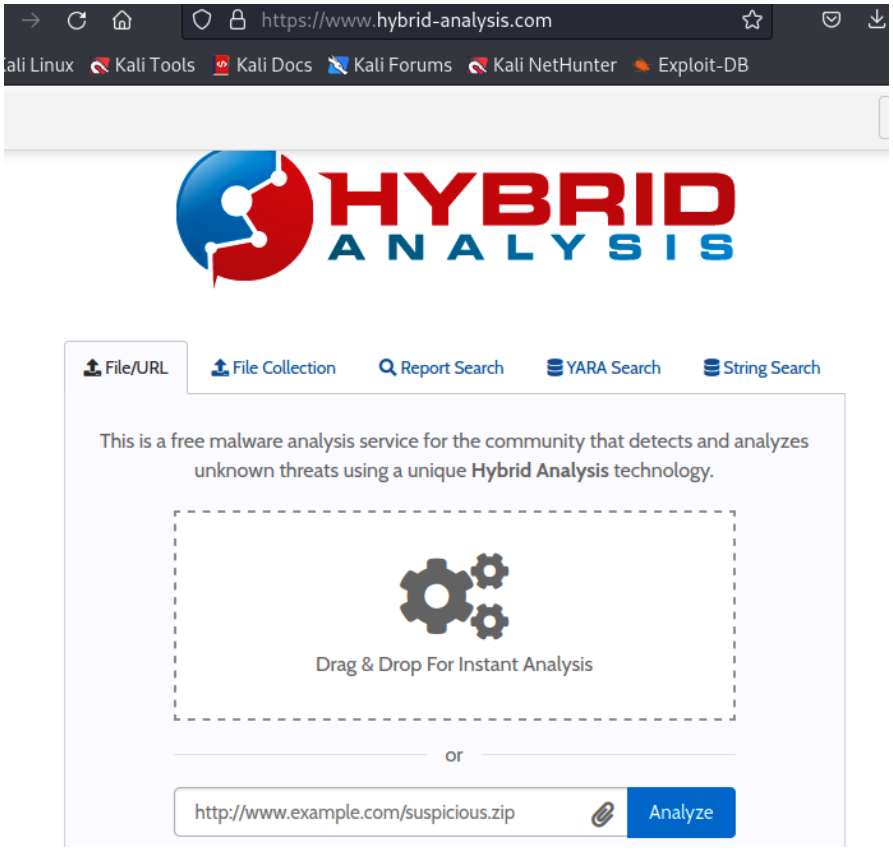
```
[+] GNOME KEYRING (823)
  [-] root:toor
```

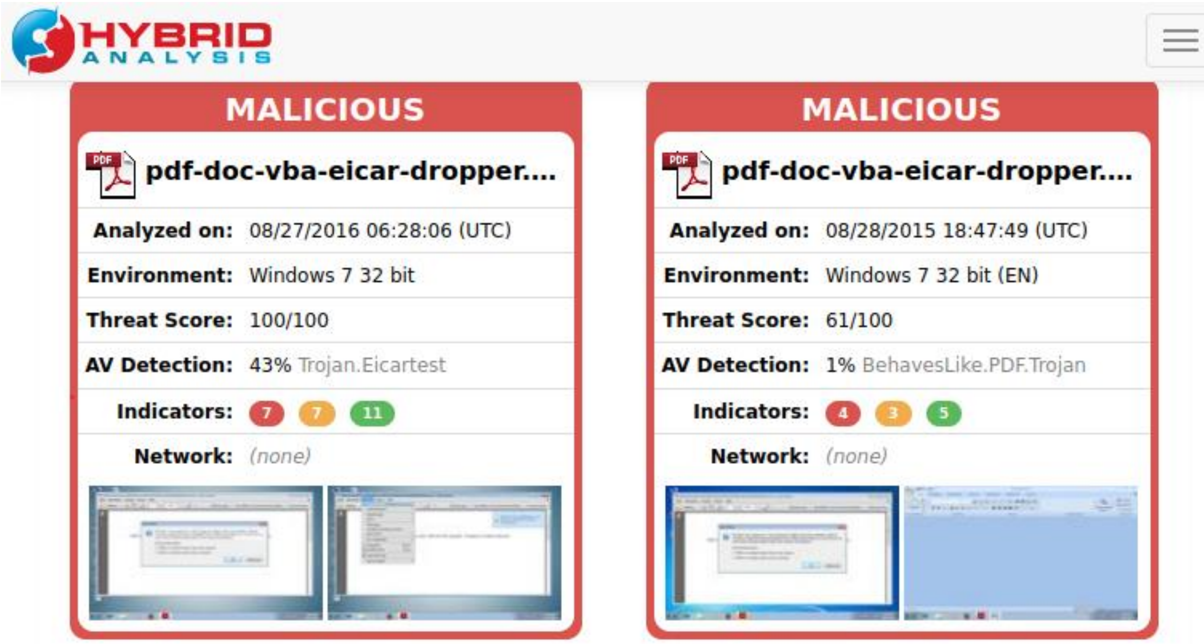
```
┌──(kali㉿kali)-[~/Desktop]
└─$ pdf-parser -h
This program has not been tested with this version of Python (3.10.6)
Should you encounter problems, please use Python version 3.10.4
Usage: pdf-parser [options] pdf-file|zip-file|url
pdf-parser, use it to parse a PDF document

Options:
  --version             show program's version number and exit
  -h, --help            show this help message and exit
  -m, --man             Print manual
  -s SEARCH, --search=SEARCH
                        string to search in indirect objects (except streams)
  -f, --filter          pass stream object through filters (FlateDecode,
                        ASCIIHexDecode, ASCII85Decode, LZWDecode and
                        RunLengthDecode only)
  -o OBJECT, --object=OBJECT
                        id(s) of indirect object(s) to select, use comma (,)
                        to separate ids (version independent)
  -r REFERENCE, --reference=REFERENCE
                        id of indirect object being referenced (version
                        independent)
  -e ELEMENTS, --elements=ELEMENTS
                        type of elements to select (cxtsi)
  -w, --raw             raw output for data and filters
  -a, --stats           display stats for pdf document
  -t TYPE, --type=TYPE  type of indirect object to select
  -O, --objstm          parse stream of /ObjStm objects
  -v, --verbose         display malformed PDF elements
```

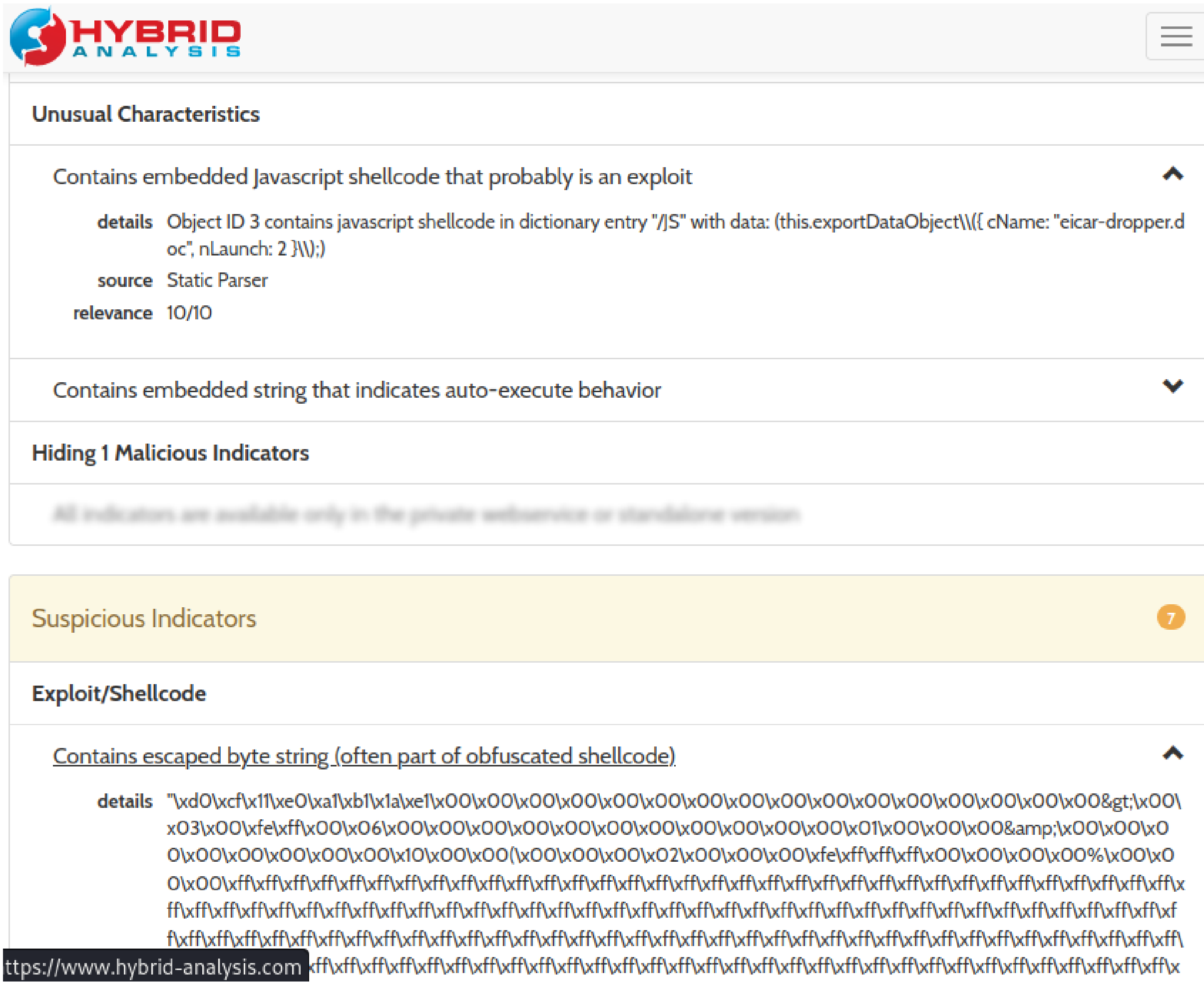
```
┌──(kali㉿kali)-[~/Desktop]
└─$ pdf-parser -a testpdf.pdf
This program has not been tested with this version of Python (3.10.6)
Should you encounter problems, please use Python version 3.10.4
Comment: 3
XREF: 1
Trailer: 1
StartXref: 1
Indirect object: 9
  1: 5
 /Action 1: 9
 /Catalog 1: 1
 /EmbeddedFile 1: 8
 /Filespec 1: 7
 /Font 1: 6
 /Outlines 1: 2
 /Page 1: 4
 /Pages 1: 3
Search keywords:
 /JS 1: 9
 /JavaScript 1: 9
 /OpenAction 1: 1
 /EmbeddedFile 1: 8
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ pdf-parser -f testpdf.pdf
This program has not been tested with this version of Python (3.10.6)
Should you encounter problems, please use Python version 3.10.4
PDF Comment '%PDF-1.1\r\n'

PDF Comment '%\xd0\xd0\xd0\xd0\r\n'

obj 1 0
 Type: /Catalog
 Referencing: 2 0 R, 3 0 R, 7 0 R, 9 0 R

  <<
    /Type /Catalog
    /Outlines 2 0 R
    /Pages 3 0 R
    /Names
      <<
        /EmbeddedFiles
          <<
            /Names [(eicar-dropper.doc) 7 0 R]
          >>
      >>
    /OpenAction 9 0 R
  >>

 [(1, '\r\n'), (2, '<<'), (1, '\r\n '), (2, '/Type'), (1, ' '), (2, '/Ca
\r\n '), (2, '/Outlines'), (1, ' '), (3, '2'), (1, ' '), (3, '0'), (1, '
 (1, '\r\n '), (2, '/Pages'), (1, ' '), (3, '3'), (1, ' '), (3, '0'), (1
'), (1, '\r\n '), (2, '/Names'), (1, ' '), (2, '<<'), (1, ' '), (2, '/Em
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ pdfid testpdf.pdf
PDFiD 0.2.8 testpdf.pdf
 PDF Header: %PDF-1.1
 obj                    9
 endobj                 9
 stream                 2
 endstream              2
 xref                   1
 trailer                1
 startxref              1
 /Page                  1
 /Encrypt               0
 /ObjStm                0
 /JS                    1
 /JavaScript            1
 /AA                    0
 /OpenAction            1
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          1
 /XFA                   0
 /Colors > 2^24         0
```




HYBRID ANALYSIS
MALICIOUS
pdf-doc-vba-eicar-dropper....
Analyzed on: 08/27/2016 06:28:06 (UTC)
Environment: Windows 7 32 bit
Threat Score: 100/100
AV Detection: 43% Trojan.Eicartest
Indicators: 7 7 11
Network: (none)
MALICIOUS
pdf-doc-vba-eicar-dropper....
Analyzed on: 08/28/2015 18:47:49 (UTC)
Environment: Windows 7 32 bit (EN)
Threat Score: 61/100
AV Detection: 1% BehavesLike.PDF.Trojan
Indicators: 4 3 5
Network: (none)


HYBRID ANALYSIS
Unusual Characteristics
Contains embedded Javascript shellcode that probably is an exploit
details Object ID 3 contains javascript shellcode in dictionary entry "/JS" with data: (this.exportDataObject\\({ cName: "eicar-dropper.doc", nLaunch: 2 }\\);)
source Static Parser
relevance 10/10
Contains embedded string that indicates auto-execute behavior
Hiding 1 Malicious Indicators
Suspicious Indicators 7
Exploit/Shellcode
Contains escaped byte string (often part of obfuscated shellcode)
details "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00>\x00\x03\x00\xfe\xff\x00\x06\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00&\x00\x00\x00\x00\x00\x00\x00\x00\x10\x00\x00(\x00\x00\x00\x02\x00\x00\x00\xfe\xff\xff\xff\x00\x00\x00\x00%\x00\x00\x00\xff\x
ttps://www.hybrid-analysis.com

```
┌──(kali㉿kali)-[~/Downloads/volatility3]
└─$ ls
build                MANIFEST.in            volshell.py
cridex_memdump.zip   mypy.ini               volshell.spec
cridex.vmem          README.md              vol.spec
development          setup.py               'wannacry pw- infected'
dist                 volatility3            'wannacry pw- infected.7z'
doc                  volatility3.egg-info   wcry.raw
LICENSE.txt          vol.py
```

```
┌──(kali㉿kali)-[~/Downloads/volatility3]
└─$ python3 vol.py -f wcry.raw windows.info
Volatility 3 Framework 1.0.0
Progress:    0.20              Reading file http://msdl.microsoft.com/download/sy
Progress:    0.40b/423320282DB84Reading file http://msdl.microsoft.com/download/sy
Progress:    0.60b/423320282DB84Reading file http://msdl.microsoft.com/download/sy
Progress:    0.80b/423320282DB84Reading file http://msdl.microsoft.com/download/sy
Progress:    1.00b/423320282DB84Reading file http://msdl.microsoft.com/download/sy
```

```
NTBuildLab      2600.xpsp_sp3_qfe.130704-0421
CSDVersion      3
KdVersionBlock  0x8054cf38
Major/Minor     15.2600
MachineType     332
KeNumberProcessors      1
SystemTime      2017-05-12 21:26:32
NtSystemRoot    C:\WINDOWS
NtProductType   NtProductWinNt
NtMajorVersion  5
NtMinorVersion  1
PE MajorOperatingSystemVersion  5
PE MinorOperatingSystemVersion  1
PE Machine      332
PE TimeDateStamp        Thu Jul  4 02:58:58 2013
```

```
┌──(kali㉿kali)-[~/Downloads/volatility3]
└─$ python3 vol.py -f wcry.raw windows.pslist
Volatility 3 Framework 1.0.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0×823c8830      51      244     N/A     False   N/A     N/A     Disabled
348     4       smss.exe        0×82169020      3       19      N/A     False   2017-05-12 21:21:55.000000      N/A     Disabled
596     348     csrss.exe       0×82161da0      12      352     0       False   2017-05-12 21:22:00.000000      N/A     Disabled
620     348     winlogon.exe    0×8216e020      23      536     0       False   2017-05-12 21:22:01.000000      N/A     Disabled
664     620     services.exe    0×821937f0      15      265     0       False   2017-05-12 21:22:01.000000      N/A     Disabled
676     620     lsass.exe       0×82191658      23      353     0       False   2017-05-12 21:22:01.000000      N/A     Disabled
836     664     svchost.exe     0×8221a2c0      19      211     0       False   2017-05-12 21:22:02.000000      N/A     Disabled
904     664     svchost.exe     0×821b5230      9       227     0       False   2017-05-12 21:22:03.000000      N/A     Disabled
1024    664     svchost.exe     0×821af7e8      79      1366    0       False   2017-05-12 21:22:03.000000      N/A     Disabled
1084    664     svchost.exe     0×8203b7a8      6       72      0       False   2017-05-12 21:22:03.000000      N/A     Disabled
1152    664     svchost.exe     0×821bea78      10      173     0       False   2017-05-12 21:22:06.000000      N/A     Disabled
1484    664     spoolsv.exe     0×821e2da0      14      124     0       False   2017-05-12 21:22:09.000000      N/A     Disabled
1636    1608    explorer.exe    0×821d9da0      11      331     0       False   2017-05-12 21:22:10.000000      N/A     Disabled
1940    1636    tasksche.exe    0×82218da0      7       51      0       False   2017-05-12 21:22:14.000000      N/A     Disabled
1956    1636    ctfmon.exe      0×82231da0      1       86      0       False   2017-05-12 21:22:14.000000      N/A     Disabled
260     664     svchost.exe     0×81fb95d8      5       105     0       False   2017-05-12 21:22:18.000000      N/A     Disabled
740     1940    @WanaDecryptor@ 0×81fde308      2       70      0       False   2017-05-12 21:22:22.000000      N/A     Disabled
1768    1024    wuauclt.exe     0×81f747c0      7       132     0       False   2017-05-12 21:22:52.000000      N/A     Disabled
544     664     alg.exe 0×82010020      6       101     0       False   2017-05-12 21:22:55.000000      N/A     Disabled
1168    1024    wscntfy.exe     0×81fea8a0      1       37      0       False   2017-05-12 21:22:56.000000      N/A     Disabled
```

```
┌──(kali㉿kali)-[~/Downloads/volatility3]
└─$ python3 vol.py -f wcry.raw windows.pslist
Volatility 3 Framework 1.0.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0×823c8830      51      244     N/A     False   N/A     N/A     Disabled
348     4       smss.exe        0×82169020      3       19      N/A     False   2017-05-12 21:21:55.000000      N/A     Disabled
596     348     csrss.exe       0×82161da0      12      352     0       False   2017-05-12 21:22:00.000000      N/A     Disabled
620     348     winlogon.exe    0×8216e020      23      536     0       False   2017-05-12 21:22:01.000000      N/A     Disabled
664     620     services.exe    0×821937f0      15      265     0       False   2017-05-12 21:22:01.000000      N/A     Disabled
676     620     lsass.exe       0×82191658      23      353     0       False   2017-05-12 21:22:01.000000      N/A     Disabled
836     664     svchost.exe     0×8221a2c0      19      211     0       False   2017-05-12 21:22:02.000000      N/A     Disabled
904     664     svchost.exe     0×821b5230      9       227     0       False   2017-05-12 21:22:03.000000      N/A     Disabled
1024    664     svchost.exe     0×821af7e8      79      1366    0       False   2017-05-12 21:22:03.000000      N/A     Disabled
1084    664     svchost.exe     0×8203b7a8      6       72      0       False   2017-05-12 21:22:03.000000      N/A     Disabled
1152    664     svchost.exe     0×821bea78      10      173     0       False   2017-05-12 21:22:06.000000      N/A     Disabled
1484    664     spoolsv.exe     0×821e2da0      14      124     0       False   2017-05-12 21:22:09.000000      N/A     Disabled
1636    1608    explorer.exe    0×821d9da0      11      331     0       False   2017-05-12 21:22:10.000000      N/A     Disabled
1940    1636    tasksche.exe    0×82218da0      7       51      0       False   2017-05-12 21:22:14.000000      N/A     Disabled
1956    1636    ctfmon.exe      0×82231da0      1       86      0       False   2017-05-12 21:22:14.000000      N/A     Disabled
260     664     svchost.exe     0×81fb95d8      5       105     0       False   2017-05-12 21:22:18.000000      N/A     Disabled
740     1940    @WanaDecryptor@ 0×81fde308      2       70      0       False   2017-05-12 21:22:22.000000      N/A     Disabled
1768    1024    wuauclt.exe     0×81f747c0      7       132     0       False   2017-05-12 21:22:52.000000      N/A     Disabled
544     664     alg.exe 0×82010020      6       101     0       False   2017-05-12 21:22:55.000000      N/A     Disabled
1168    1024    wscntfy.exe     0×81fea8a0      1       37      0       False   2017-05-12 21:22:56.000000      N/A     Disabled
```

```
└─$ python3 vol.py -f wcry.raw windows.pstree
Volatility 3 Framework 1.0.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime

4       0       System  0×81fea8a0      51      244     N/A     False   N/A     N/A
* 348   4       smss.exe        0×81fea8a0      3       19      N/A     False   2017-05-12 21:21:55.000000      N/A
** 620  348     winlogon.exe    0×81fea8a0      23      536     0       False   2017-05-12 21:22:01.000000      N/A
** 664 620      services.exe    0×81fea8a0      15      265     0       False   2017-05-12 21:22:01.000000      N/A
**** 1024       664     svchost.exe     0×81fea8a0      79      1366    0       False   2017-05-12 21:22:03.000000
***** 1768      1024    wuauclt.exe     0×81fea8a0      7       132     0       False   2017-05-12 21:22:52.000000
***** 1168      1024    wscntfy.exe     0×81fea8a0      1       37      0       False   2017-05-12 21:22:56.000000
**** 1152       664     svchost.exe     0×81fea8a0      10      173     0       False   2017-05-12 21:22:06.000000
**** 544        664     alg.exe 0×81fea8a0      6       101     0       False   2017-05-12 21:22:55.000000      N/A
**** 836        664     svchost.exe     0×81fea8a0      19      211     0       False   2017-05-12 21:22:02.000000
**** 260        664     svchost.exe     0×81fea8a0      5       105     0       False   2017-05-12 21:22:18.000000
**** 904        664     svchost.exe     0×81fea8a0      9       227     0       False   2017-05-12 21:22:03.000000
**** 1484       664     spoolsv.exe     0×81fea8a0      14      124     0       False   2017-05-12 21:22:09.000000
**** 1084       664     svchost.exe     0×81fea8a0      6       72      0       False   2017-05-12 21:22:03.000000
** 676 620      lsass.exe       0×81fea8a0      23      353     0       False   2017-05-12 21:22:01.000000      N/A
** 596  348     csrss.exe       0×81fea8a0      12      352     0       False   2017-05-12 21:22:00.000000      N/A
1636    1608    explorer.exe    0×81fea8a0      11      331     0       False   2017-05-12 21:22:10.000000      N/A
* 1956  1636    ctfmon.exe      0×81fea8a0      1       86      0       False   2017-05-12 21:22:14.000000      N/A
* 1940  1636    tasksche.exe    0×81fea8a0      7       51      0       False   2017-05-12 21:22:14.000000      N/A
** 740  1940     @WanaDecryptor@ 0×81fea8a0      2       70      0       False   2017-05-12 21:22:22.000000      N/A
```

```
└─$ python3 vol.py -f wcry.raw windows.psscan
Volatility 3 Framework 1.0.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset  Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

860     1940    taskdl.exe      0x1f4daf0       0       -       0       False   2017-05-12 21:26:23.000000      2017-05-12 21:26:23.000000
536     1940    taskse.exe      0x1f53d18       0       -       0       False   2017-05-12 21:26:22.000000      2017-05-12 21:26:23.000000
424     1940    @WanaDecryptor@ 0x1f69b50       0       -       0       False   2017-05-12 21:25:52.000000      2017-05-12 21:25:53.000000
1768    1024    wuauclt.exe     0x1f747c0       7       132     0       False   2017-05-12 21:22:52.000000      N/A     Disabled
576     1940    @WanaDecryptor@ 0x1f8ba58       0       -       0       False   2017-05-12 21:26:22.000000      2017-05-12 21:26:23.000000
260     664     svchost.exe     0x1fb95d8       5       105     0       False   2017-05-12 21:22:18.000000      N/A     Disabled
740     1940    @WanaDecryptor@ 0x1fde308       2       70      0       False   2017-05-12 21:22:22.000000      N/A     Disabled
1168    1024    wscntfy.exe     0x1fea8a0       1       37      0       False   2017-05-12 21:22:56.000000      N/A     Disabled
544     664     alg.exe 0x2010020       6       101     0       False   2017-05-12 21:22:55.000000      N/A     Disabled
1084    664     svchost.exe     0x203b7a8       6       72      0       False   2017-05-12 21:22:03.000000      N/A     Disabled
596     348     csrss.exe       0x2161da0       12      352     0       False   2017-05-12 21:22:00.000000      N/A     Disabled
348     4       smss.exe        0x2169020       3       19      N/A     False   2017-05-12 21:21:55.000000      N/A     Disabled
620     348     winlogon.exe    0x216e020       23      536     0       False   2017-05-12 21:22:01.000000      N/A     Disabled
676     620     lsass.exe       0x2191658       23      353     0       False   2017-05-12 21:22:01.000000      N/A     Disabled
664     620     services.exe    0x21937f0       15      265     0       False   2017-05-12 21:22:01.000000      N/A     Disabled
1024    664     svchost.exe     0x21af7e8       79      1366    0       False   2017-05-12 21:22:03.000000      N/A     Disabled
904     664     svchost.exe     0x21b5230       9       227     0       False   2017-05-12 21:22:03.000000      N/A     Disabled
1152    664     svchost.exe     0x21bea78       10      173     0       False   2017-05-12 21:22:06.000000      N/A     Disabled
1636    1608    explorer.exe    0x21d9da0       11      331     0       False   2017-05-12 21:22:10.000000      N/A     Disabled
1484    664     spoolsv.exe     0x21e2da0       14      124     0       False   2017-05-12 21:22:09.000000      N/A     Disabled
1940    1636    tasksche.exe    0x2218da0       7       51      0       False   2017-05-12 21:22:14.000000      N/A     Disabled
836     664     svchost.exe     0x221a2c0       19      211     0       False   2017-05-12 21:22:02.000000      N/A     Disabled
1956    1636    ctfmon.exe      0x2231da0       1       86      0       False   2017-05-12 21:22:14.000000      N/A     Disabled
4       0       System  0x23c8830       51      244     N/A     False   N/A     N/A     Disabled
```

```
└─$ python3 vol.py -f wcry.raw windows.cmdline
Volatility 3 Framework 1.0.0
Progress:  100.00               PDB scanning finished
PID     Process Args

4       System  Required memory at 0x10 is not valid (process exited?)
348     smss.exe        \SystemRoot\System32\smss.exe
596     csrss.exe       C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSe
rverDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Of
620     winlogon.exe    winlogon.exe
664     services.exe    C:\WINDOWS\system32\services.exe
676     lsass.exe       C:\WINDOWS\system32\lsass.exe
836     svchost.exe     C:\WINDOWS\system32\svchost -k DcomLaunch
904     svchost.exe     C:\WINDOWS\system32\svchost -k rpcss
1024    svchost.exe     C:\WINDOWS\System32\svchost.exe -k netsvcs
1084    svchost.exe     C:\WINDOWS\system32\svchost.exe -k NetworkService
1152    svchost.exe     C:\WINDOWS\system32\svchost.exe -k LocalService
1484    spoolsv.exe     C:\WINDOWS\system32\spoolsv.exe
1636    explorer.exe    C:\WINDOWS\Explorer.EXE
1940    tasksche.exe    "C:\Intel\ivecuqmanpnirkt615\tasksche.exe"
1956    ctfmon.exe      "C:\WINDOWS\system32\ctfmon.exe"
260     svchost.exe     C:\WINDOWS\system32\svchost.exe -k LocalService
740     @WanaDecryptor@ @WanaDecryptor@.exe
1768    wuauclt.exe     "C:\WINDOWS\system32\wuauclt.exe" /RunStoreAsComServer Local\[4
544     alg.exe C:\WINDOWS\System32\alg.exe
1168    wscntfy.exe     C:\WINDOWS\system32\wscntfy.exe
```

```
└─$ python3 vol.py -f wcry.raw windows.envars
Volatility 3 Framework 1.0.0
Progress:  100.00               PDB scanning finished
PID     Process Block   Variable        Value

348     smss.exe        0x110048        Path    C:\WINDOWS\System32
348     smss.exe        0x110048        SystemDrive     C:
348     smss.exe        0x110048        SystemRoot      C:\WINDOWS
348     smss.exe        0x110048        ve      C:
348     smss.exe        0x110048        SystemRoot      C:\WINDOWS
348     smss.exe        0x110048        oot     C:\WINDOWS
596     csrss.exe       0x110048        ComSpec C:\WINDOWS\system32\cmd.exe
596     csrss.exe       0x110048        FP_NO_HOST_CHECK        NO
596     csrss.exe       0x110048        NUMBER_OF_PROCESSORS    1
```

```
740     @WanaDecryptor@ 0x20048 ALLUSERSPROFILE C:\Documents and Settings\All Users
740     @WanaDecryptor@ 0x20048 APPDATA C:\Documents and Settings\donny\Application Data
740     @WanaDecryptor@ 0x20048 CLIENTNAME      Console
740     @WanaDecryptor@ 0x20048 CommonProgramFiles      C:\Program Files\Common Files
740     @WanaDecryptor@ 0x20048 COMPUTERNAME    INFOSECL-5A7C18
740     @WanaDecryptor@ 0x20048 ComSpec C:\WINDOWS\system32\cmd.exe
740     @WanaDecryptor@ 0x20048 FP_NO_HOST_CHECK        NO
740     @WanaDecryptor@ 0x20048 HOMEDRIVE       C:
740     @WanaDecryptor@ 0x20048 HOMEPATH        \Documents and Settings\donny
740     @WanaDecryptor@ 0x20048 LOGONSERVER     \\INFOSECL-5A7C18
740     @WanaDecryptor@ 0x20048 NUMBER_OF_PROCESSORS    1
740     @WanaDecryptor@ 0x20048 OS      Windows_NT
740     @WanaDecryptor@ 0x20048 Path    C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
740     @WanaDecryptor@ 0x20048 PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
740     @WanaDecryptor@ 0x20048 PROCESSOR_ARCHITECTURE  x86
740     @WanaDecryptor@ 0x20048 PROCESSOR_IDENTIFIER    x86 Family 6 Model 78 Stepping 3, GenuineIntel
740     @WanaDecryptor@ 0x20048 PROCESSOR_LEVEL 6
740     @WanaDecryptor@ 0x20048 PROCESSOR_REVISION      4e03
740     @WanaDecryptor@ 0x20048 ProgramFiles    C:\Program Files
740     @WanaDecryptor@ 0x20048 SESSIONNAME     Console
740     @WanaDecryptor@ 0x20048 SystemDrive     C:
740     @WanaDecryptor@ 0x20048 SystemRoot      C:\WINDOWS
740     @WanaDecryptor@ 0x20048 TEMP    C:\DOCUME~1\donny\LOCALS~1\Temp
740     @WanaDecryptor@ 0x20048 TMP     C:\DOCUME~1\donny\LOCALS~1\Temp
740     @WanaDecryptor@ 0x20048 USERDOMAIN      INFOSECL-5A7C18
740     @WanaDecryptor@ 0x20048 USERNAME        donny
```

```
└─$ python3 vol.py -f wcry.raw windows.getsids
Volatility 3 Framework 1.0.0
Progress:  100.00               PDB scanning finished
PID     Process SID     Name

4       System  S-1-5-18        Local System
4       System  S-1-5-32-544    Administrators
4       System  S-1-1-0 Everyone
4       System  S-1-5-11        Authenticated Users
348     smss.exe        S-1-5-18        Local System
348     smss.exe        S-1-5-32-544    Administrators
348     smss.exe        S-1-1-0 Everyone
348     smss.exe        S-1-5-11        Authenticated Users
596     csrss.exe       S-1-5-18        Local System
596     csrss.exe       S-1-5-32-544    Administrators
596     csrss.exe       S-1-1-0 Everyone
596     csrss.exe       S-1-5-11        Authenticated Users
620     winlogon.exe    S-1-5-18        Local System
620     winlogon.exe    S-1-5-32-544    Administrators
620     winlogon.exe    S-1-1-0 Everyone
620     winlogon.exe    S-1-5-11        Authenticated Users
664     services.exe    S-1-5-18        Local System
664     services.exe    S-1-5-32-544    Administrators
```

```
740     @WanaDecryptor@ S-1-5-21-602162358-764733703-1957994488-1003    donny
740     @WanaDecryptor@ S-1-5-21-602162358-764733703-1957994488-513     Domain Users
740     @WanaDecryptor@ S-1-1-0 Everyone
740     @WanaDecryptor@ S-1-5-32-544    Administrators
740     @WanaDecryptor@ S-1-5-32-545    Users
740     @WanaDecryptor@ S-1-5-4 Interactive
740     @WanaDecryptor@ S-1-5-11        Authenticated Users
740     @WanaDecryptor@ S-1-5-5-0-39677 Logon Session
740     @WanaDecryptor@ S-1-2-0 Local (Users with the ability to log in locally)
```

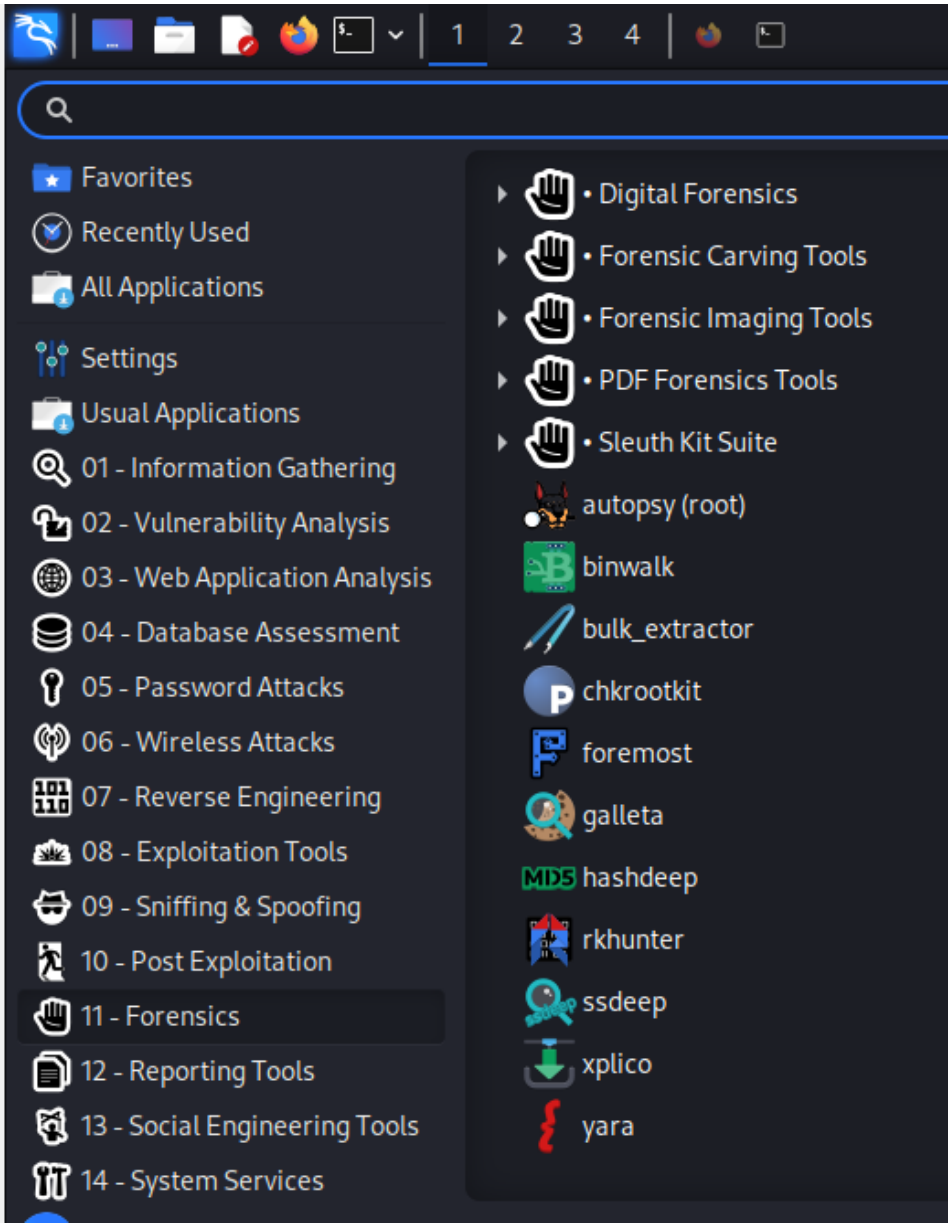
```
740   @WanaDecryptor@ 23    SeChangeNotifyPrivilege Present,Enabled,Default Receive notifications of changes to files
740   @WanaDecryptor@ 8     SeSecurityPrivilege     Present Manage auditing and security log
740   @WanaDecryptor@ 17    SeBackupPrivilege       Present Backup files and directories
740   @WanaDecryptor@ 18    SeRestorePrivilege      Present Restore files and directories
740   @WanaDecryptor@ 12    SeSystemtimePrivilege   Present Change the system time
740   @WanaDecryptor@ 19    SeShutdownPrivilege     Present Shut down the system
740   @WanaDecryptor@ 24    SeRemoteShutdownPrivilege       Present Force shutdown from a remote system
740   @WanaDecryptor@ 9     SeTakeOwnershipPrivilege        Present Take ownership of files/objects
740   @WanaDecryptor@ 20    SeDebugPrivilege        Present Debug programs
740   @WanaDecryptor@ 22    SeSystemEnvironmentPrivilege    Present Edit firmware environment values
740   @WanaDecryptor@ 11    SeSystemProfilePrivilege        Present Profile system performance
740   @WanaDecryptor@ 13    SeProfileSingleProcessPrivilege Present Profile a single process
740   @WanaDecryptor@ 14    SeIncreaseBasePriorityPrivilege Present Increase scheduling priority
740   @WanaDecryptor@ 10    SeLoadDriverPrivilege   Present,Enabled Load and unload device drivers
740   @WanaDecryptor@ 15    SeCreatePagefilePrivilege       Present Create a pagefile
740   @WanaDecryptor@ 5     SeIncreaseQuotaPrivilege        Present Increase quotas
740   @WanaDecryptor@ 25    SeUndockPrivilege       Present,Enabled Remove computer from docking station
740   @WanaDecryptor@ 28    SeManageVolumePrivilege Present Manage the files on a volume
740   @WanaDecryptor@ 29    SeImpersonatePrivilege  Present,Enabled,Default Impersonate a client after authentication
740   @WanaDecryptor@ 30    SeCreateGlobalPrivilege Present,Enabled,Default Create global objects
```

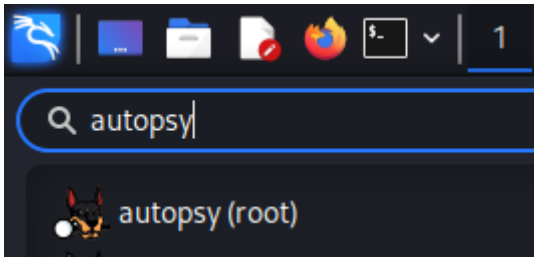
```
└─$ python3 vol.py -f wcry.raw windows.malfind
Volatility 3 Framework 1.0.0
Progress:  100.00               PDB scanning finished
PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory

596     csrss.exe       0x7f6f0000      0x7f7effff      Vad     PAGE_EXECUTE_READWRITE  0
c8 00 00 00 8b 01 00 00 ........
ff ee ff ee 08 70 00 00 .....p..
08 00 00 00 00 fe 00 00 ........
00 00 10 00 00 20 00 00 ........
00 02 00 00 00 20 00 00 ........
8d 01 00 00 ff ef fd 7f ........
03 00 08 06 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........        c8 00 00 00 8b 01 00 00 ff ee ff ee 08 70 00 00 08 00 0
 03 00 08 06 00 00 00 00 00 00 00 00 00 00 00
620     winlogon.exe    0x21400000      0x21403fff      VadS    PAGE_EXECUTE_READWRITE  4
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 28 00 28 00 ....(.(.
01 00 00 00 00 00 00 00 ........        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
 00 00 00 00 28 00 28 00 01 00 00 00 00 00 00 00
620     winlogon.exe    0x3f8b0000      0x3f8b3fff      VadS    PAGE_EXECUTE_READWRITE  4
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 25 00 25 00 ....%.%.
01 00 00 00 00 00 00 00 ........        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
 00 00 00 00 25 00 25 00 01 00 00 00 00 00 00 00
620     winlogon.exe    0x44b90000      0x44b93fff      VadS    PAGE_EXECUTE_READWRITE  4
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
```

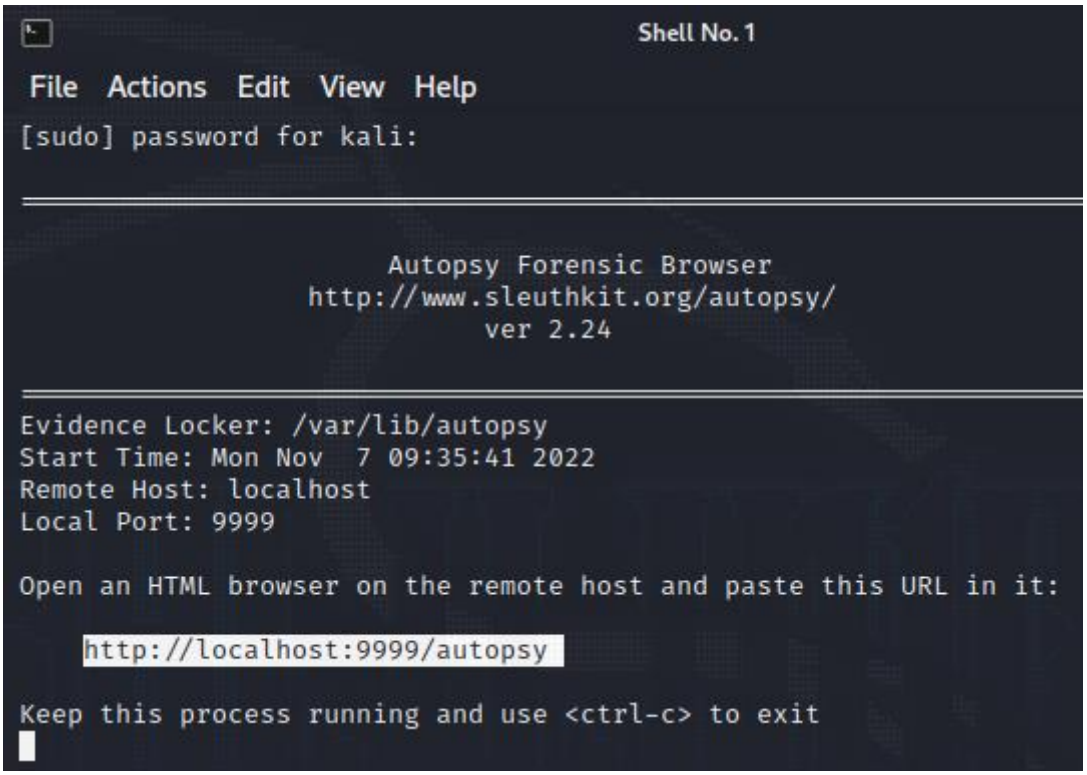
Chapter 12: Autopsy Forensic Browser

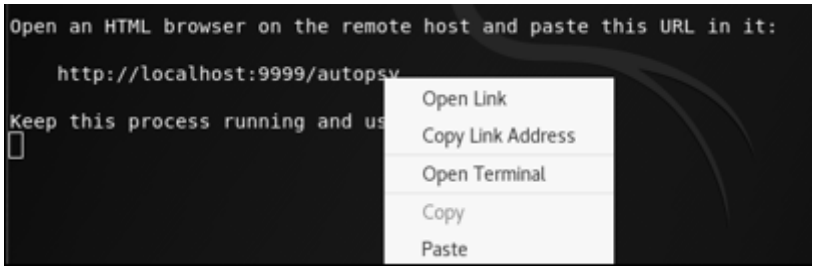
corpora/scenarios/2009-m57-patents/usb/ files:

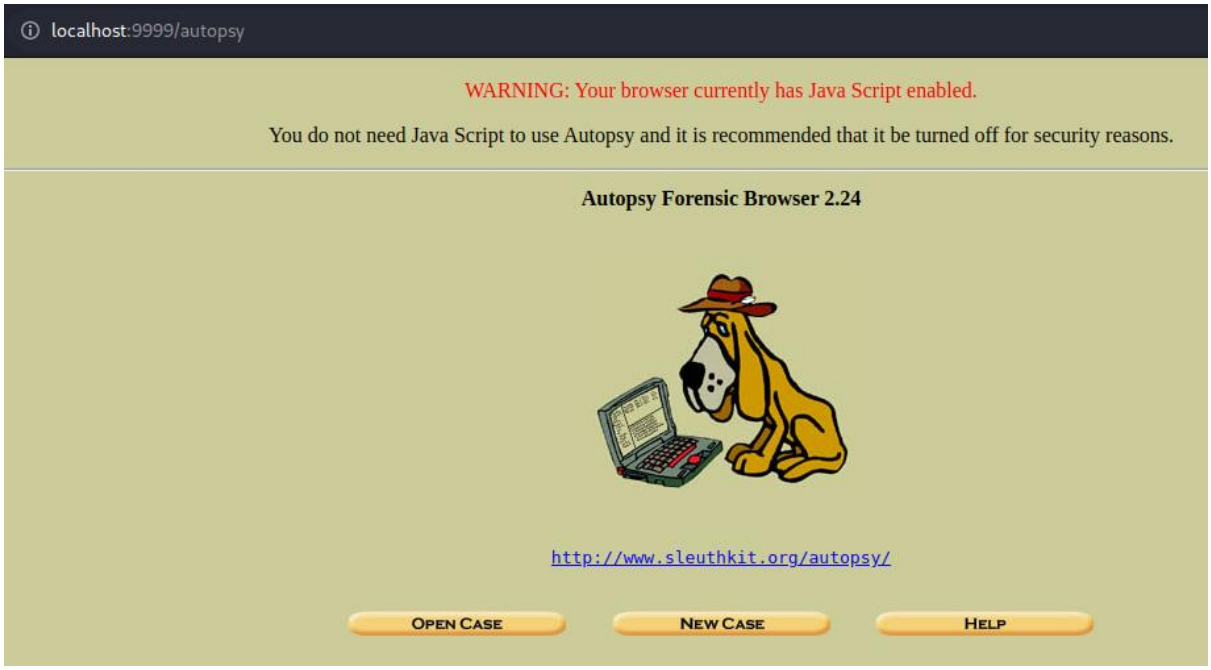
Name	Size	Last Modified	SHA2-256
charlie-work-usb-2009-12-11.E01	9,265,553	2020-11-22 09:40:13+00:00	7a998c556b22f5dc9426a33dcaceadd21a14c9cfb22957edce461d58a14fb40a
jo-favorites-usb-2009-12-11.E01	227,073,046	2020-11-22 09:40:15+00:00	1798e0436f99f2490dbf92f09fdf7956b0f2a6cf6cafde6a426094c9de6aec54
jo-work-usb-2009-12-11.E01	118,233,120	2020-11-22 09:40:39+00:00	d3751b55c1b88e1a5fb1940a9a41cc87e750b61e4aa59f9c76bd2f17e17c3cc2
terry-work-usb-2009-12-11.E01	33,499,203	2020-11-22 09:40:41+00:00	1600fe2bdfb2bec0b006aa9d1c0ce6d3ad0b6666141a333bf830af7800fb9230



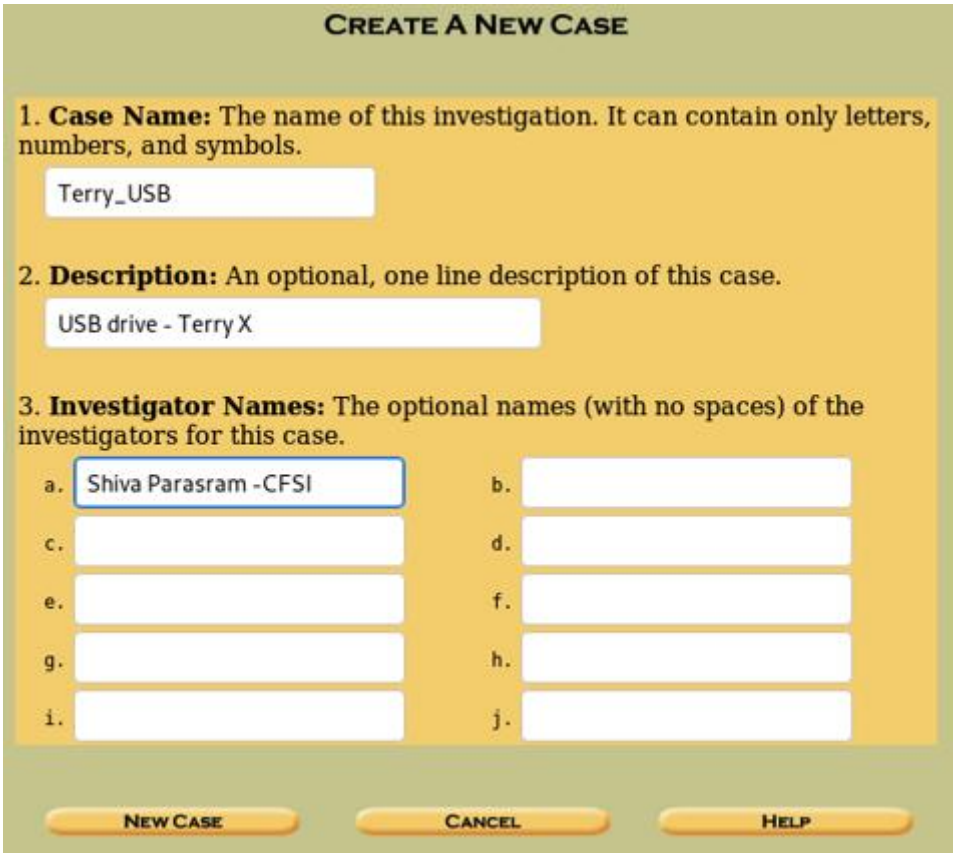

1
autopsy
autopsy (root)

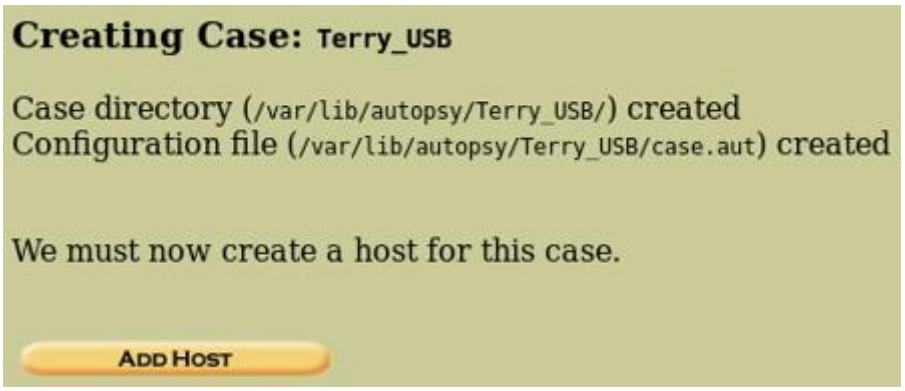

Shell No. 1
File Actions Edit View Help
[sudo] password for kali:
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24
Evidence Locker: /var/lib/autopsy
Start Time: Mon Nov 7 09:35:41 2022
Remote Host: localhost
Local Port: 9999
Open an HTML browser on the remote host and paste this URL in it:
http://localhost:9999/autopsy
Keep this process running and use <ctrl-c> to exit


Open an HTML browser on the remote host and paste this URL in it:
http://localhost:9999/autopsy
Keep this process running and us
Open Link
Copy Link Address
Open Terminal
Copy
Paste


localhost:9999/autopsy
WARNING: Your browser currently has Java Script enabled.
You do not need Java Script to use Autopsy and it is recommended that it be turned off for security reasons.
Autopsy Forensic Browser 2.24
http://www.sleuthkit.org/autopsy/
OPEN CASE
NEW CASE
HELP


http://www.sleuthkit.org/autopsy/
OPEN CASE
NEW CASE
HELP


CREATE A NEW CASE
1. Case Name: The name of this investigation. It can contain only letters, numbers, and symbols.
Terry_USB
2. Description: An optional, one line description of this case.
USB drive - Terry X
3. Investigator Names: The optional names (with no spaces) of the investigators for this case.
a. Shiva Parasram -CFSI
b.
c.
d.
e.
f.
g.
h.
i.
j.
NEW CASE
CANCEL
HELP


Creating Case: Terry_USB
Case directory (/var/lib/autopsy/Terry_USB/) created
Configuration file (/var/lib/autopsy/Terry_USB/case.aut) created
We must now create a host for this case.
ADD HOST

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

host1

2. **Description:** An optional one-line description or note about this computer.

Forensic_Analyzer_3

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

GMT-4

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

0

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of known good files.

ADD HOST CANCEL HELP

Adding host: `host1` to case `Terry_USB`

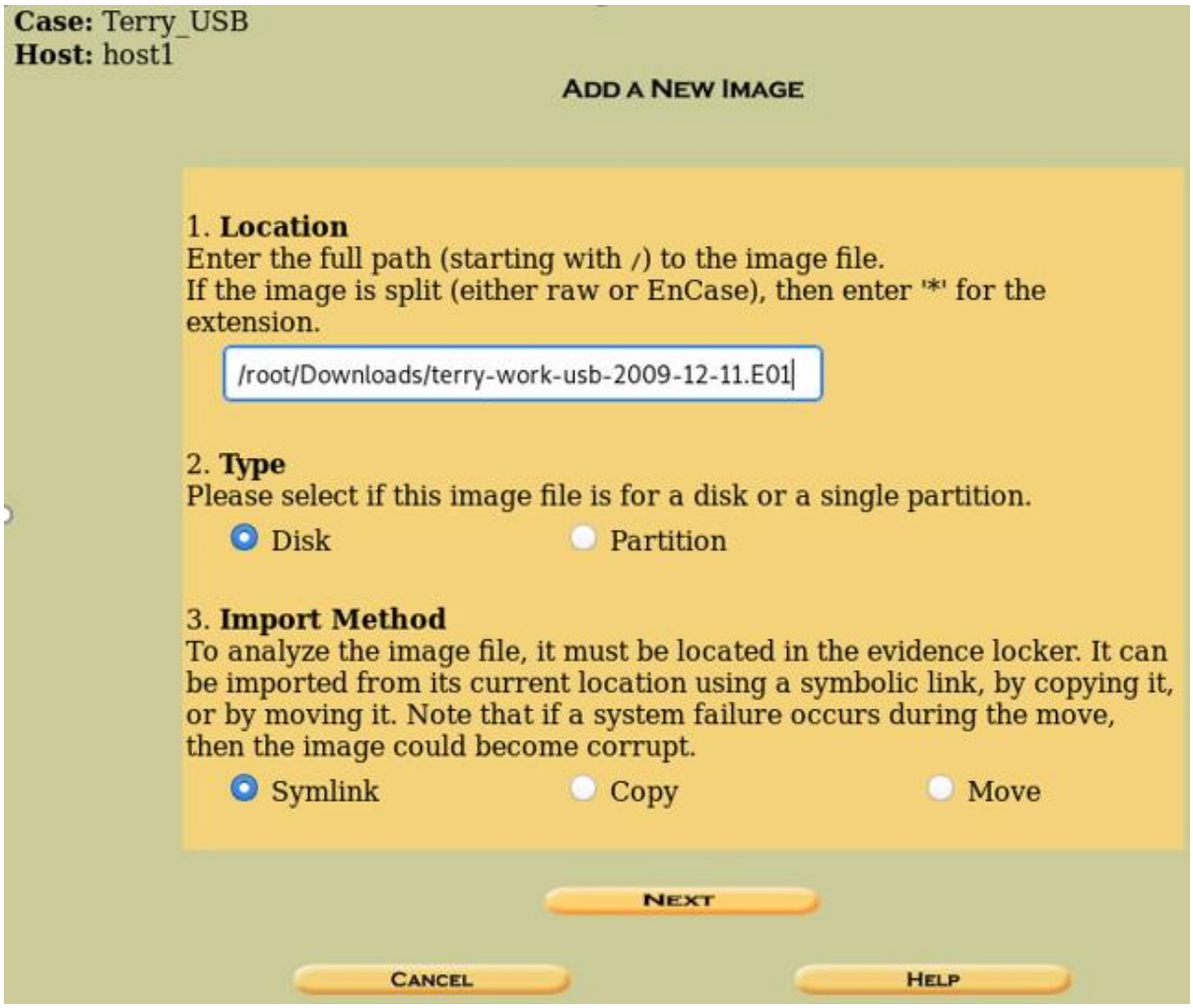
Host Directory (`/var/lib/autopsy/Terry_USB/host1/`) created

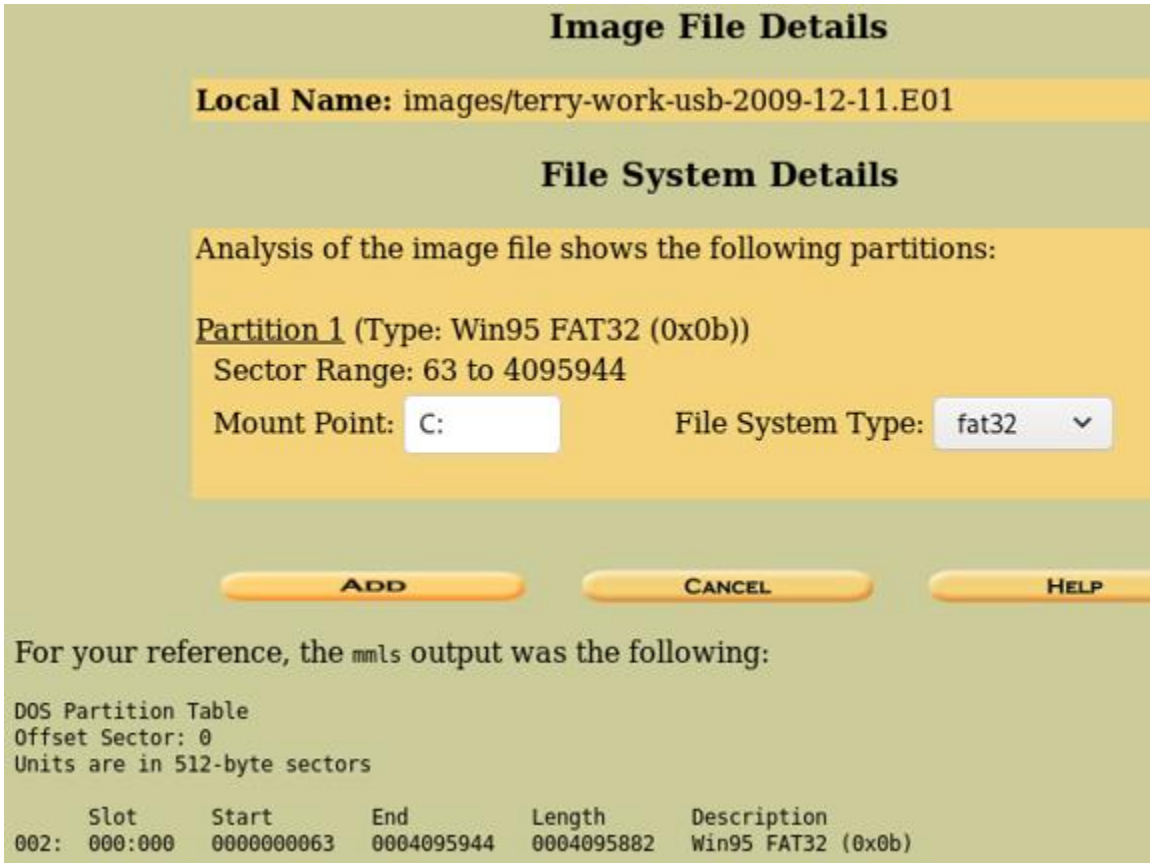
Configuration file (`/var/lib/autopsy/Terry_USB/host1/host.aut`) created

We must now import an image file for this host

ADD IMAGE

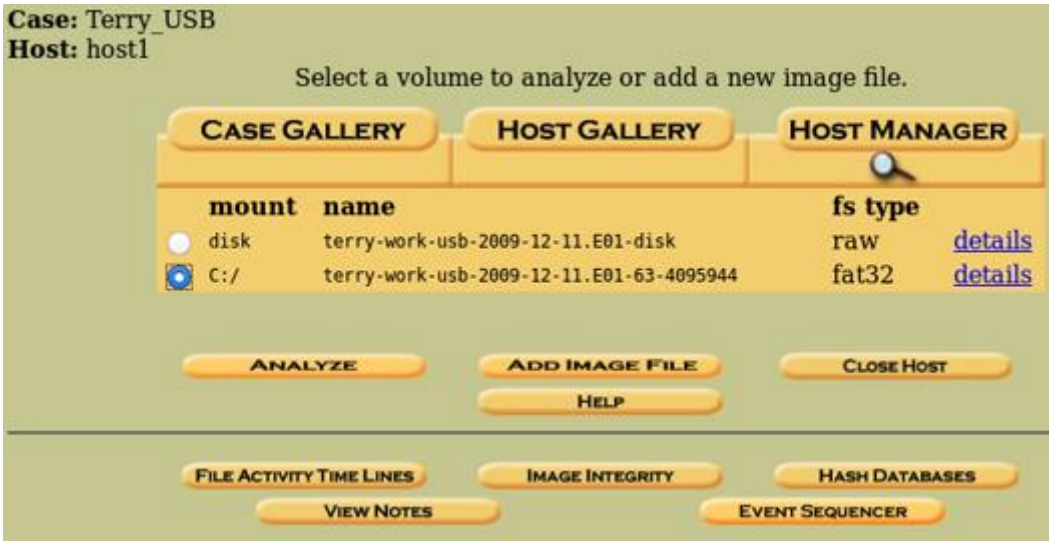

Case: Terry_USB
Host: host1
No images have been added to this host yet
Select the Add Image File button below to add one
ADD IMAGE FILE
CLOSE HOST
HELP
FILE ACTIVITY TIME LINES
IMAGE INTEGRITY
HASH DATABASES
VIEW NOTES
EVENT SEQUENCER

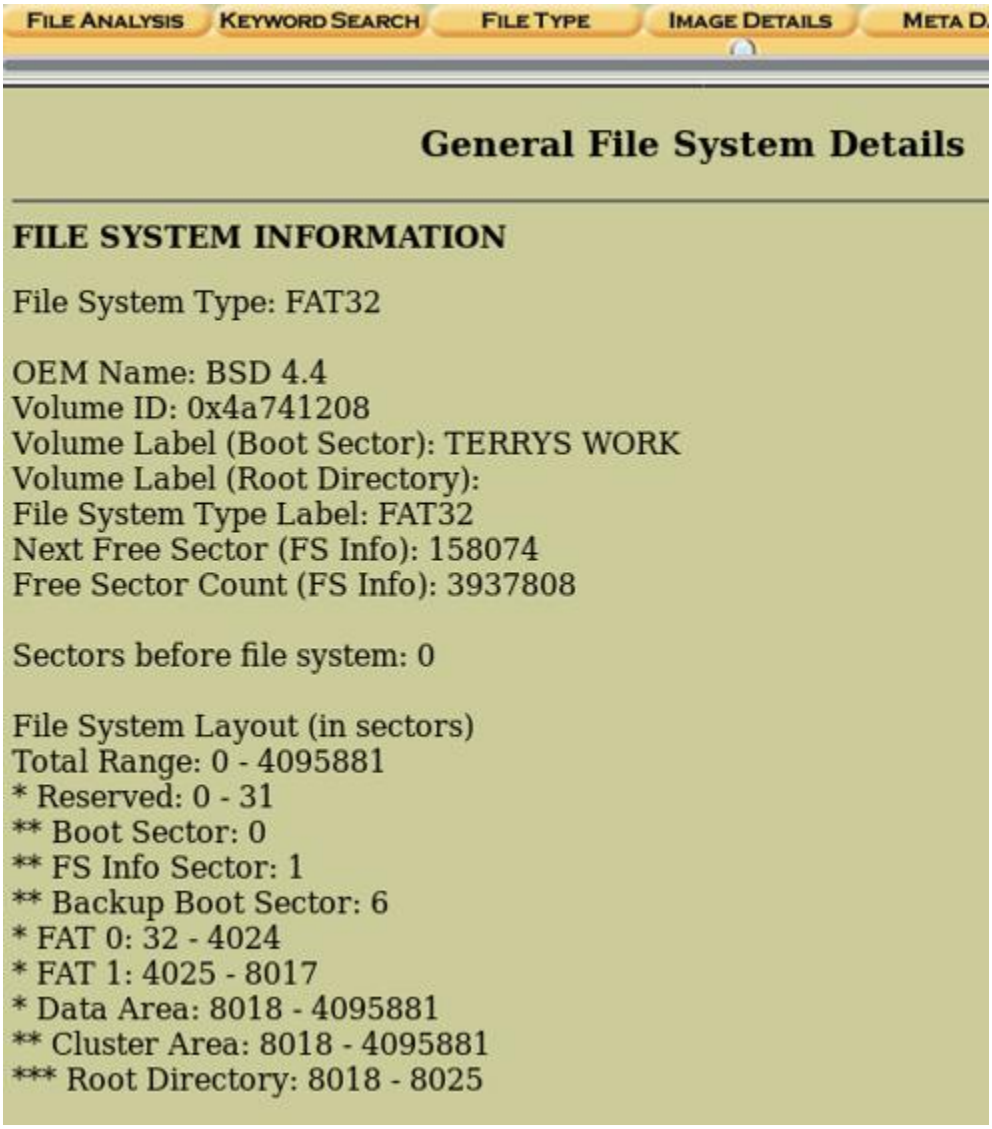

Case: Terry_USB
Host: host1
ADD A NEW IMAGE
1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.
/root/Downloads/terry-work-usb-2009-12-11.E01
2. Type
Please select if this image file is for a disk or a single partition.
Disk
Partition
3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.
Symlink
Copy
Move
NEXT
CANCEL
HELP



For your reference, the `mmls` output was the following:

```
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
002:  000:000   0000000063   0004095944   0004095882   Win95 FAT32 (0x0b)
```




FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META D
General File System Details
FILE SYSTEM INFORMATION
File System Type: FAT32
OEM Name: BSD 4.4
Volume ID: 0x4a741208
Volume Label (Boot Sector): TERRYS WORK
Volume Label (Root Directory):
File System Type Label: FAT32
Next Free Sector (FS Info): 158074
Free Sector Count (FS Info): 3937808
Sectors before file system: 0
File System Layout (in sectors)
Total Range: 0 - 4095881
* Reserved: 0 - 31
** Boot Sector: 0
** FS Info Sector: 1
** Backup Boot Sector: 6
* FAT 0: 32 - 4024
* FAT 1: 4025 - 8017
* Data Area: 8018 - 4095881
** Cluster Area: 8018 - 4095881
*** Root Directory: 8018 - 8025


FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
DEL
Type
dir / in
NAME
WRITTEN
ACCESSED
CREATED
SIZE
UID
GID
META
Error Parsing File (Invalid Characters?):
V/V 65405830: $OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0
v / v $FAT1 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 2044416 0 0 65405828
v / v $FAT2 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 2044416 0 0 65405829
v / v $MBR 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 512 0 0 65405827
r / r ._.Trashes 2009-11-17 10:47:46 (GMT) 2009-11-17 00:00:00 (GMT) 2009-11-17 10:47:47 (GMT) 4096 0 0 5
r / r ._MS7biz.jpg 2009-11-17 10:49:24 (GMT) 2009-11-17 00:00:00 (GMT) 2009-11-17 10:49:25 (GMT) 4096 0 0 17
r / r ._patentauto.py 2009-11-17 13:47:18 (GMT) 2009-11-17 00:00:00 (GMT) 2009-11-17 13:47:19 (GMT) 4096 0 0 54

✓	d / d	.fseventsd/	2009-11-17 10:48:38 (GMT)	2009-11-17 00:00:00 (GMT)	2009-11-17 10:48:38 (GMT)	0	0	0	10
	d / d	.Spotlight-V100/	2009-11-17 10:47:46 (GMT)	2009-11-17 00:00:00 (GMT)	2009-11-17 10:47:47 (GMT)	4096	0	0	13
	d / d	.Trashes/	2009-11-17 10:47:46 (GMT)	2009-11-17 00:00:00 (GMT)	2009-11-17 10:47:47 (GMT)	4096	0	0	8
✓	d / d	_078421_/	2009-11-20 10:59:48 (GMT)	2009-11-20 00:00:00 (GMT)	2009-11-20 10:59:47 (GMT)	0	0	0	65
✓	d / d	_189812_/	2009-11-20 11:33:04 (GMT)	2009-11-20 00:00:00 (GMT)	2009-11-20 11:33:03 (GMT)	0	0	0	67
✓	d / d	_452781_/	2009-11-20 11:06:04 (GMT)	2009-11-20 00:00:00 (GMT)	2009-11-20 11:06:02 (GMT)	0	0	0	66
✓	d / d	_461531_/	2009-11-20 10:49:32 (GMT)	2009-11-20 00:00:00 (GMT)	2009-11-20 10:49:30 (GMT)	0	0	0	63
✓	r / r	_54402.EXE	2009-11-20 10:31:36 (GMT)	2009-11-20 00:00:00 (GMT)	2009-11-20 10:31:34 (GMT)	0	0	0	61
✓	d / d	_604468_/	2009-11-20 10:51:54 (GMT)	2009-11-20 00:00:00 (GMT)	2009-11-20 10:51:53 (GMT)	0	0	0	64
	d / d	Log/	2009-12-07	2009-12-07	2009-12-07	643072	0	0	72

r / r	urlstime_machine.txt	2009-11-16 10:22:50 (GMT)	2009-11-24 00:00:00 (GMT)	2009-11-16 10:22:51 (GMT)	1538990	0	0	20
r / r	vnc-4_1_3-x86_win32.exe	2008-10-15 17:14:08 (GMT)	2009-12-07 00:00:00 (GMT)	2008-10-15 17:14:08 (GMT)	741744	0	0	75
r / r	webauto.py	2009-11-16 14:23:38 (GMT)	2009-11-24 00:00:00 (GMT)	2009-11-14 17:39:19 (GMT)	2237	0	0	6
r / r	xpadvancedkeylogger.exe	2009-12-03 09:40:44 (GMT)	2009-12-07 00:00:00 (GMT)	2009-12-03 09:41:16 (GMT)	1580660	0	0	70

Directory Seek

Enter the name of a directory that you want to view.

C:/

VIEW

File Name Search

Enter a Perl regular expression for the file names you want to find.

SEARCH

ALL DELETED FILES

EXPAND DIRECTORIES

Directory Seek

Enter the name of a directory that you want to view.
C:/

VIEW

File Name Search

Enter a Perl regular expression for the file names you want to find.

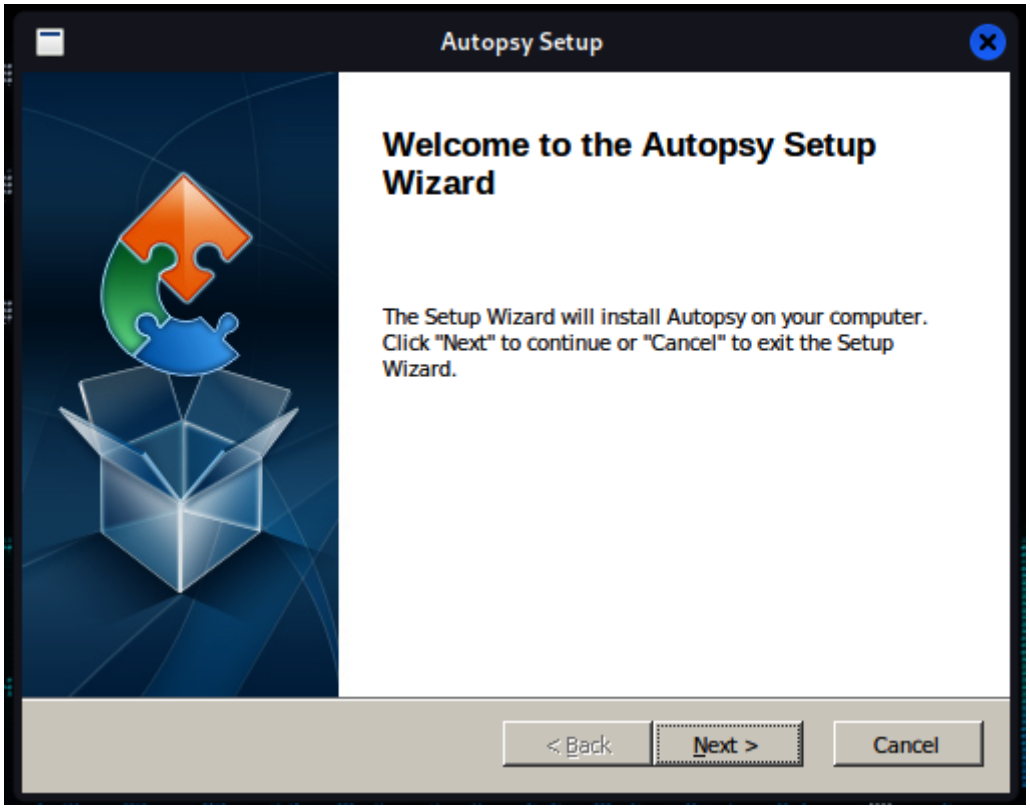
SEARCH

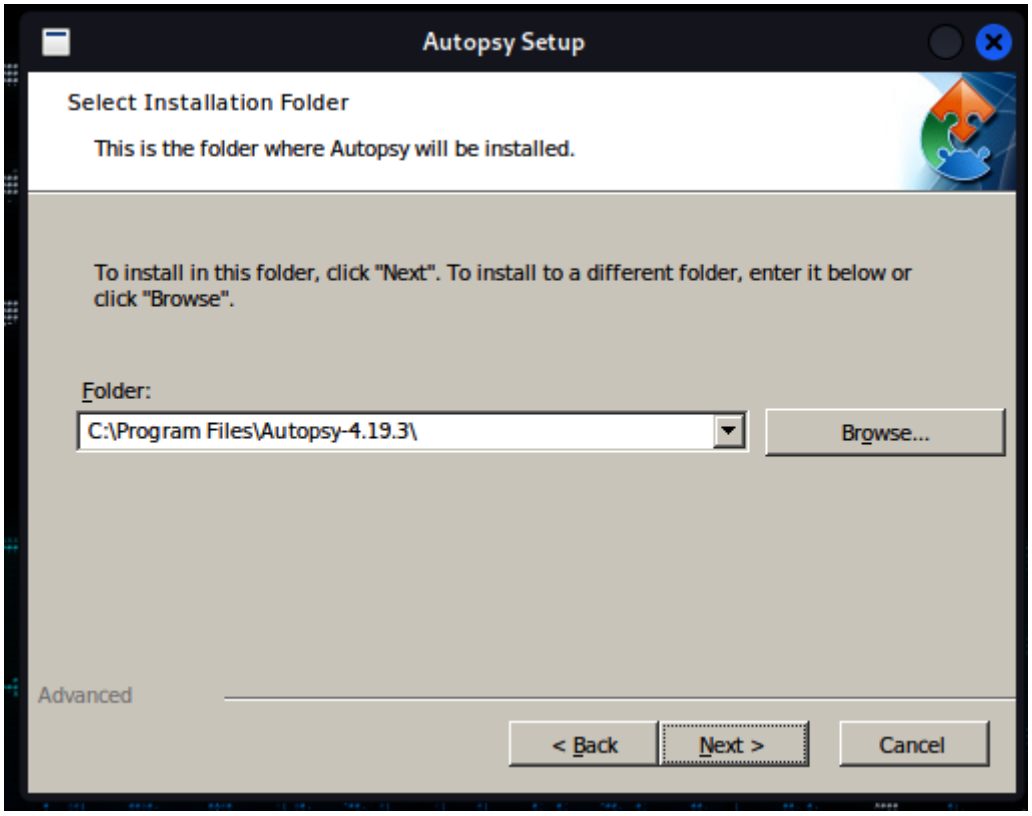
ALL DELETED FILES

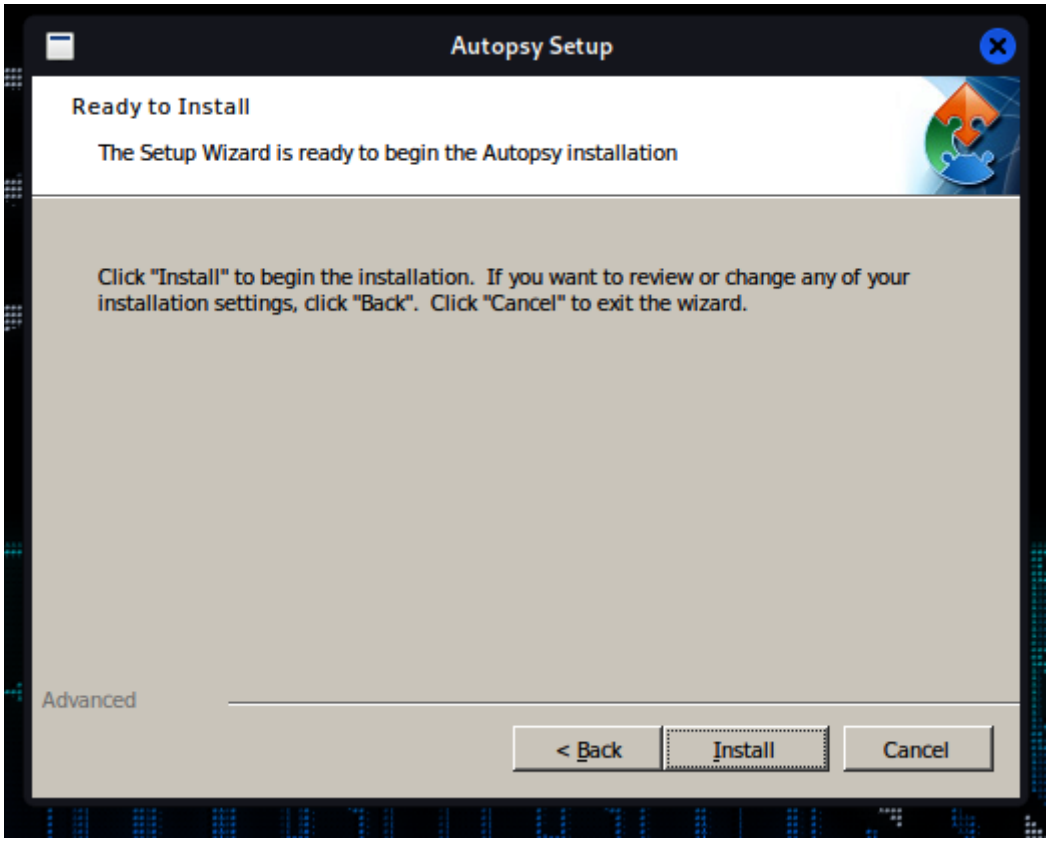
EXPAND DIRECTORIES

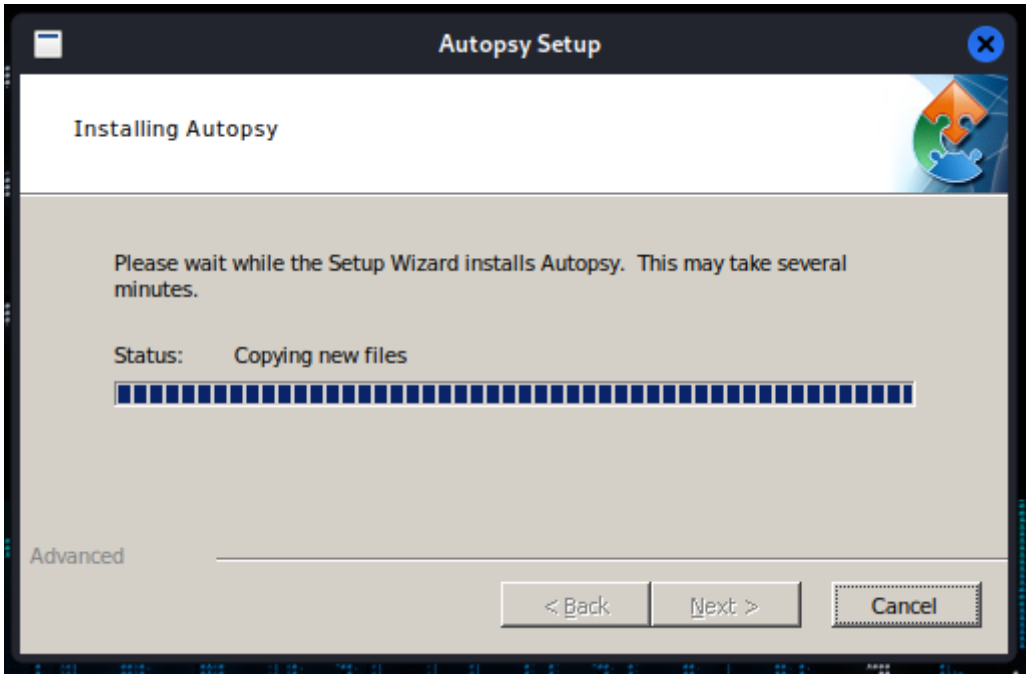
	/tmp.0.cmpt.indexCompactDirectory					
r / r	C:/.Spotlight-V100/Store-V1/Stores/7680DE76-88D9-43B3-AC7E-3B02E7F38194 /tmp.0.cmpt.indexArrays	2009-11-17 13:35:14 (GMT)	2009-11-17 00:00:00 (GMT)	2009-11-17 13:35:14 (GMT)	66800	0
r / r	C:/.Spotlight-V100/Store-V1/Stores/7680DE76-88D9-43B3-AC7E-3B02E7F38194 /tmp.0.cmpt.newTermIDMap	2009-11-17 13:35:14 (GMT)	2009-11-17 00:00:00 (GMT)	2009-11-17 13:35:14 (GMT)	360	0
r / r	C:/.Spotlight-V100/Store-V1/Stores/7680DE76-88D9-43B3-AC7E-3B02E7F38194 /tmp.0.cmpt.compactPayloads1.idx	2009-11-17 13:35:14 (GMT)	2009-11-17 00:00:00 (GMT)	2009-11-17 13:35:14 (GMT)	0	0
r / r	C:/.Spotlight-V100/Store-V1/Stores/7680DE76-88D9-43B3-AC7E-3B02E7F38194 /tmp.0.cmpt.compactPayloads2.idx	2009-11-17 13:35:14 (GMT)	2009-11-17 00:00:00 (GMT)	2009-11-17 13:35:14 (GMT)	0	0
r / r	C:/_54402.EXE	2009-11-20 10:31:36 (GMT)	2009-11-20 00:00:00 (GMT)	2009-11-20 10:31:34 (GMT)	0	0
d / d	C:/_461531_	2009-11-20 10:49:32 (GMT)	2009-11-20 00:00:00 (GMT)	2009-11-20 10:49:30 (GMT)	0	0
d / d	C:/_604468_	2009-11-20 10:51:54 (GMT)	2009-11-20 00:00:00 (GMT)	2009-11-20 10:51:53 (GMT)	0	0
d / d	C:/_078421_	2009-11-20 10:59:48 (GMT)	2009-11-20 00:00:00 (GMT)	2009-11-20 10:59:47 (GMT)	0	0
d / d	C:/_452781_	2009-11-20 11:06:04 (GMT)	2009-11-20 00:00:00 (GMT)	2009-11-20 11:06:02 (GMT)	0	0
d / d	C:/_189812_	2009-11-20 11:33:04 (GMT)	2009-11-20 00:00:00 (GMT)	2009-11-20 11:33:03 (GMT)	0	0
r / r	C:/xpadvancedkeylogger.exe	2009-12-03	2009-12-07	2009-12-03	1580660	0

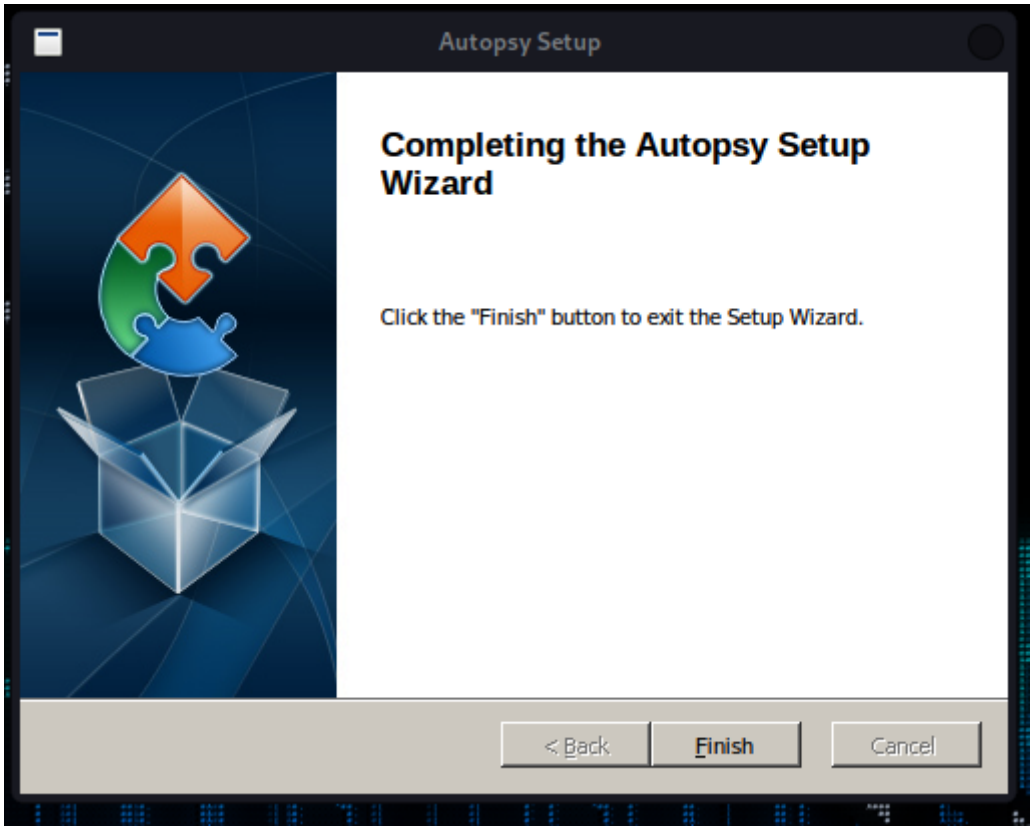
Chapter 13: Performing a Full DFIR Analysis with the Autopsy 4 GUI

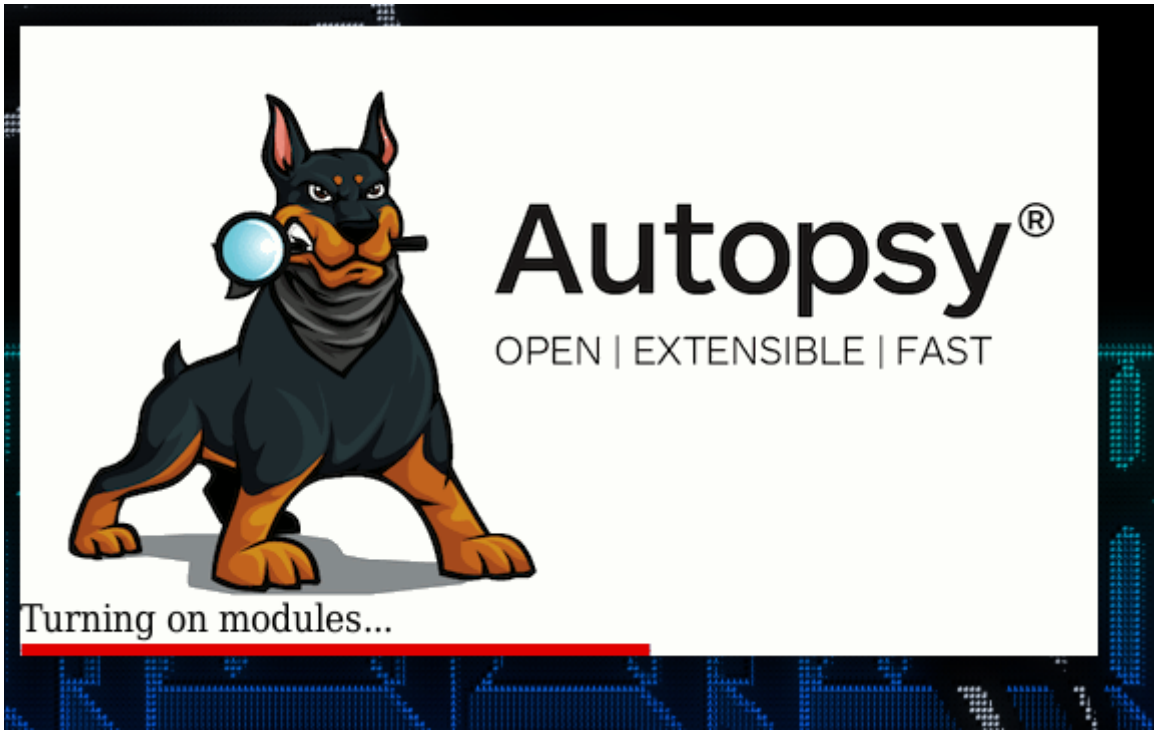


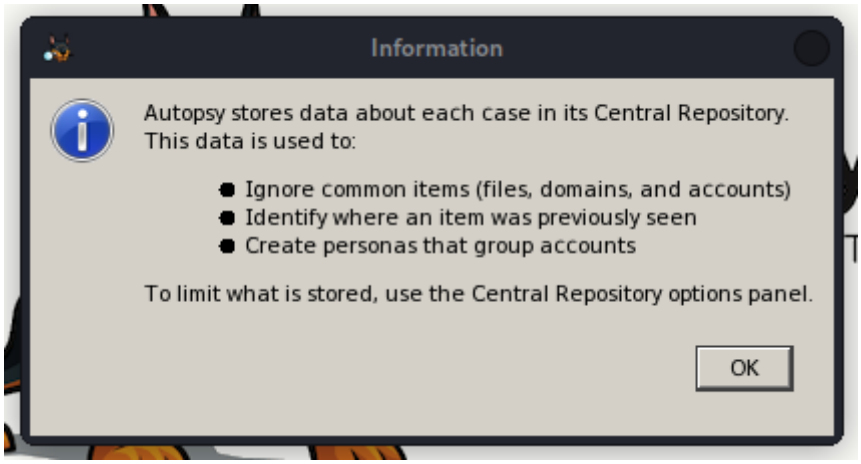

Autopsy Setup
Select Installation Folder
This is the folder where Autopsy will be installed.
To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".
Folder:
C:\Program Files\Autopsy-4.19.3\
Browse...
Advanced
< Back
Next >
Cancel


Autopsy Setup
Ready to Install
The Setup Wizard is ready to begin the Autopsy installation
Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.
Advanced
< Back
Install
Cancel

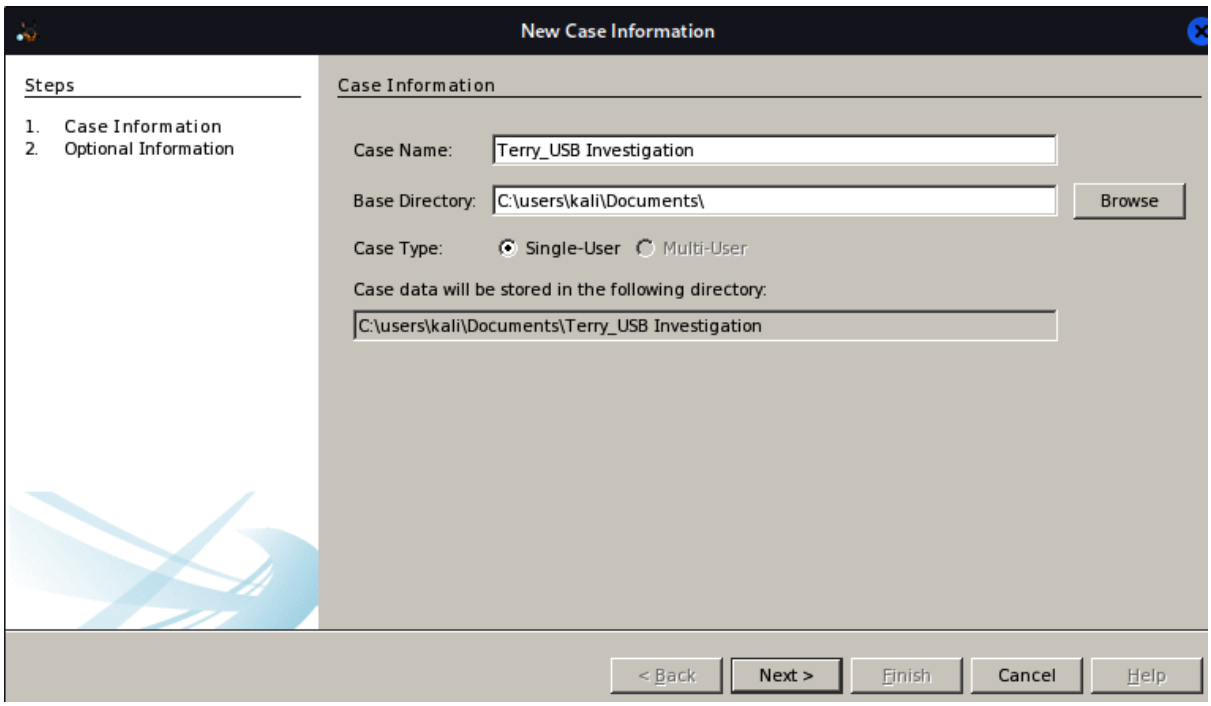

Autopsy Setup
Installing Autopsy
Please wait while the Setup Wizard installs Autopsy. This may take several minutes.
Status: Copying new files
Advanced
< Back
Next >
Cancel

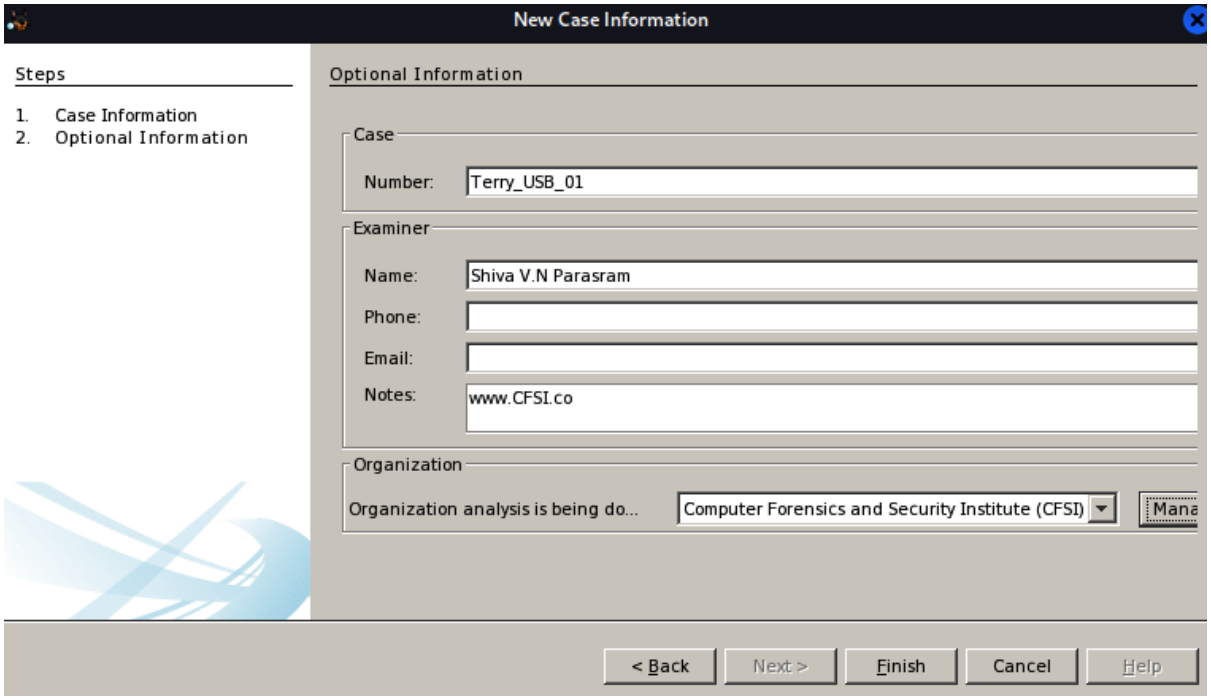

Autopsy Setup
Completing the Autopsy Setup Wizard
Click the "Finish" button to exit the Setup Wizard.
< Back
Finish
Cancel

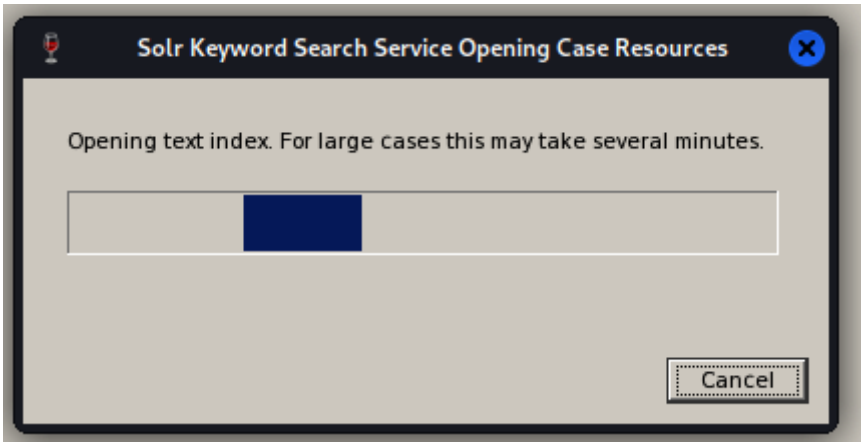

Autopsy®
OPEN | EXTENSIBLE | FAST
Turning on modules...

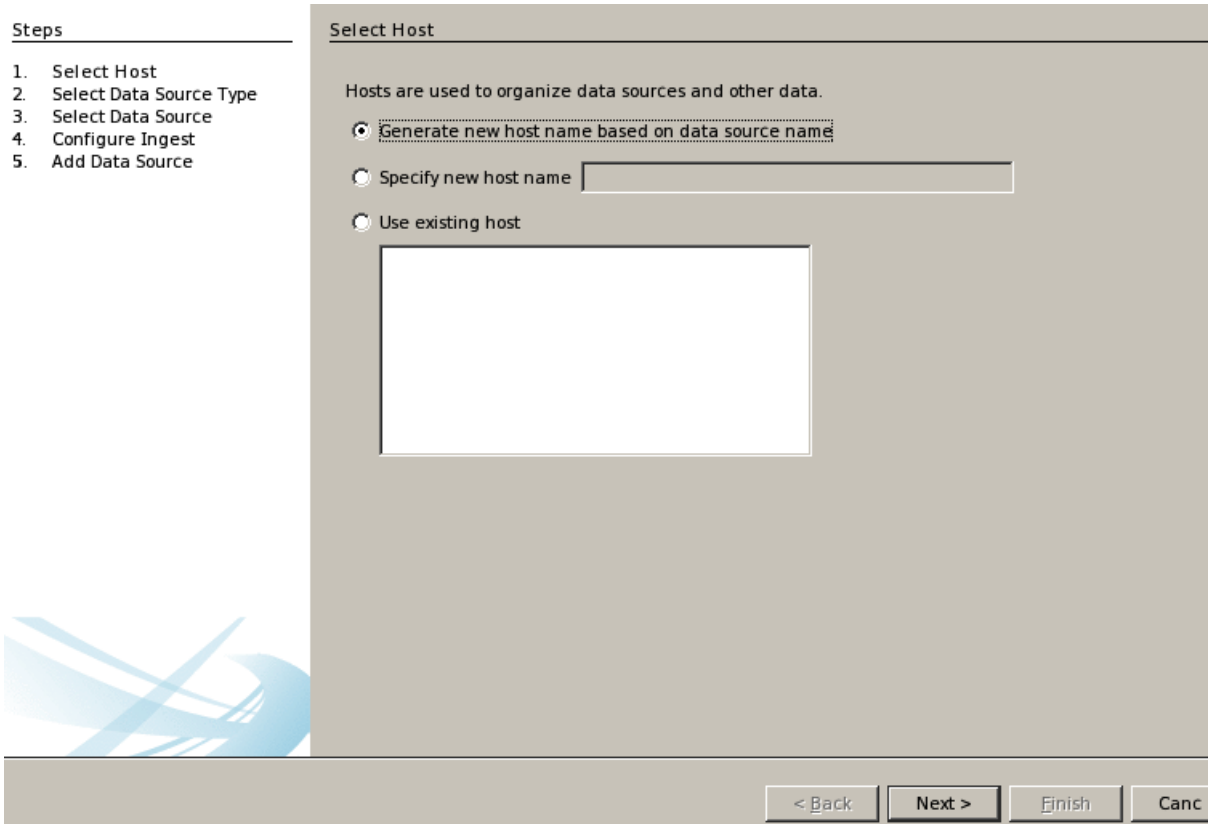

Information
Autopsy stores data about each case in its Central Repository.
This data is used to:
Ignore common items (files, domains, and accounts)
Identify where an item was previously seen
Create personas that group accounts
To limit what is stored, use the Central Repository options panel.
OK

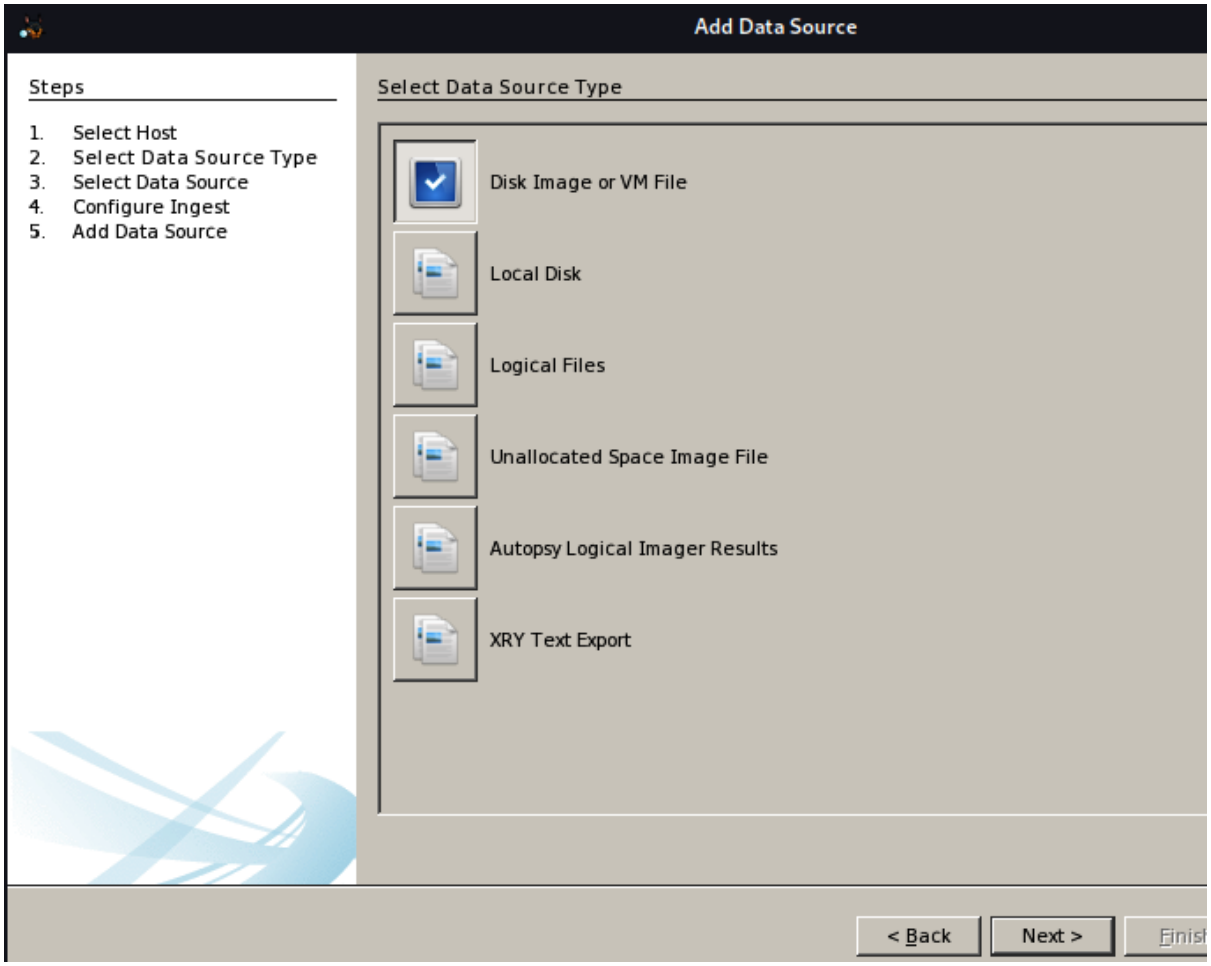

Autopsy 4.19.3
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Keyword Lists
Keyword Search
Welcome
New Case
Open Recent Case
Open Case
Autopsy®
OPEN | EXTENSIBLE | FAST
Close

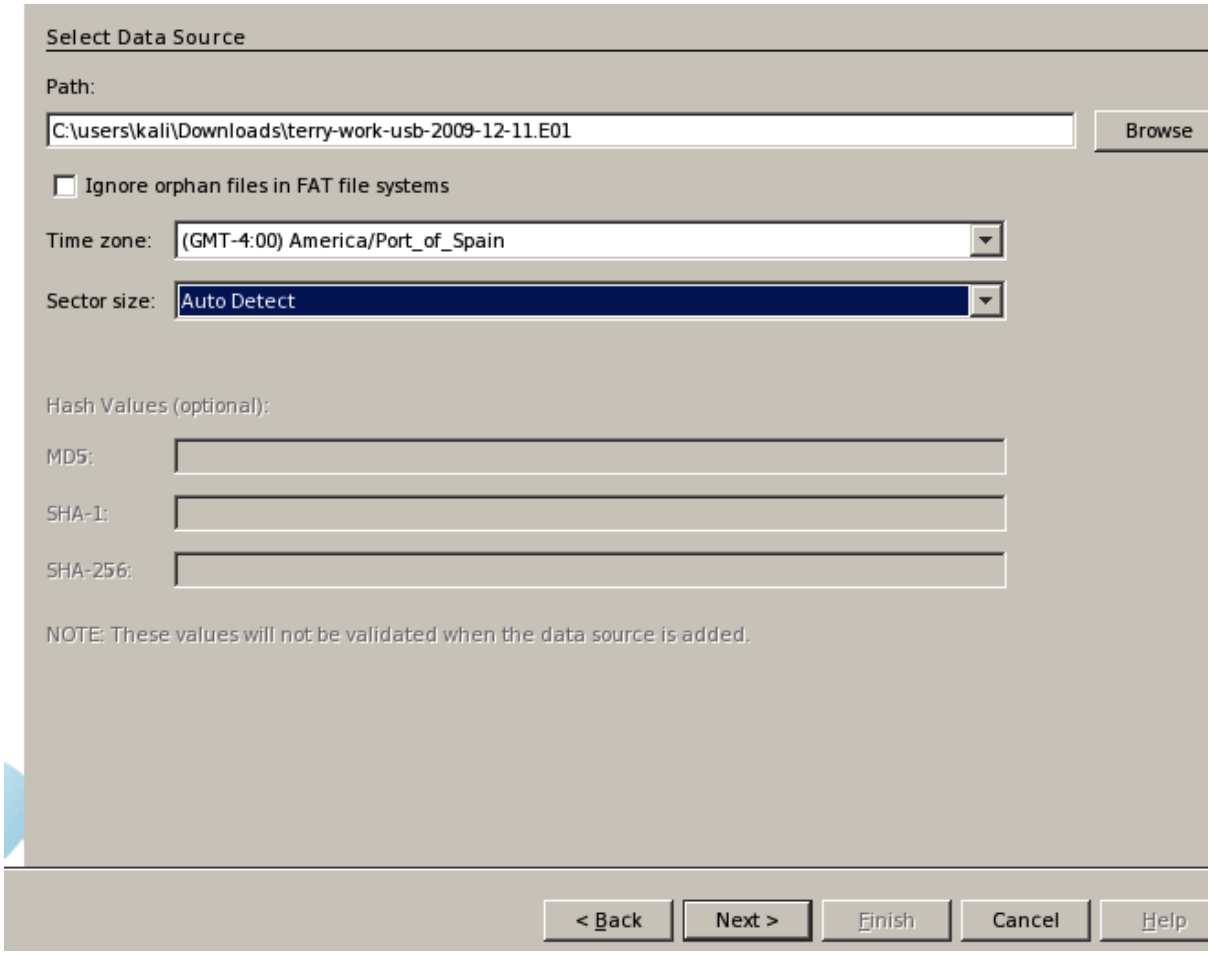

New Case Information
Steps
1. Case Information
2. Optional Information
Case Information
Case Name: Terry_USB Investigation
Base Directory: C:\users\kali\Documents\
Browse
Case Type: Single-User Multi-User
Case data will be stored in the following directory:
C:\users\kali\Documents\Terry_USB Investigation
< Back
Next >
Finish
Cancel
Help

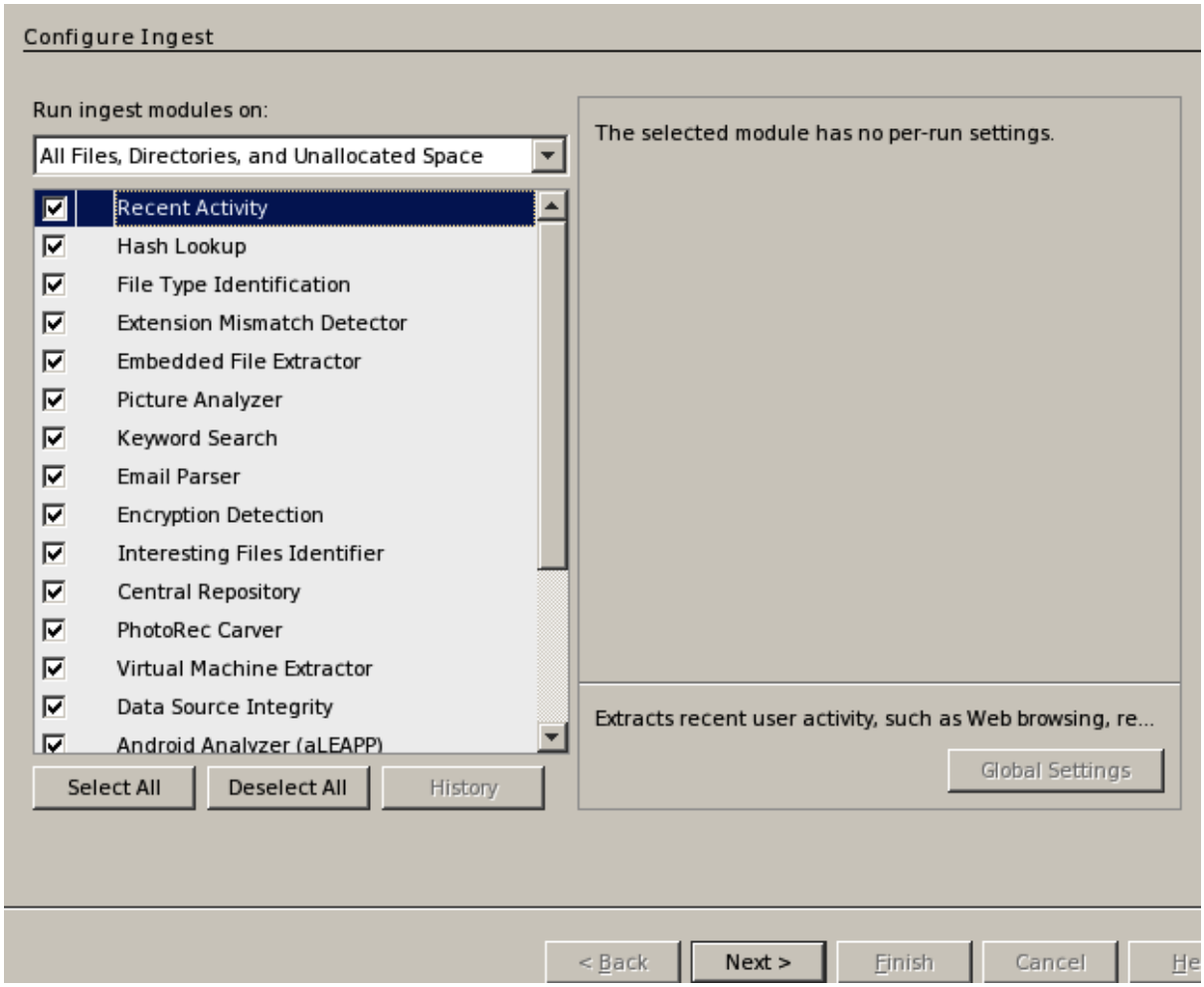

New Case Information
Steps
1. Case Information
2. Optional Information
Optional Information
Case
Number: Terry_USB_01
Examiner
Name: Shiva V.N Parasram
Phone:
Email:
Notes: www.CFSI.co
Organization
Organization analysis is being do...
Computer Forensics and Security Institute (CFSI)
Mana
< Back
Next >
Finish
Cancel
Help

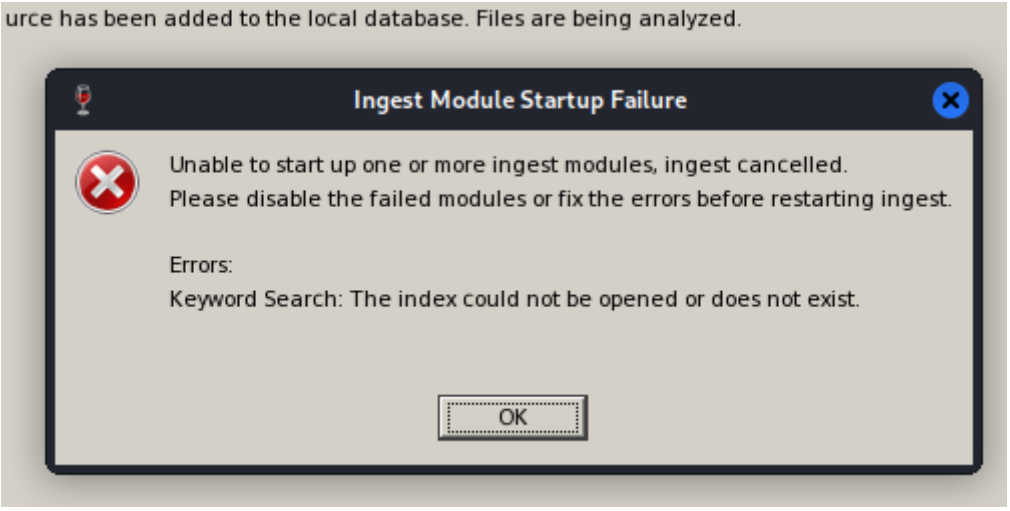

Solr Keyword Search Service Opening Case Resources
Opening text index. For large cases this may take several minutes.
Cancel

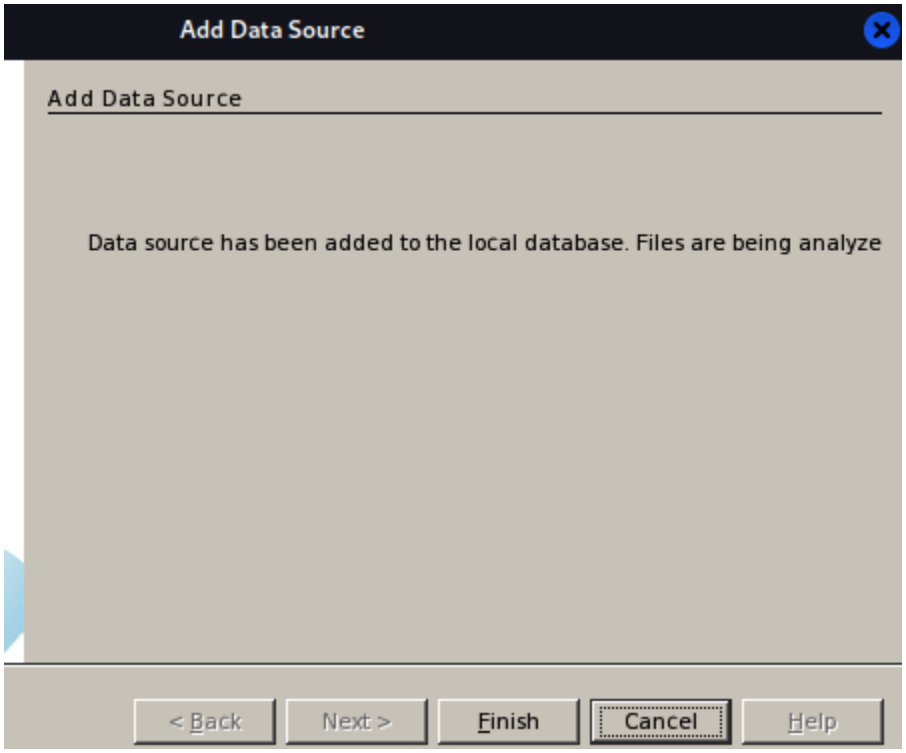

Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Host
Hosts are used to organize data sources and other data.
Generate new host name based on data source name
Specify new host name
Use existing host
< Back
Next >
Finish
Canc

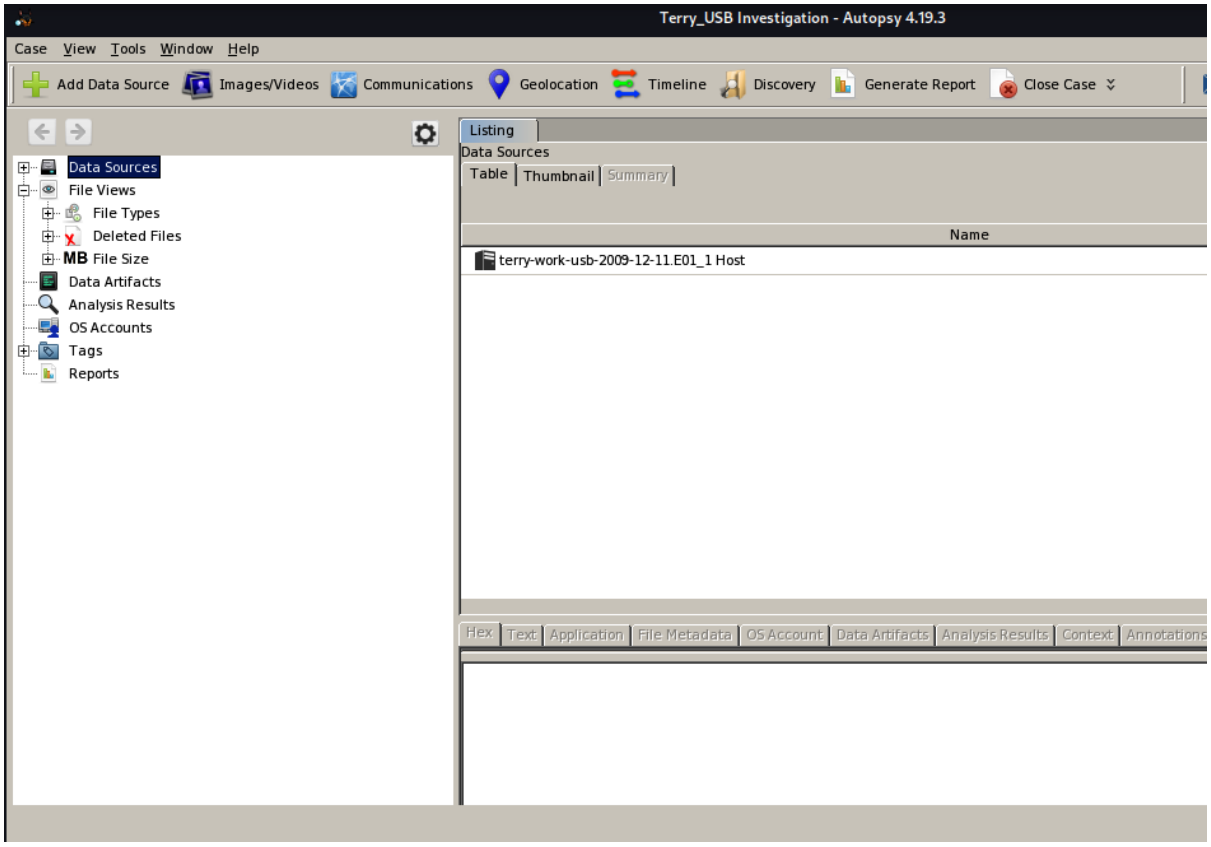

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source Type
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
< Back
Next >

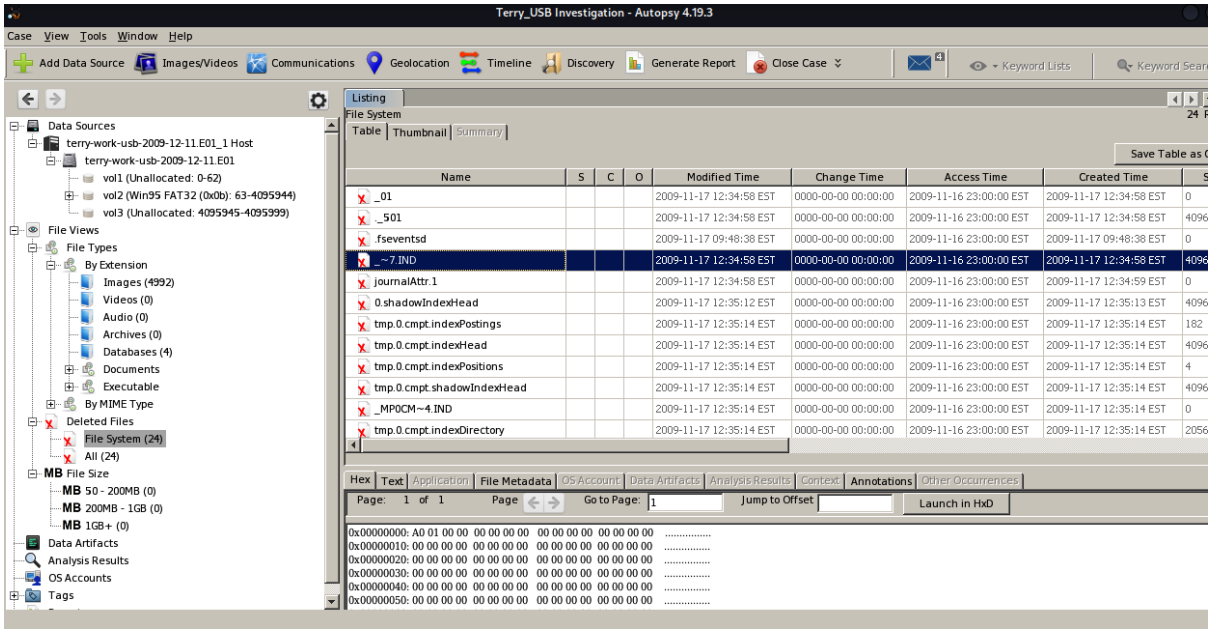

Select Data Source
Path:
C:\users\kali\Downloads\terry-work-usb-2009-12-11.E01
Browse
Ignore orphan files in FAT file systems
Time zone:
(GMT-4:00) America/Port_of_Spain
Sector size:
Auto Detect
Hash Values (optional):
MD5:
SHA-1:
SHA-256:
NOTE: These values will not be validated when the data source is added.
< Back
Next >
Finish
Cancel
Help

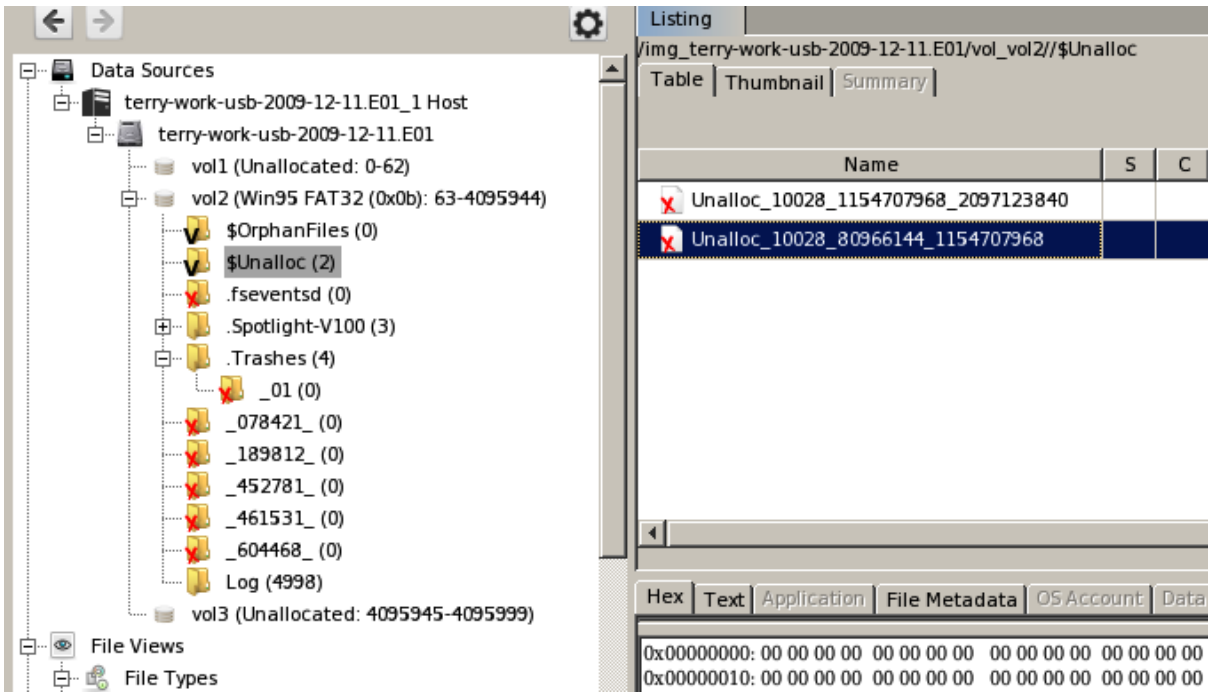

Configure Ingest
Run ingest modules on:
All Files, Directories, and Unallocated Space
Recent Activity
Hash Lookup
File Type Identification
Extension Mismatch Detector
Embedded File Extractor
Picture Analyzer
Keyword Search
Email Parser
Encryption Detection
Interesting Files Identifier
Central Repository
PhotoRec Carver
Virtual Machine Extractor
Data Source Integrity
Android Analyzer (aLEAPP)
Select All
Deselect All
History
The selected module has no per-run settings.
Extracts recent user activity, such as Web browsing, re...
Global Settings
< Back
Next >
Finish
Cancel

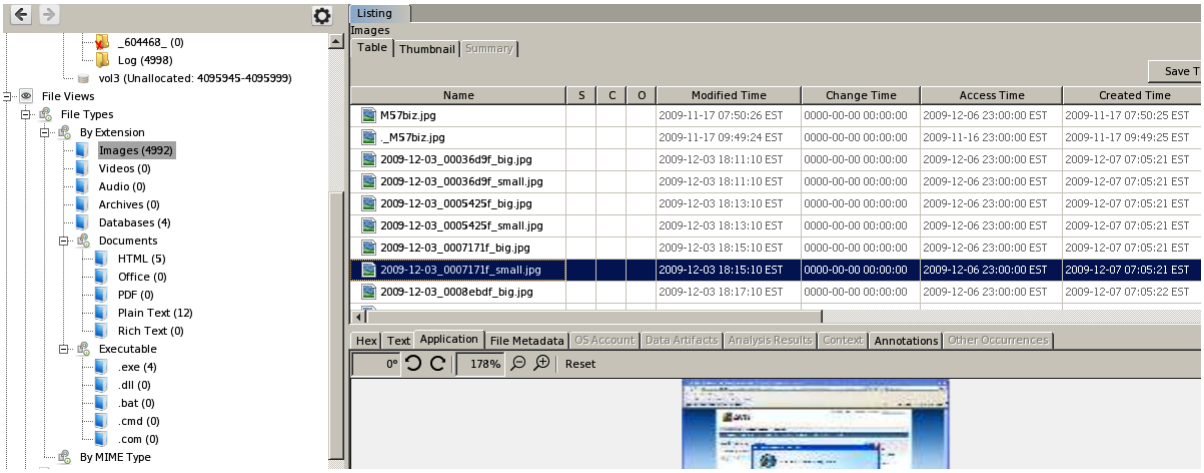

urce has been added to the local database. Files are being analyzed.
Ingest Module Startup Failure
Unable to start up one or more ingest modules, ingest cancelled.
Please disable the failed modules or fix the errors before restarting ingest.
Errors:
Keyword Search: The index could not be opened or does not exist.
OK

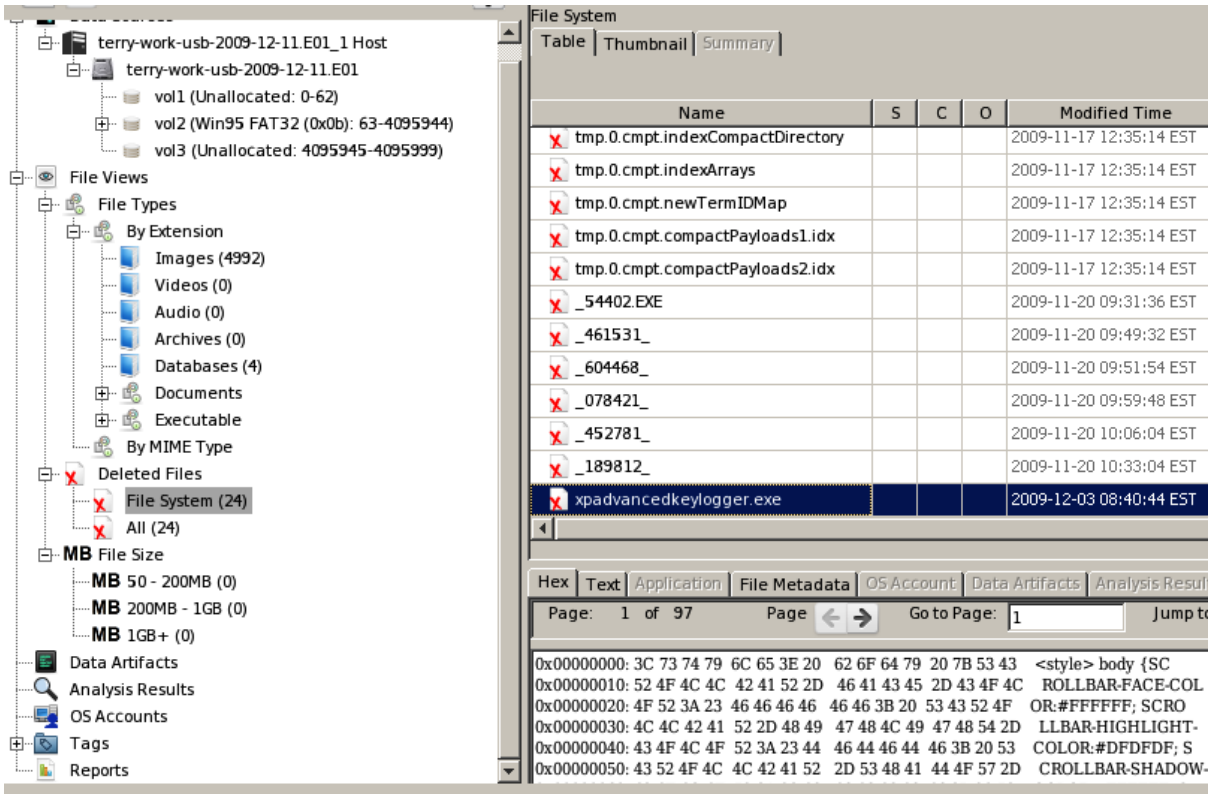

Add Data Source
Add Data Source
Data source has been added to the local database. Files are being analyze
< Back
Next >
Finish
Cancel
Help

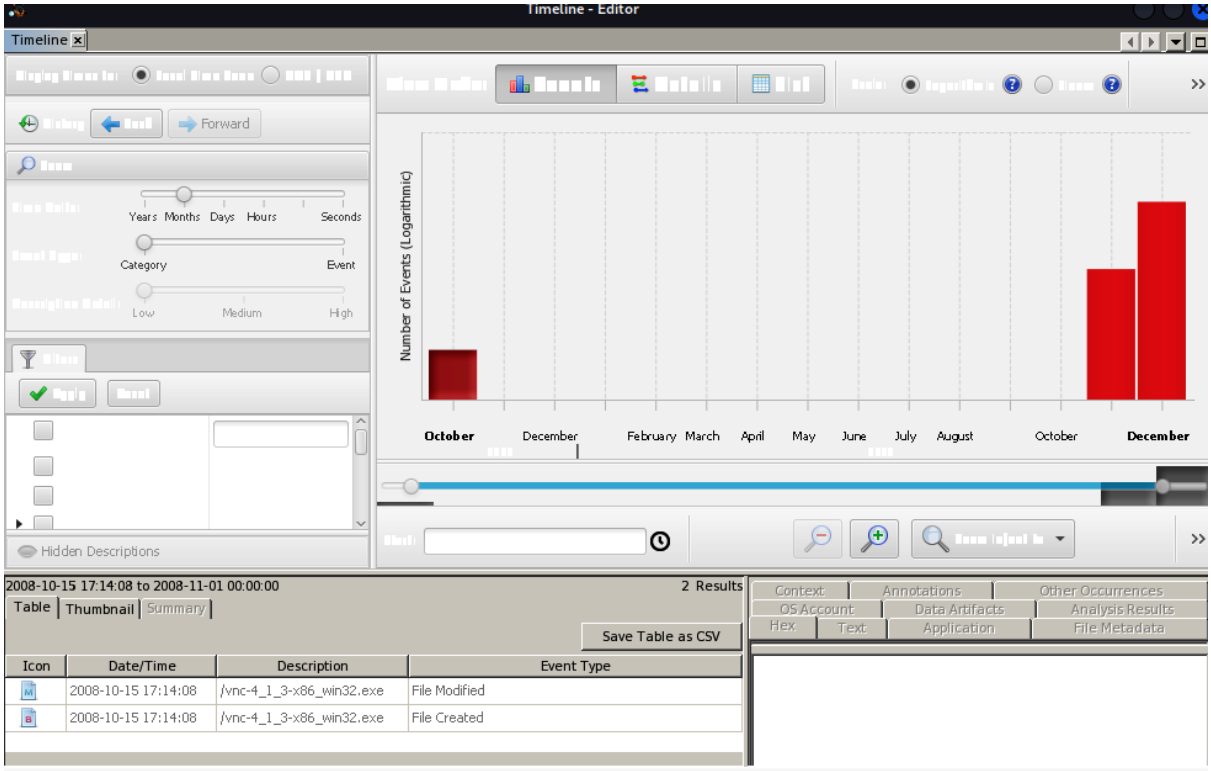

Terry_USB Investigation - Autopsy 4.19.3
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Data Sources
File Views
File Types
Deleted Files
MB File Size
Data Artifacts
Analysis Results
OS Accounts
Tags
Reports
Listing
Data Sources
Table
Thumbnail
Summary
Name
terry-work-usb-2009-12-11.E01_1 Host
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations

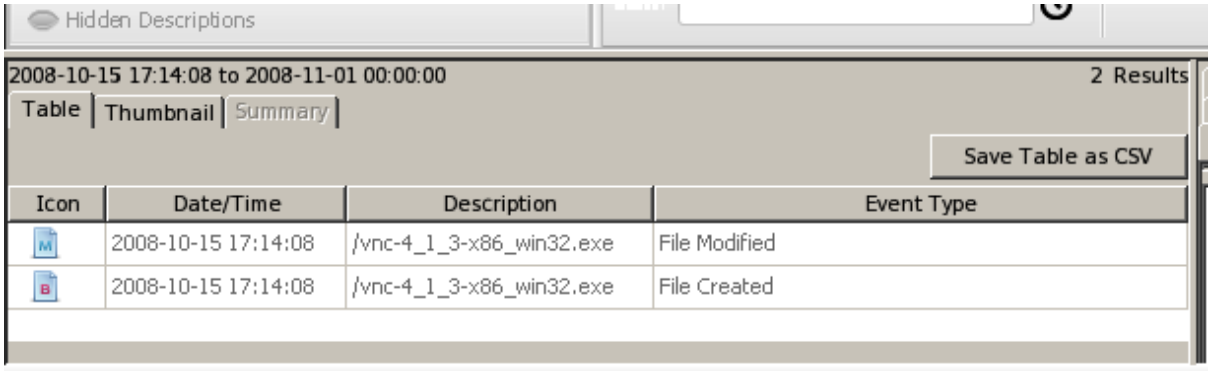

Terry_USB Investigation - Autopsy 4.19.3
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Data Sources
terry-work-usb-2009-12-11.E01_1 Host
terry-work-usb-2009-12-11.E01
vol1 (Unallocated: 0-62)
vol2 (Win95 FAT32 (0x0b): 63-4095944)
vol3 (Unallocated: 4095945-4095999)
File Views
File Types
By Extension
Images (4992)
Videos (0)
Audio (0)
Archives (0)
Databases (4)
Documents
Executable
By MIME Type
Deleted Files
File System (24)
All (24)
MB File Size
MB 50 - 200MB (0)
MB 200MB - 1GB (0)
MB 1GB+ (0)
Data Artifacts
Analysis Results
OS Accounts
Tags
Listing
File System
Table
Thumbnail
Summary
Save Table as
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
_01
._501
.fseventsd
_~7.IND
journalAttr.1
0.shadowIndexHead
tmp.0.cmpt.indexPostings
tmp.0.cmpt.indexHead
tmp.0.cmpt.indexPositions
tmp.0.cmpt.shadowIndexHead
_MP0CM~4.IND
tmp.0.cmpt.indexDirectory
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Page: 1 of 1
Page
Go to Page:
Jump to Offset
Launch in HxD


Data Sources
terry-work-usb-2009-12-11.E01_1 Host
terry-work-usb-2009-12-11.E01
vol1 (Unallocated: 0-62)
vol2 (Win95 FAT32 (0x0b): 63-4095944)
$OrphanFiles (0)
$Unalloc (2)
.fseventsd (0)
.Spotlight-V100 (3)
.Trashes (4)
_01 (0)
_078421_ (0)
_189812_ (0)
_452781_ (0)
_461531_ (0)
_604468_ (0)
Log (4998)
vol3 (Unallocated: 4095945-4095999)
File Views
File Types
Listing
/img_terry-work-usb-2009-12-11.E01/vol_vol2//$Unalloc
Table
Thumbnail
Summary
Name
S
C
Unalloc_10028_1154707968_2097123840
Unalloc_10028_80966144_1154707968
Hex
Text
Application
File Metadata
OS Account
0x00000000: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x00000010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00


_604468_ (0)
Log (4998)
vol3 (Unallocated: 4095945-4095999)
File Views
File Types
By Extension
Images (4992)
Videos (0)
Audio (0)
Archives (0)
Databases (4)
Documents
HTML (5)
Office (0)
PDF (0)
Plain Text (12)
Rich Text (0)
Executable
.exe (4)
.dll (0)
.bat (0)
.cmd (0)
.com (0)
By MIME Type
Listing
Images
Table
Thumbnail
Summary
Save T
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
M57biz.jpg
_M57biz.jpg
2009-12-03_00036d9f_big.jpg
2009-12-03_00036d9f_small.jpg
2009-12-03_0005425f_big.jpg
2009-12-03_0005425f_small.jpg
2009-12-03_0007171f_big.jpg
2009-12-03_0007171f_small.jpg
2009-12-03_0008ebdf_big.jpg
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
178%
Reset


terry-work-usb-2009-12-11.E01_1 Host
terry-work-usb-2009-12-11.E01
vol1 (Unallocated: 0-62)
vol2 (Win95 FAT32 (0x0b): 63-4095944)
vol3 (Unallocated: 4095945-4095999)
File Views
File Types
By Extension
Images (4992)
Videos (0)
Audio (0)
Archives (0)
Databases (4)
Documents
Executable
By MIME Type
Deleted Files
File System (24)
All (24)
MB File Size
MB 50 - 200MB (0)
MB 200MB - 1GB (0)
MB 1GB+ (0)
Data Artifacts
Analysis Results
OS Accounts
Tags
Reports
File System
Table
Thumbnail
Summary
Name
S
C
O
Modified Time
tmp.0.cmpt.indexCompactDirectory
tmp.0.cmpt.indexArrays
tmp.0.cmpt.newTermIDMap
tmp.0.cmpt.compactPayloads1.idx
tmp.0.cmpt.compactPayloads2.idx
_54402.EXE
_461531_
_604468_
_078421_
_452781_
_189812_
xpadvancedkeylogger.exe
2009-12-03 08:40:44 EST
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Page: 1 of 97
Page
Go to Page: 1
0x00000000: 3C 73 74 79 6C 65 3E 20 62 6F 64 79 20 7B 53 43 <style> body {SC
0x00000010: 52 4F 4C 4C 42 41 52 2D 46 41 43 45 2D 43 4F 4C ROLLBAR-FACE-COL
0x00000020: 4F 52 3A 23 46 46 46 46 46 46 3B 20 53 43 52 4F OR:#FFFFFF; SCRO
0x00000030: 4C 4C 42 41 52 2D 48 49 47 48 4C 49 47 48 54 2D LLBAR-HIGHLIGHT-
0x00000040: 43 4F 4C 4F 52 3A 23 44 46 44 46 44 46 3B 20 53 COLOR:#DFDFDF; S
0x00000050: 43 52 4F 4C 4C 42 41 52 2D 53 48 41 44 4F 57 2D CROLLBAR-SHADOW-

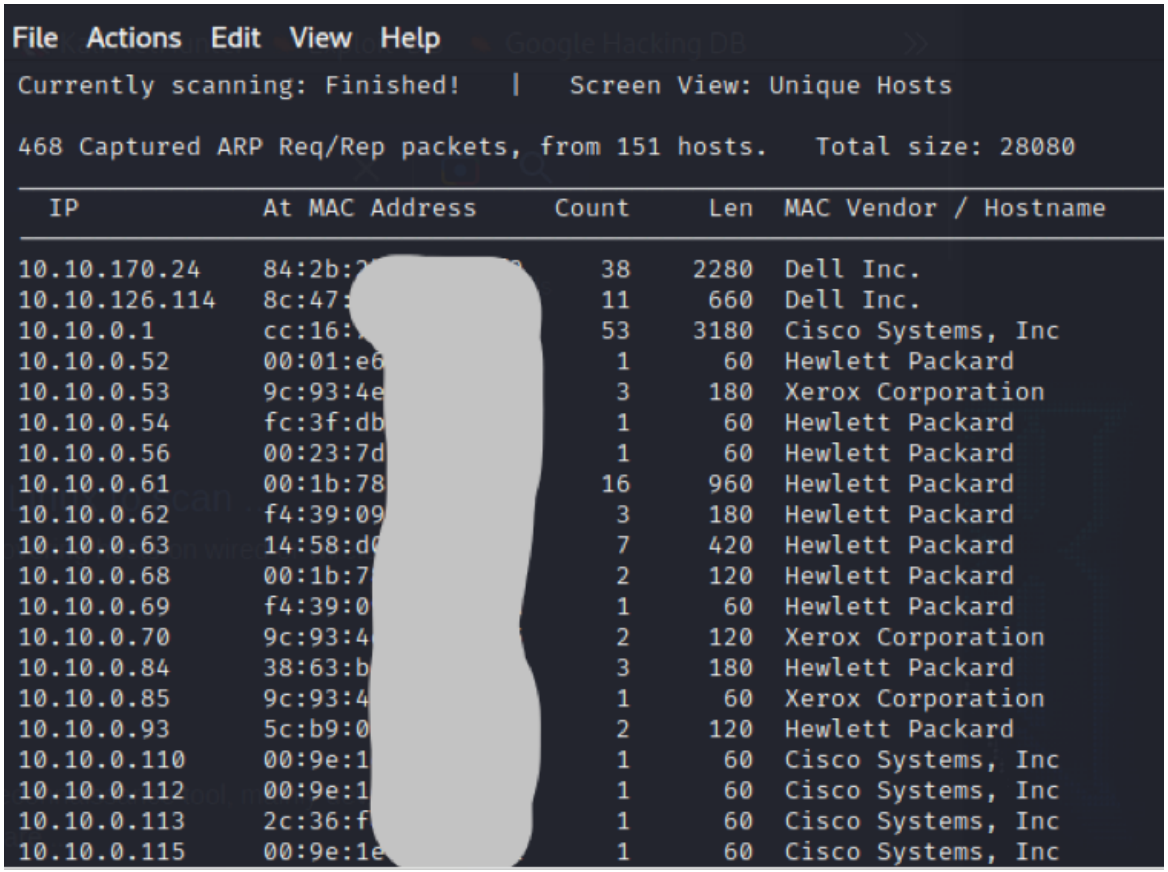

Timeline - Editor
Timeline
Forward
Years Months Days Hours Seconds
Category Event
Low Medium High
Number of Events (Logarithmic)
October December February March April May June July August October December
Hidden Descriptions
2008-10-15 17:14:08 to 2008-11-01 00:00:00
2 Results
Table Thumbnail Summary
Save Table as CSV
Icon Date/Time Description Event Type
2008-10-15 17:14:08 /vnc-4_1_3-x86_win32.exe File Modified
2008-10-15 17:14:08 /vnc-4_1_3-x86_win32.exe File Created
Context Annotations Other Occurrences
OS Account Data Artifacts Analysis Results
Hex Text Application File Metadata


Hidden Descriptions
2008-10-15 17:14:08 to 2008-11-01 00:00:00
2 Results
Table Thumbnail Summary
Save Table as CSV
Icon Date/Time Description Event Type
2008-10-15 17:14:08 /vnc-4_1_3-x86_win32.exe File Modified
2008-10-15 17:14:08 /vnc-4_1_3-x86_win32.exe File Created

Chapter 14: Network Discovery Tools

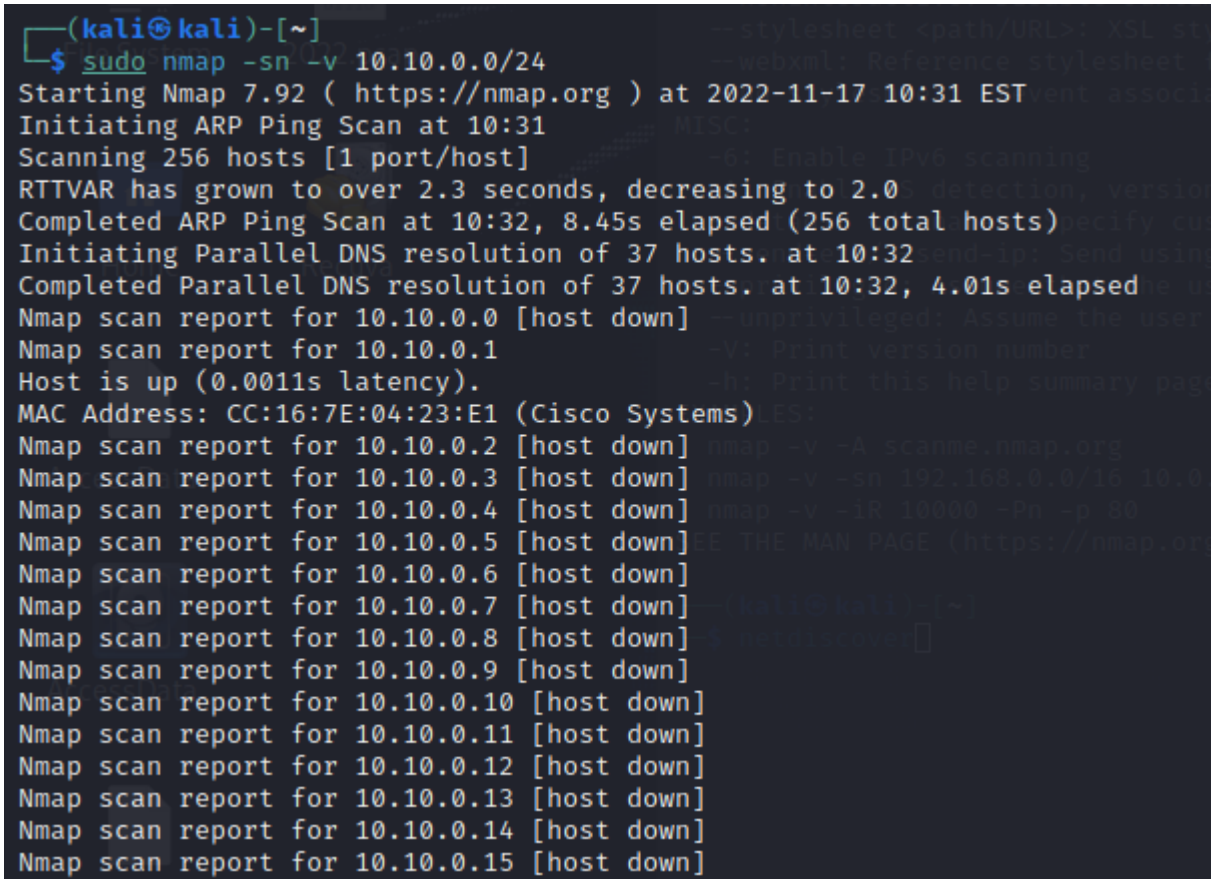
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.170.105  netmask 255.255.0.0  broadcast 10.10.255.255
        inet6 fe80::71ce:b8aa:c039:d0bd  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:22:46:4f  txqueuelen 1000  (Ethernet)
        RX packets 3159246  bytes 1121334766 (1.0 GiB)
        RX errors 0  dropped 16  overruns 0  frame 0
        TX packets 325325  bytes 21899177 (20.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 108  bytes 6010 (5.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 108  bytes 6010 (5.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

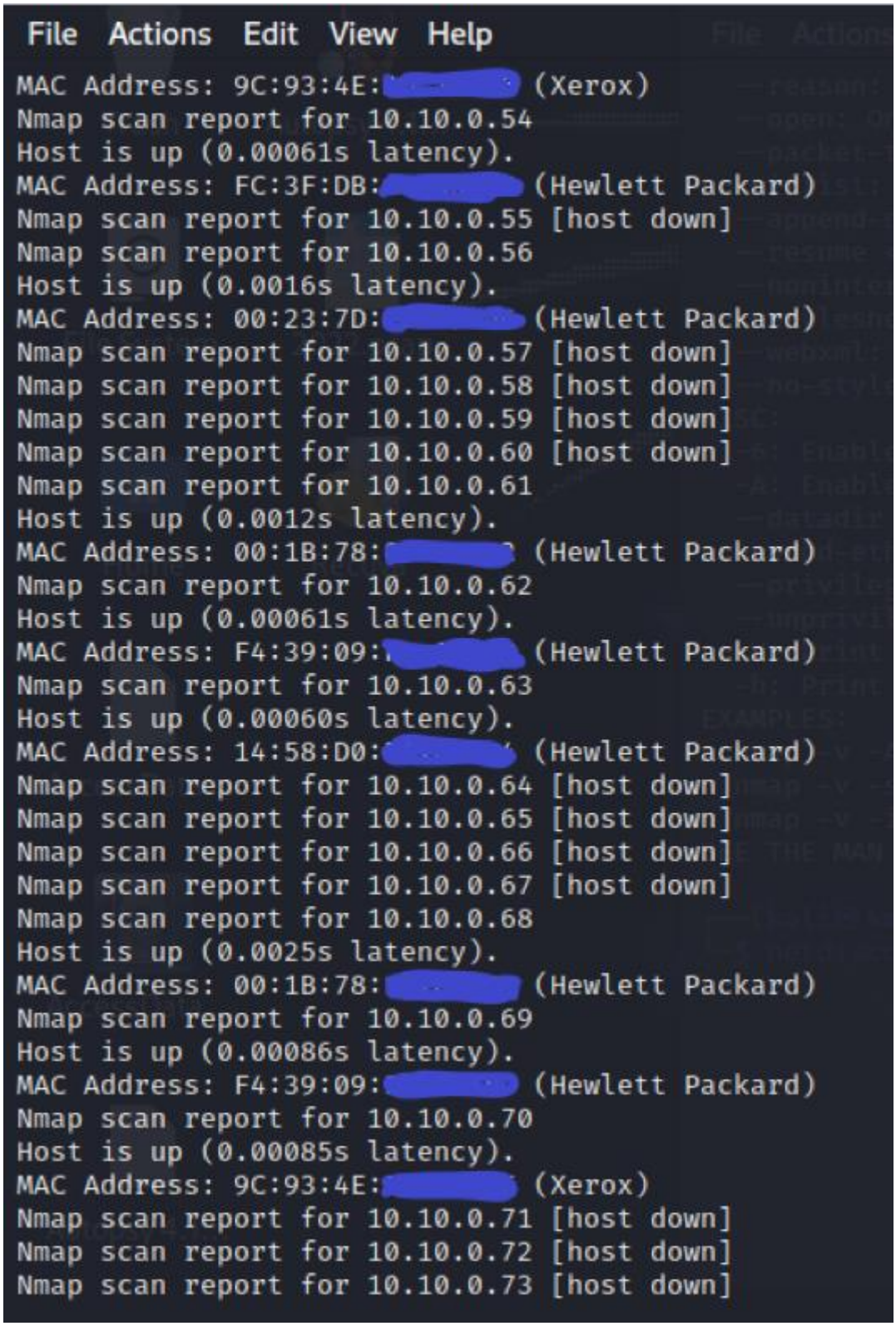
```
┌──(kali㉿kali)-[~]
└─$ sudo netdiscover -h
[sudo] password for kali:
Netdiscover 0.9 [Active/passive ARP reconnaissance tool]
Written by: Jaime Penalba <jpenalbae@gmail.com>

Usage: netdiscover [-i device] [-r range | -l file | -p] [-m file] [-F filter] [-s time]
 [-c count] [-n node] [-dfPLNS]
  -i device: your network device
  -r range: scan a given range instead of auto scan. 192.168.6.0/24,/16,/8
  -l file: scan the list of ranges contained into the given file
  -p passive mode: do not send anything, only sniff
  -m file: scan a list of known MACs and host names
  -F filter: customize pcap filter expression (default: "arp")
  -s time: time to sleep between each ARP request (milliseconds)
  -c count: number of times to send each ARP request (for nets with packet loss)
  -n node: last source IP octet used for scanning (from 2 to 253)
  -d ignore home config files for autoscan and fast mode
  -f enable fastmode scan, saves a lot of time, recommended for auto
  -P print results in a format suitable for parsing by another program and stop after ac
```



```
File  Actions  Edit  View  Help
Currently scanning: Finished!   |   Screen View: Unique Hosts

468 Captured ARP Req/Rep packets, from 151 hosts.   Total size: 28080
 IP            At MAC Address     Count     Len  MAC Vendor / Hostname
10.10.170.24    84:2b:2[redacted]    38    2280  Dell Inc.
10.10.126.114   8c:47:[redacted]     11     660  Dell Inc.
10.10.0.1       cc:16:7[redacted]    53    3180  Cisco Systems, Inc
10.10.0.52      00:01:e6[redacted]    1      60  Hewlett Packard
10.10.0.53      9c:93:4e[redacted]    3     180  Xerox Corporation
10.10.0.54      fc:3f:db[redacted]    1      60  Hewlett Packard
10.10.0.56      00:23:7d[redacted]    1      60  Hewlett Packard
10.10.0.61      00:1b:78[redacted]   16     960  Hewlett Packard
10.10.0.62      f4:39:09[redacted]    3     180  Hewlett Packard
10.10.0.63      14:58:d0[redacted]    7     420  Hewlett Packard
10.10.0.68      00:1b:7[redacted]     2     120  Hewlett Packard
10.10.0.69      f4:39:0[redacted]     1      60  Hewlett Packard
10.10.0.70      9c:93:4[redacted]     2     120  Xerox Corporation
10.10.0.84      38:63:b[redacted]     3     180  Hewlett Packard
10.10.0.85      9c:93:4[redacted]     1      60  Xerox Corporation
10.10.0.93      5c:b9:0[redacted]     2     120  Hewlett Packard
10.10.0.110     00:9e:1[redacted]     1      60  Cisco Systems, Inc
10.10.0.112     00:9e:1[redacted]     1      60  Cisco Systems, Inc
10.10.0.113     2c:36:f[redacted]     1      60  Cisco Systems, Inc
10.10.0.115     00:9e:1e[redacted]    1      60  Cisco Systems, Inc
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -h
[sudo] password for kali:
Nmap 7.92 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
```


┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn -v 10.10.0.0/24
Starting Nmap 7.92 (https://nmap.org) at 2022-11-17 10:31 EST
Initiating ARP Ping Scan at 10:31
Scanning 256 hosts [1 port/host]
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Completed ARP Ping Scan at 10:32, 8.45s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 37 hosts. at 10:32
Completed Parallel DNS resolution of 37 hosts. at 10:32, 4.01s elapsed
Nmap scan report for 10.10.0.0 [host down]
Nmap scan report for 10.10.0.1
Host is up (0.0011s latency).
MAC Address: CC:16:7E:04:23:E1 (Cisco Systems)
Nmap scan report for 10.10.0.2 [host down]
Nmap scan report for 10.10.0.3 [host down]
Nmap scan report for 10.10.0.4 [host down]
Nmap scan report for 10.10.0.5 [host down]
Nmap scan report for 10.10.0.6 [host down]
Nmap scan report for 10.10.0.7 [host down]
Nmap scan report for 10.10.0.8 [host down]
Nmap scan report for 10.10.0.9 [host down]
Nmap scan report for 10.10.0.10 [host down]
Nmap scan report for 10.10.0.11 [host down]
Nmap scan report for 10.10.0.12 [host down]
Nmap scan report for 10.10.0.13 [host down]
Nmap scan report for 10.10.0.14 [host down]
Nmap scan report for 10.10.0.15 [host down]

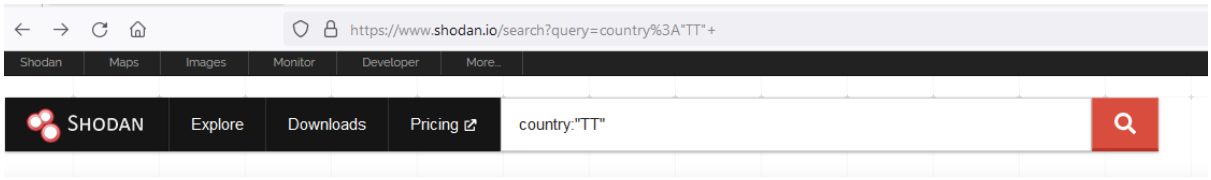

File Actions Edit View Help
MAC Address: 9C:93:4E: (Xerox)
Nmap scan report for 10.10.0.54
Host is up (0.00061s latency).
MAC Address: FC:3F:DB: (Hewlett Packard)
Nmap scan report for 10.10.0.55 [host down]
Nmap scan report for 10.10.0.56
Host is up (0.0016s latency).
MAC Address: 00:23:7D: (Hewlett Packard)
Nmap scan report for 10.10.0.57 [host down]
Nmap scan report for 10.10.0.58 [host down]
Nmap scan report for 10.10.0.59 [host down]
Nmap scan report for 10.10.0.60 [host down]
Nmap scan report for 10.10.0.61
Host is up (0.0012s latency).
MAC Address: 00:1B:78: (Hewlett Packard)
Nmap scan report for 10.10.0.62
Host is up (0.00061s latency).
MAC Address: F4:39:09: (Hewlett Packard)
Nmap scan report for 10.10.0.63
Host is up (0.00060s latency).
MAC Address: 14:58:D0: (Hewlett Packard)
Nmap scan report for 10.10.0.64 [host down]
Nmap scan report for 10.10.0.65 [host down]
Nmap scan report for 10.10.0.66 [host down]
Nmap scan report for 10.10.0.67 [host down]
Nmap scan report for 10.10.0.68
Host is up (0.0025s latency).
MAC Address: 00:1B:78: (Hewlett Packard)
Nmap scan report for 10.10.0.69
Host is up (0.00086s latency).
MAC Address: F4:39:09: (Hewlett Packard)
Nmap scan report for 10.10.0.70
Host is up (0.00085s latency).
MAC Address: 9C:93:4E: (Xerox)
Nmap scan report for 10.10.0.71 [host down]
Nmap scan report for 10.10.0.72 [host down]
Nmap scan report for 10.10.0.73 [host down]

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A -v 10.10.10.10
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-17 11:15 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:15
Completed NSE at 11:15, 0.00s elapsed
Initiating NSE at 11:15
Completed NSE at 11:15, 0.00s elapsed
Initiating NSE at 11:15
```

```
PORT     STATE SERVICE            VERSION
135/tcp  open  msrpc              Microsoft Windows RPC
139/tcp  open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds       Windows 10 Education 10586 microsoft-ds
3389/tcp open  ssl/ms-wbt-server?
```

```
| rdp-ntlm-info:
|   Target_Name: [redacted]
|   NetBIOS_Domain_Name: [redacted]
|   NetBIOS_Computer_Name: DESKTOP-CL6HVR6
|   DNS_Domain_Name: [redacted]
|   DNS_Computer_Name: DESKTOP-CL6HVR6.[redacted]
|   DNS_Tree_Name: [redacted]
|   Product_Version: 10.0.10586
|_  System_Time: 2022-11-17T16:16:15+00:00
```

```
MAC Address: F0:1F:AF:[redacted] (Dell)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
Uptime guess: 3.066 days (since Mon Nov 14 09:40:36 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: DESKTOP-CL6HVR6; OS: Windows; CPE: cpe:/o:microsoft:windows
```



TOTAL RESULTS

124,921

TOP CITIES

Port of Spain	46,420
Chaguanas	38,470
San Fernando	12,491
Arouca	4,087
Mon Repos	3,501

More...

TOP PORTS

8081	51,551
80	19,407
443	11,033
554	8,023
53	6,000

More...

TOP ORGANIZATIONS

Telecommunication Services of Trinid...	85,435
Columbus Communications Trinidad Li...	27,115
Digicel Trinidad and Tobago Ltd.	5,353
AMPLIA COMMUNICATIONS LTD.	1,882
AIR LINK COMMUNICATIONS	1,406

View Report | Download Results | Historical Trend | Browse Images | View on Map

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

186.44.217.173

0-1f-fb-b-bb-3f.dynamic.wimax.tstt.net.tt
Telecommunication Services of Trinidad and Tobago
Trinidad and Tobago, Port of Spain

```
No data returned
```

bMobile - Live Chat

196.3.132.218
kt.tstt.co.tt
tstt.co.tt
Telecommunications Services of Trinidad and Tobago
Trinidad and Tobago, Port of Spain

SSL Certificate

Issued By:
|- Common Name:
Sectigo RSA Domain Validation Secure Server CA
|- Organization:
Sectigo Limited

Issued To:
|- Common Name:
***.tstt.co.tt**

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

Diffie-Hellman Fingerprint:
RFC3526/Oakley Group 14

```
HTTP/1.1 200 OK
Date: Tue, 23 Aug 2022 12:53:51 GMT
Server: Apache/2.2.22 (@RELEASE@)
X-Powered-By: PHP/5.6.33
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

401 Unauthorized

186.45.67.82
186-45-67-82.dynamic.tstt.net.tt
Telecommunication Services of Trinidad and Tobago
Trinidad and Tobago, Port of Spain

```
HTTP/1.1 401 Unauthorized
Server: micro_httpd
Cache-Control: no-cache
Date: Tue, 23 Aug 2022 08:53:14 GMT
WWW-Authenticate: Basic realm="Broadband Router"
Content-Type: text/html
Connection: close
```

SHODAN | Explore | Downloads | Pricing | country:"TT" product:"Fortinet"

TOTAL RESULTS

54

TOP CITIES

Port of Spain	16
Chaguanas	15
San Fernando	14
Scarborough	3
Arima	2

More...

TOP PORTS

541	53
161	1

TOP ORGANIZATIONS

Digicel Trinidad and Tobago Ltd.	21
Columbus Communications Trinidad Limit...	17
Telecommunication Services of Trinidad an...	8
AMPLIA COMMUNICATIONS LTD.	4
Direct TV	1

More...

View Report | Download Results | Historical Trend | View on Map

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

181.118.55.126

Digicel Trinidad and Tobago Ltd.

Trinidad and Tobago, Chaguanas

self-signed

SSL Certificate

Issued By:
|- Common Name: support
|- Organization: Fortinet

Issued To:
|- Common Name: support
|- Organization: Fortinet

```
Fortinet FortiGate:
  Device: FortiGate-100E
  Model: FG100E
  Serial Number: FG100ETK19035697
```

190.83.155.214

Columbus Communications Trinidad Limited.

Trinidad and Tobago, Port of Spain

self-signed

SSL Certificate

Issued By:
|- Common Name: support
|- Organization: Fortinet

Issued To:
|- Common Name: support
|- Organization: Fortinet

```
Fortinet FortiGate:
  Device: FortiGate-81E
  Model: FGT81E
  Serial Number: FGT81ETK19000610
```

190.213.106.203

mail.smctt.com

Columbus Communications Trinidad Limited.

Trinidad and Tobago, San Fernando

```
SNMP:
  Versions:
    3
  Engineid Format: text
```

TOTAL RESULTS

11

TOP CITIES

Port of Spain	9
Chaguanas	2

TOP PORTS

80	7
443	4

TOP ORGANIZATIONS

Lisa Communications Ltd	8
Customs & Excise Division Trinidad	2
Telecommunication Services of Trinidad an...	1

View Report | Download Results | Historical Trend | View on Map

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

Home - The Republic of Trinidad And Tobago - Customs and Excise Division

190.213.2.154

ns2.customs.gov.tt

Customs & Excise Division Trinidad

Trinidad and Tobago, Chaguanas

```
HTTP/1.1 200 OK
Date: Thu, 17 Nov 2022 12:48:06 GMT
Server: Apache/2.2.3 (Red Hat)
X-Powered-By: PHP/5.4.19
Set-Cookie: PHPSESSID=mr55akiqpb6n36kom4kk46o354; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: ...
```

Test Page for the Apache HTTP Server on Red Hat Enterprise Linux

200.3.176.2

ns2.lisacommunications.com

Lisa Communications Ltd

Trinidad and Tobago, Port of Spain

```
HTTP/1.1 403 Forbidden
Date: Wed, 16 Nov 2022 22:06:14 GMT
Server: Apache/2.2.3 (Red Hat)
Accept-Ranges: bytes
Content-Length: 3985
Connection: close
Content-Type: text/html; charset=UTF-8
```

Home - The Republic of Trinidad And Tobago - Customs and Excise Division

190.213.6.155

Customs & Excise Division Trinidad

Trinidad and Tobago, Chaguanas

```
HTTP/1.1 200 OK
Date: Sat, 12 Nov 2022 14:48:13 GMT
Server: Apache/2.2.3 (Red Hat)
X-Powered-By: PHP/5.4.6
Set-Cookie: PHPSESSID=1okthefdv8sgbibpbgtleeh2l0; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: n...
```

SHODAN | Explore | Downloads | Pricing | country:"TT" product:"Hikvision IP Camera"

TOTAL RESULTS

7,689

TOP CITIES

Chaguanas	1,418
Port of Spain	1,328
San Fernando	939
Arima	578
Arouca	492

More...

TOP PORTS

80	6,977
8080	133
81	113
8001	58
443	55

More...

TOP ORGANIZATIONS

Columbus Communications Trinidad Li...	6,345
Telecommunication Services of Trinidad ...	457
NETWORK TECHNOLOGIES LIMITED	245
Digicel Trinidad and Tobago Ltd.	214
RVR INTERNATIONAL LIMITED	189

View Report | Download Results | Historical Trend | Brow

New Service: Keep track of what you have connected to the Internet.

131.221.28.123

NETWORK TECHNOLOGIES LIMITED

Trinidad and Tobago, Rio Claro

```
HTTP/1.1 200 OK
Date: Thu, 17 Nov 2022 15:02:31 GMT
Server: Webs
X-Frame-Options: SAMEORIGIN
ETag: "0-aec-1e0"
Content-Length: 480
Content-Type: text/html
Connection: keep-alive
Keep-Alive: timeout=60, max=99
Last-Modified: Wed, 25 Sep 2019 08:02:22 GMT

Hikvision IP Camera:
  Web Ver...
```

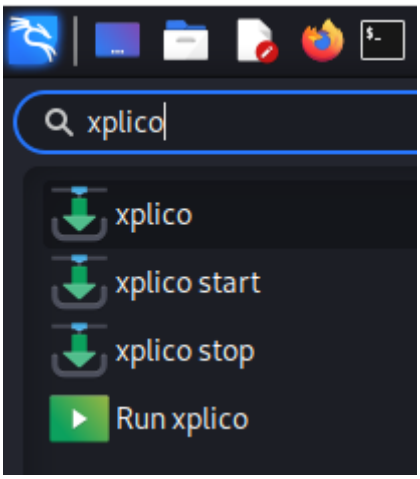
190.83.147.178

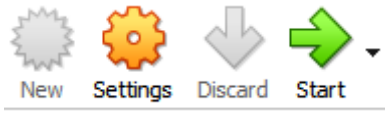
Columbus Communications Trinidad Limited.

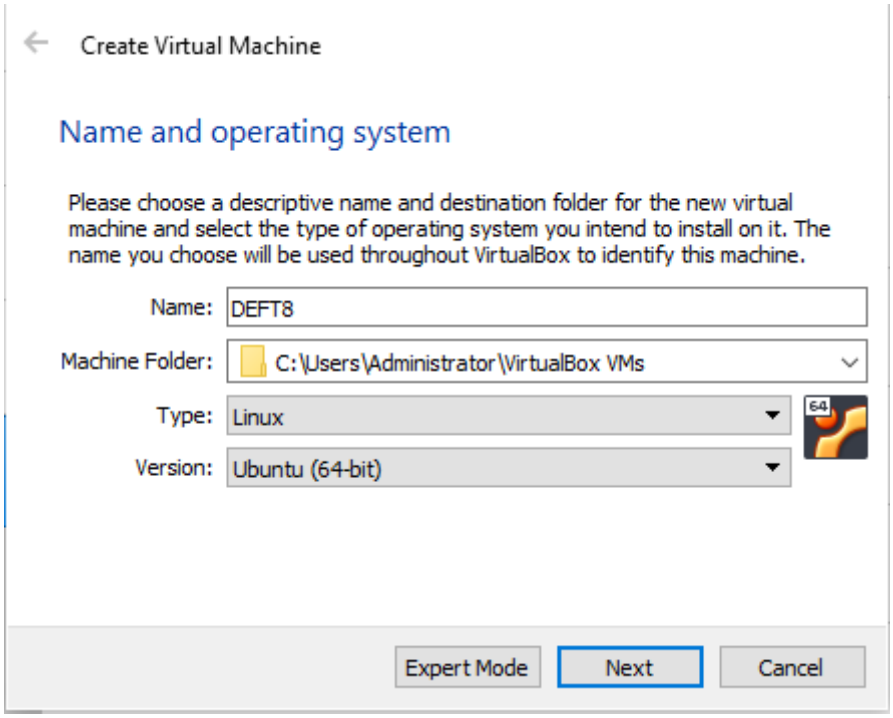
Trinidad and Tobago, Arima

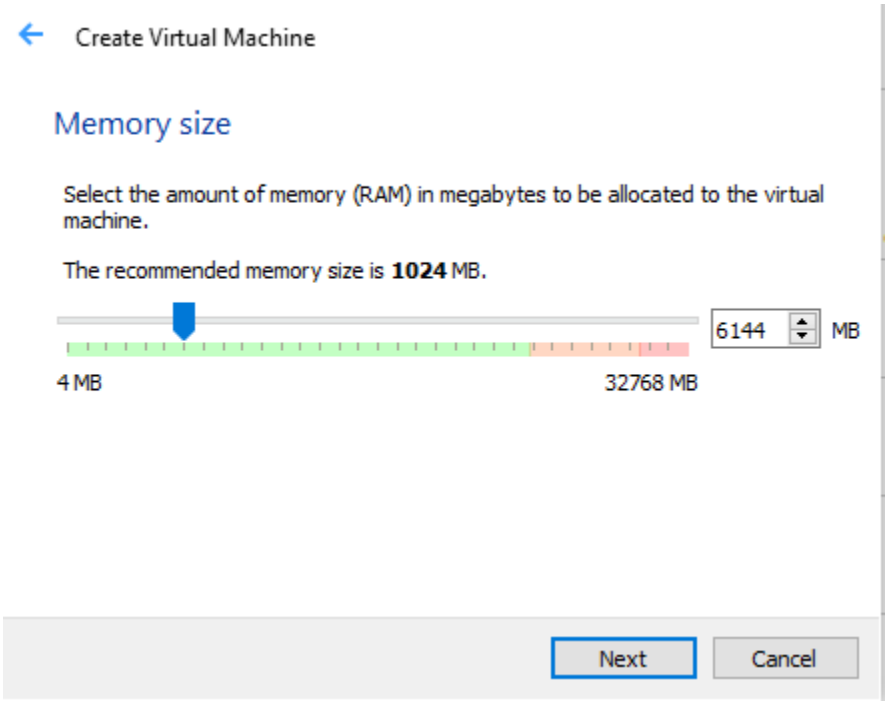
```
HTTP/1.1 200 OK
Date: Thu, 17 Nov 2022 14:53:52 GMT
Server: Webs
X-Frame-Options: SAMEORIGIN
ETag: "0-1b51-1e1"
Content-Length: 481
Content-Type: text/html
Connection: keep-alive
Keep-Alive: timeout=180, max=99
Last-Modified: Fri, 08 Jan 2021 08:42:23 GMT

Hikvision IP Camera:
  Web V...
```

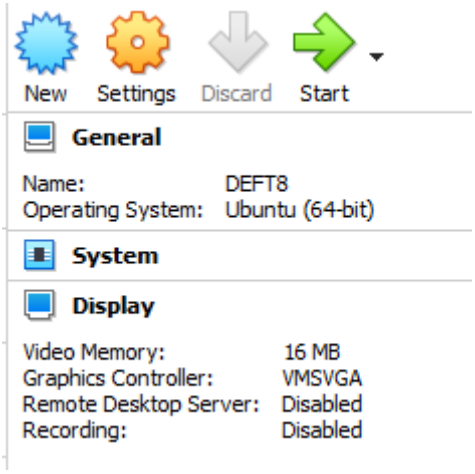
Chapter 15: Packet Capture Analysis with Xplico

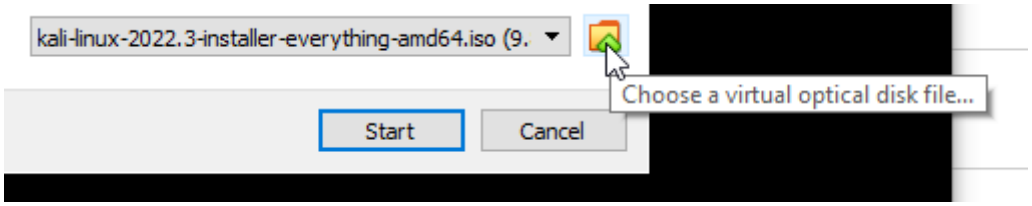


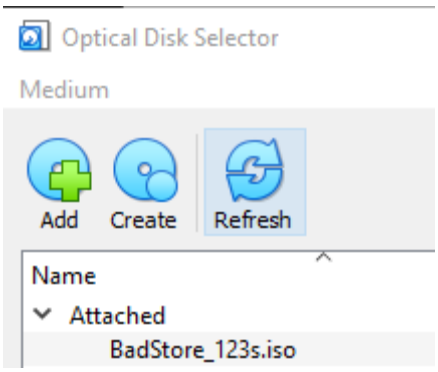


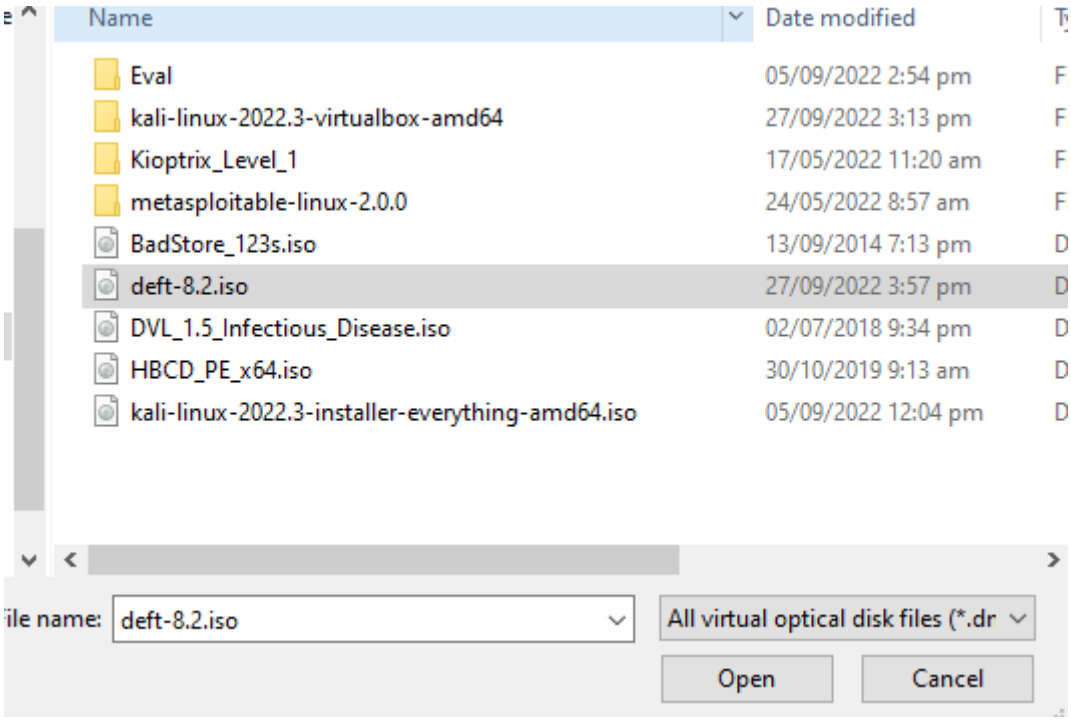


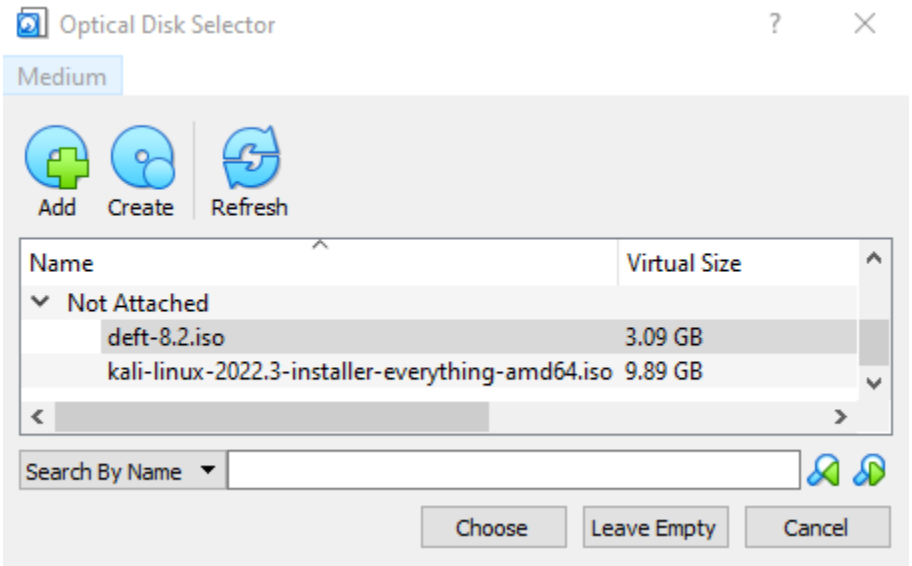

Create Virtual Machine
Memory size
Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.
The recommended memory size is 1024 MB.
6144
MB
4 MB
32768 MB
Next
Cancel

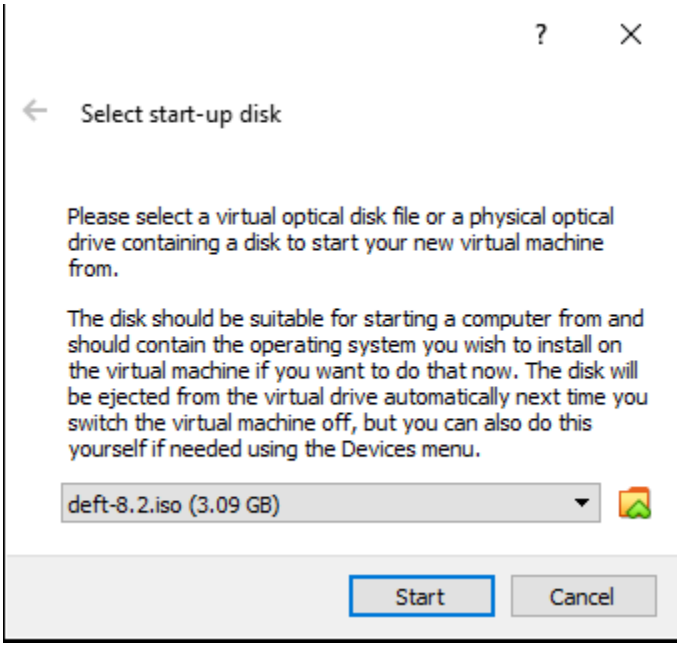

New
Settings
Discard
Start
General
Name: DEFT8
Operating System: Ubuntu (64-bit)
System
Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled


kali-linux-2022.3-installer-everything-amd64.iso (9.
Choose a virtual optical disk file...
Start
Cancel


Optical Disk Selector
Medium
Add
Create
Refresh
Name
Attached
BadStore_123s.iso


Name
Date modified
Eval
05/09/2022 2:54 pm
kali-linux-2022.3-virtualbox-amd64
27/09/2022 3:13 pm
Kioptrix_Level_1
17/05/2022 11:20 am
metasploitable-linux-2.0.0
24/05/2022 8:57 am
BadStore_123s.iso
13/09/2014 7:13 pm
deft-8.2.iso
27/09/2022 3:57 pm
DVL_1.5_Infectious_Disease.iso
02/07/2018 9:34 pm
HBCD_PE_x64.iso
30/10/2019 9:13 am
kali-linux-2022.3-installer-everything-amd64.iso
05/09/2022 12:04 pm
ile name:
deft-8.2.iso
All virtual optical disk files (*.dr
Open
Cancel


Optical Disk Selector
Medium
Add
Create
Refresh
Name
Virtual Size
Not Attached
deft-8.2.iso
3.09 GB
kali-linux-2022.3-installer-everything-amd64.iso
9.89 GB
Search By Name
Choose
Leave Empty
Cancel

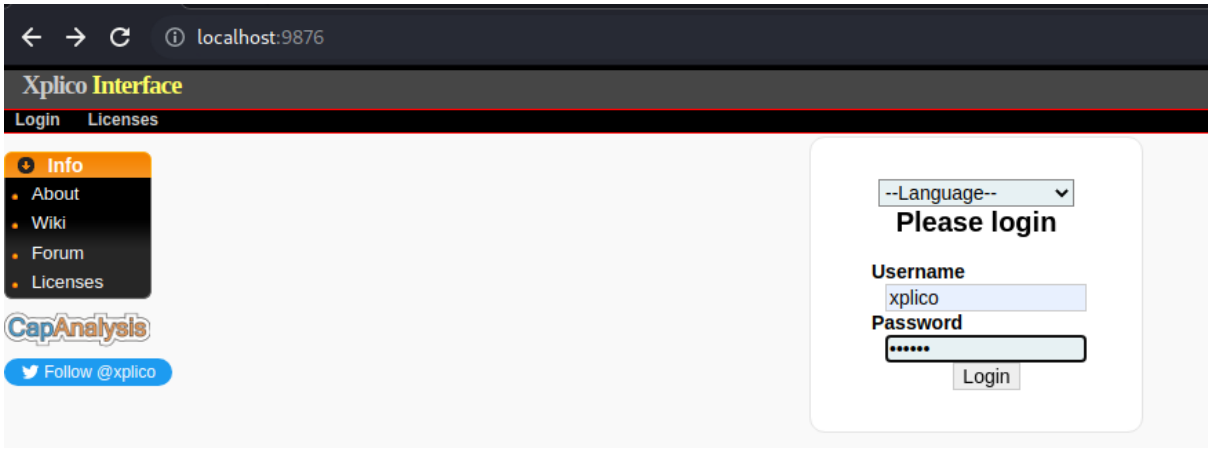

Select start-up disk
Please select a virtual optical disk file or a physical optical drive containing a disk to start your new virtual machine from.
The disk should be suitable for starting a computer from and should contain the operating system you wish to install on the virtual machine if you want to do that now. The disk will be ejected from the virtual drive automatically next time you switch the virtual machine off, but you can also do this yourself if needed using the Devices menu.
deft-8.2.iso (3.09 GB)
Start
Cancel

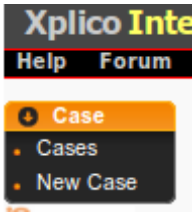

DEFT8 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
deft
DEFT Linux 8 live
DEFT Linux 8 live text mode
26 s
Install DEFT Linux 8
Check disc for defects
Test memory
Boot from first hard disk
English
Español
Italiano
F1 Help F2 Language F3 Keymap F4 Modes F5 Accessibility F6 Other Options

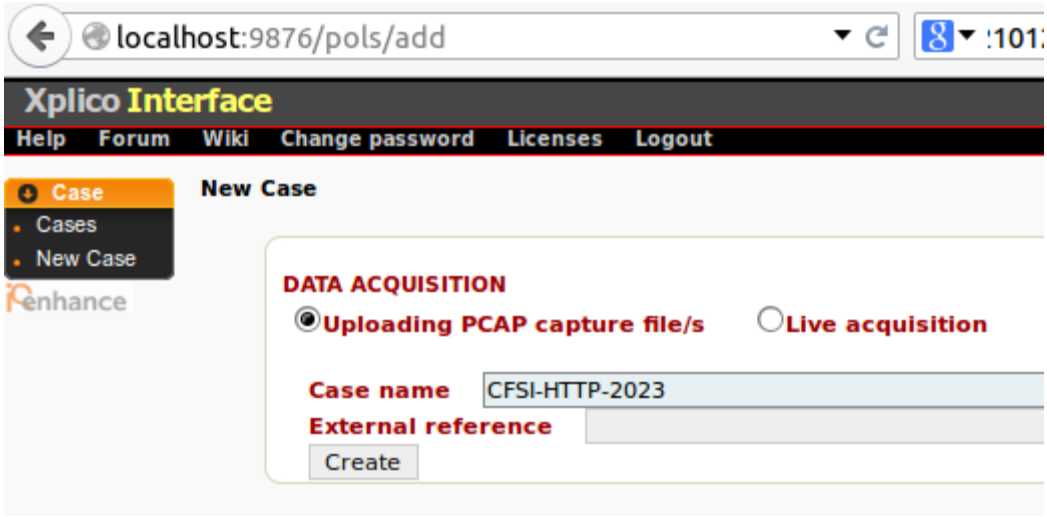

DEFT8 [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
LXTerminal
evidence
File Manager
Guymager
deft
14:29
Right Ctrl

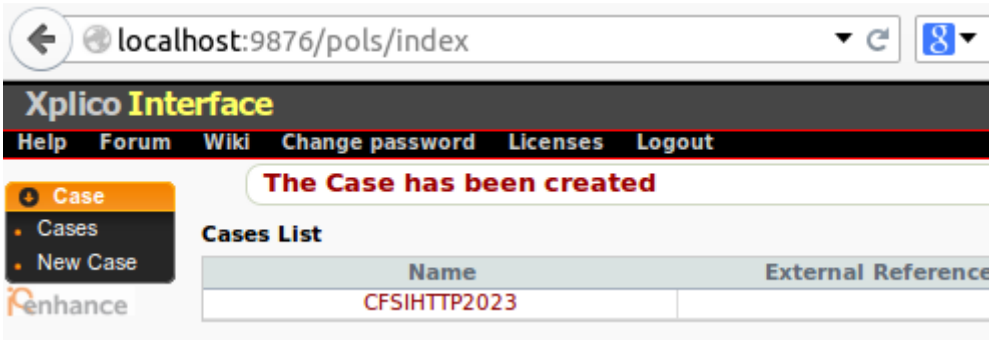

DEFT8 [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
LXTerminal
evidence
File Manager
Guymager
deft
14:29
Right Ctrl

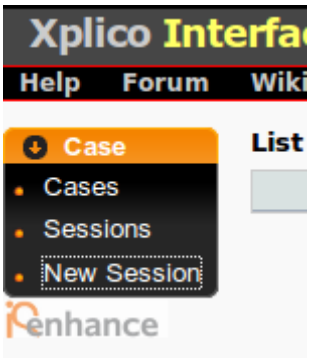

Accessories
DEFT
Graphics
Internet
Office
Programming
Service
Sound & Video
Wine
System Tools
Preferences
Run
Logout
Analysis
Antimalware
Data Recovery
Hashing
Imaging
Mobile Forensics
Network Forensics
OSINT
Password recovery
Reporting tools
Disks
File Manager PCManFM
GParted
Midnight Commander
MountManager
CapAnalysis
Nmap
Wireshark
Xplico

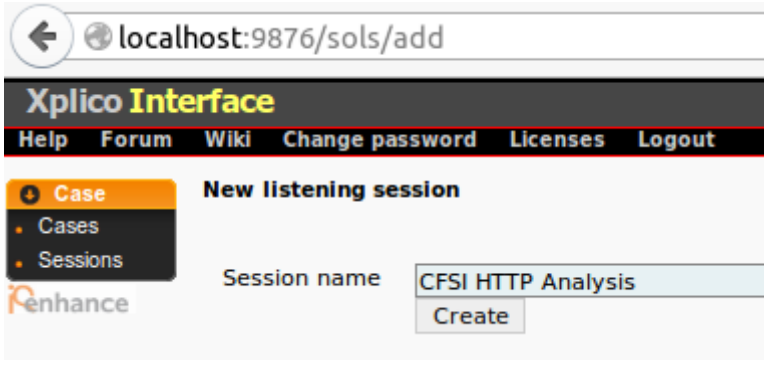

localhost:9876
Xplico Interface
Login
Licenses
Info
About
Wiki
Forum
Licenses
CapAnalysis
Follow @xplico
--Language--
Please login
Username
xplico
Password
Login

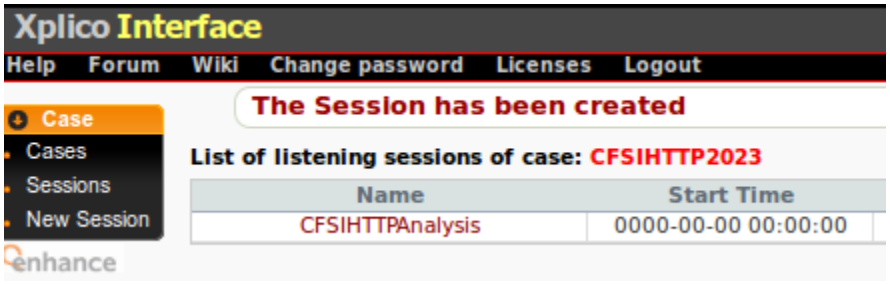

Xplico Inte
Help
Forum
Case
Cases
New Case

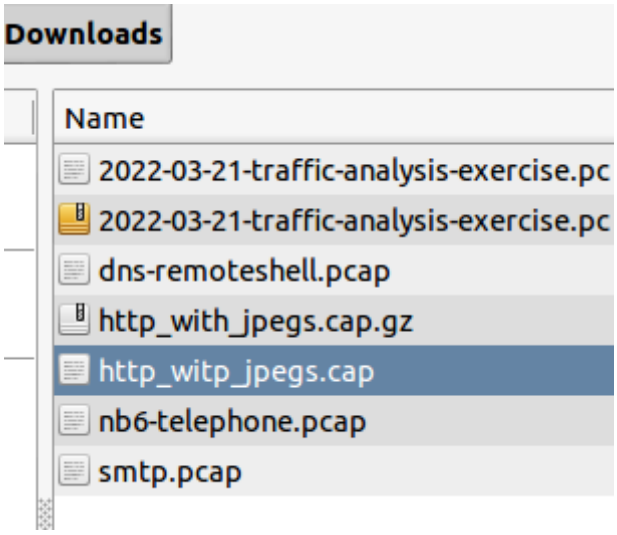

localhost:9876/pols/add
Xplico Interface
Help Forum Wiki Change password Licenses Logout
Case
Cases
New Case
New Case
DATA ACQUISITION
Uploading PCAP capture file/s
Live acquisition
Case name
CFSI-HTTP-2023
External reference
Create

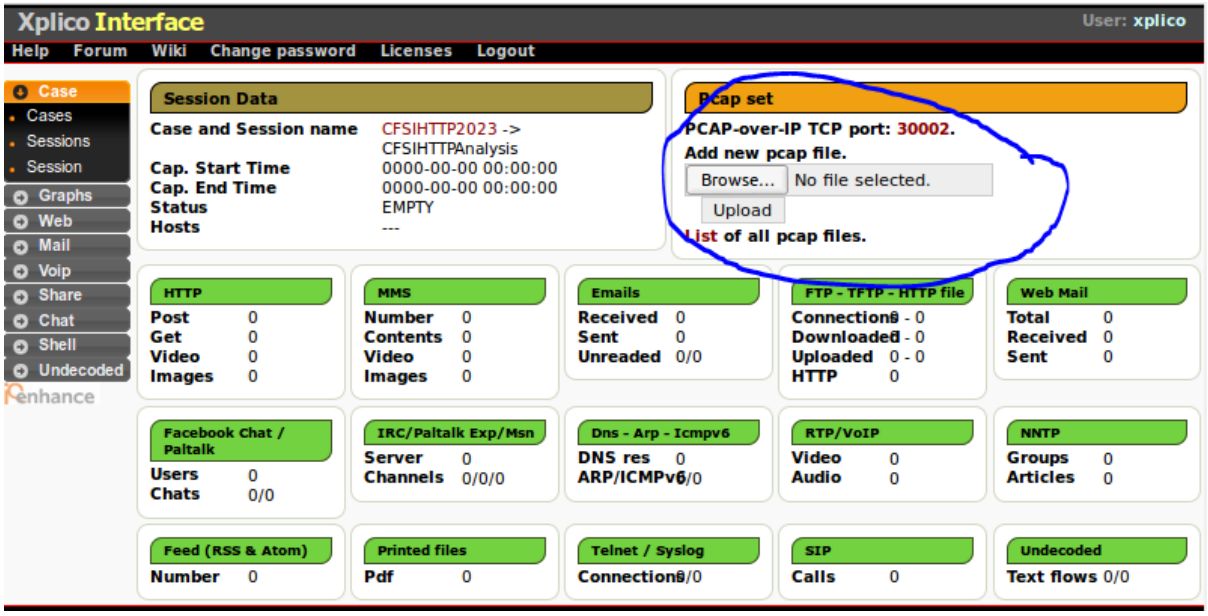

localhost:9876/pols/index
Xplico Interface
Help Forum Wiki Change password Licenses Logout
Case
Cases
New Case
The Case has been created
Cases List
Name
External Reference
CFSIHTTP2023

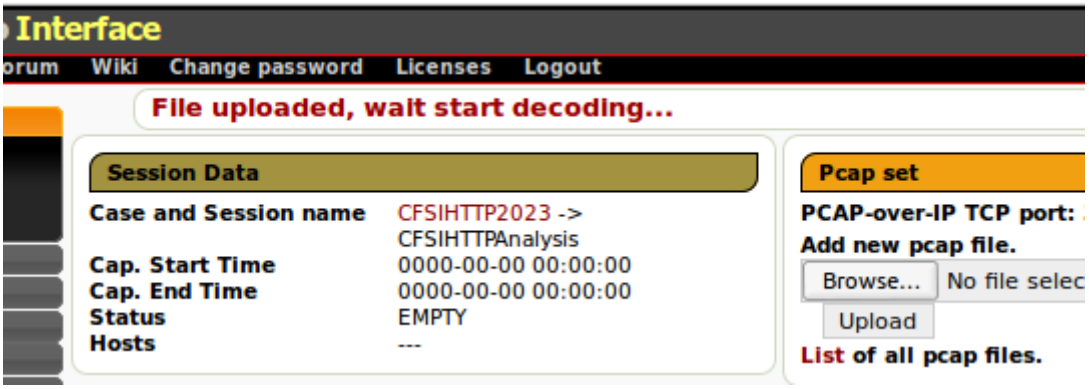

Help Forum
Case
Cases
Sessions
New Session

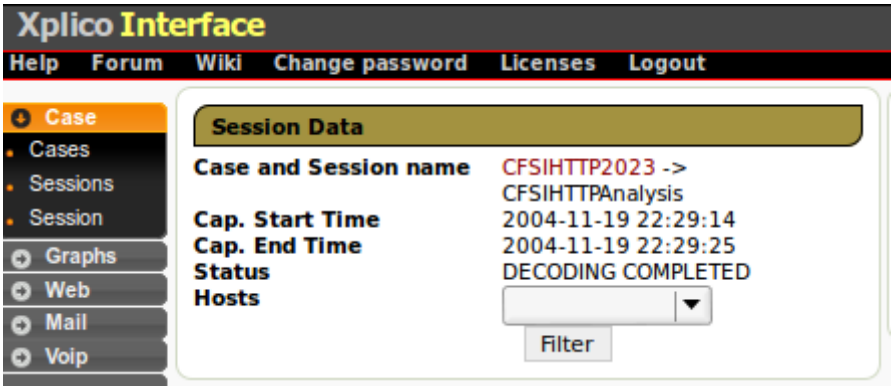

localhost:9876/sols/add
Xplico Interface
Help Forum Wiki Change password Licenses Logout
Case
Cases
Sessions
New listening session
Session name
CFSI HTTP Analysis
Create

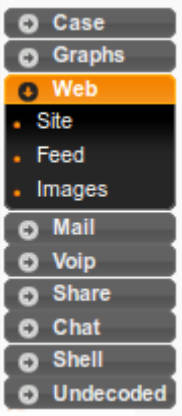

Xplico Interface
Help Forum Wiki Change password Licenses Logout
Case
Cases
Sessions
New Session
The Session has been created
List of listening sessions of case: CFSIHTTP2023
Name
Start Time
CFSIHTTPAnalysis
0000-00-00 00:00:00
enhance

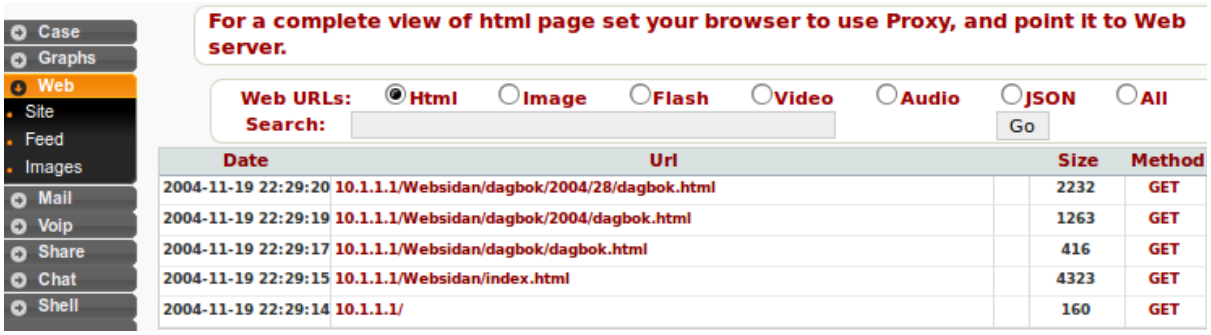

Downloads
Name
2022-03-21-traffic-analysis-exercise.pc
2022-03-21-traffic-analysis-exercise.pc
dns-remoteshell.pcap
http_with_jpegs.cap.gz
http_witp_jpegs.cap
nb6-telephone.pcap
smtp.pcap

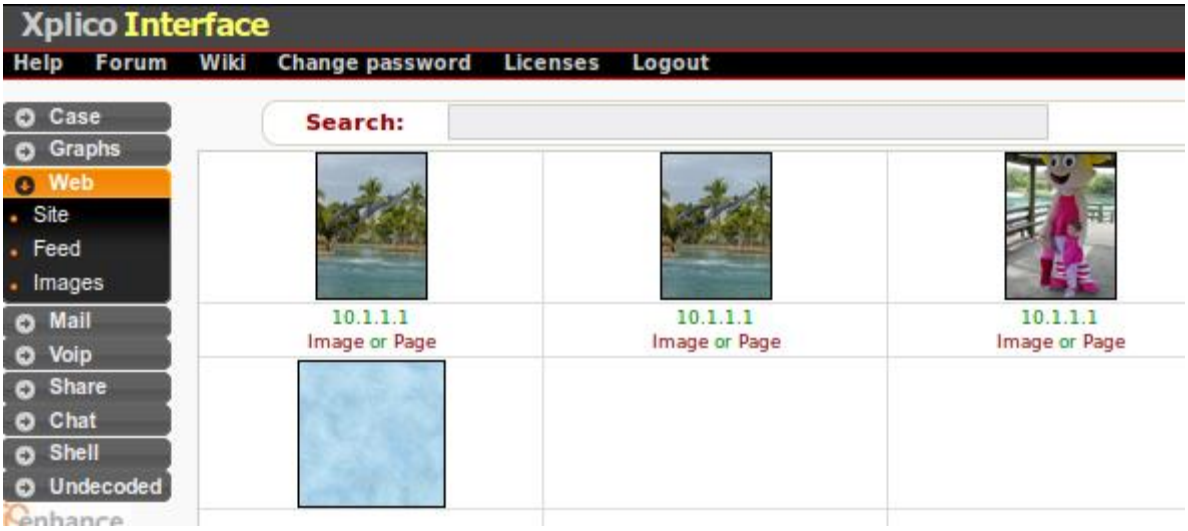

Xplico Interface
User: xplico
Help Forum Wiki Change password Licenses Logout
Case
Cases
Sessions
Session
Graphs
Web
Mail
Voip
Share
Chat
Shell
Undecoded
enhance
Session Data
Case and Session name CFSIHTTP2023 -> CFSIHTTPAnalysis
Cap. Start Time 0000-00-00 00:00:00
Cap. End Time 0000-00-00 00:00:00
Status EMPTY
Hosts ---
Pcap set
PCAP-over-IP TCP port: 30002.
Add new pcap file.
Browse... No file selected.
Upload
List of all pcap files.
HTTP
Post 0
Get 0
Video 0
Images 0
MMS
Number 0
Contents 0
Video 0
Images 0
Emails
Received 0
Sent 0
Unreaded 0/0
FTP - TFTP - HTTP file
Connections 0 - 0
Downloaded 0 - 0
Uploaded 0 - 0
HTTP 0
Web Mail
Total 0
Received 0
Sent 0
Facebook Chat / Paltalk
Users 0
Chats 0/0
IRC/Paltalk Exp/Msn
Server 0
Channels 0/0/0
Dns - Arp - Icmpv6
DNS res 0
ARP/ICMPv6 0/0
RTP/VoIP
Video 0
Audio 0
NNTP
Groups 0
Articles 0
Feed (RSS & Atom)
Number 0
Printed files
Pdf 0
Telnet / Syslog
Connections 0/0
SIP
Calls 0
Undecoded
Text flows 0/0

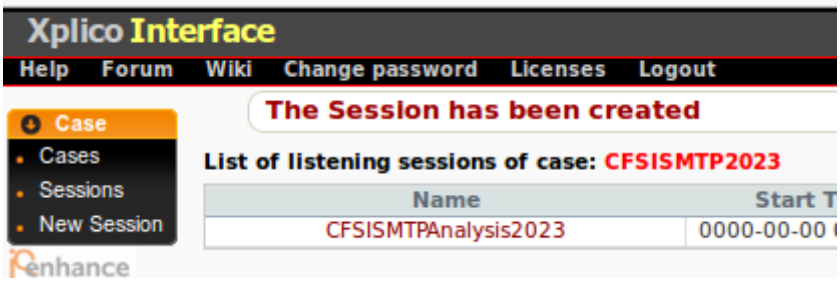

Interface
orum Wiki Change password Licenses Logout
File uploaded, wait start decoding...
Session Data
Case and Session name CFSIHTTP2023 -> CFSIHTTPAnalysis
Cap. Start Time 0000-00-00 00:00:00
Cap. End Time 0000-00-00 00:00:00
Status EMPTY
Hosts ---
Pcap set
PCAP-over-IP TCP port:
Add new pcap file.
Browse... No file selec
Upload
List of all pcap files.

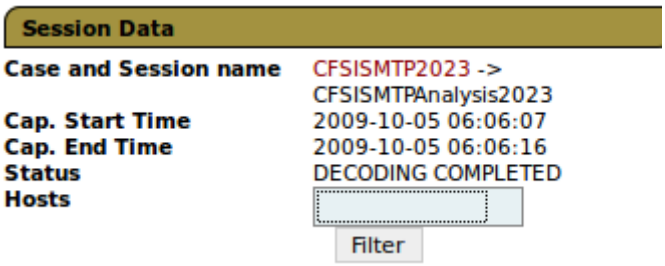

Xplico Interface
Help Forum Wiki Change password Licenses Logout
Case
Cases
Sessions
Session
Graphs
Web
Mail
Voip
Session Data
Case and Session name CFSIHTTP2023 -> CFSIHTTPAnalysis
Cap. Start Time 2004-11-19 22:29:14
Cap. End Time 2004-11-19 22:29:25
Status DECODING COMPLETED
Hosts
Filter

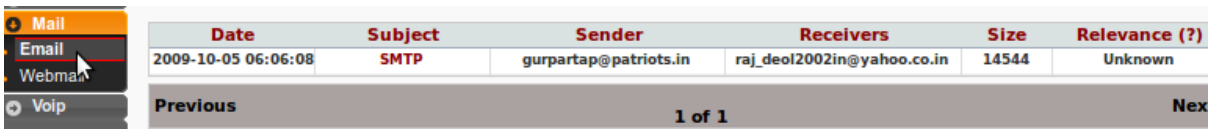

Case
Graphs
Web
Site
Feed
Images
Mail
Voip
Share
Chat
Shell
Undecoded

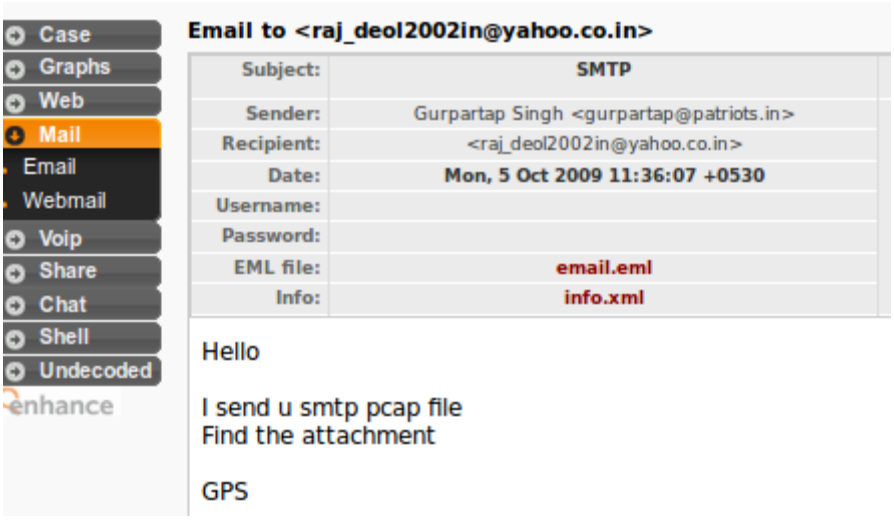

Case
Graphs
Web
Site
Feed
Images
Mail
Voip
Share
Chat
Shell
For a complete view of html page set your browser to use Proxy, and point it to Web server.
Web URLs: Html Image Flash Video Audio JSON All
Search:
Go
Date Url Size Method
2004-11-19 22:29:20 10.1.1.1/Websidan/dagbok/2004/28/dagbok.html 2232 GET
2004-11-19 22:29:19 10.1.1.1/Websidan/dagbok/2004/dagbok.html 1263 GET
2004-11-19 22:29:17 10.1.1.1/Websidan/dagbok/dagbok.html 416 GET
2004-11-19 22:29:15 10.1.1.1/Websidan/index.html 4323 GET
2004-11-19 22:29:14 10.1.1.1/ 160 GET

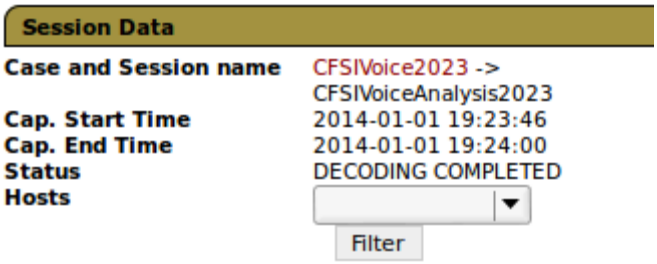

Xplico Interface
Help Forum Wiki Change password Licenses Logout
Case
Graphs
Web
Site
Feed
Images
Mail
Voip
Share
Chat
Shell
Undecoded
Search:
10.1.1.1
Image or Page
10.1.1.1
Image or Page
10.1.1.1
Image or Page

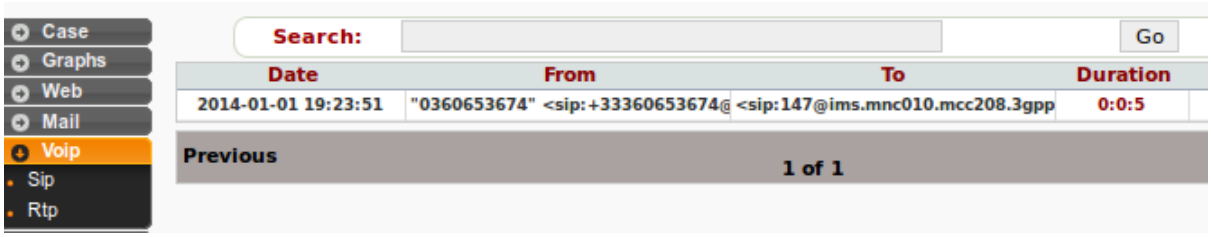

Xplico Interface
Help Forum Wiki Change password Licenses Logout
Case
Cases
Sessions
New Session
The Session has been created
List of listening sessions of case: CFSISMTP2023
Name
Start T
CFSISMTPAnalysis2023
0000-00-00


Session Data
Case and Session name
CFSISMTP2023 ->
CFSISMTPAnalysis2023
Cap. Start Time
2009-10-05 06:06:07
Cap. End Time
2009-10-05 06:06:16
Status
DECODING COMPLETED
Hosts
Filter


Mail
Email
Webmail
Voip
Date
Subject
Sender
Receivers
Size
Relevance (?)
2009-10-05 06:06:08
SMTP
gurpartap@patriots.in
raj_deol2002in@yahoo.co.in
14544
Unknown
Previous
1 of 1
Nex


Case
Graphs
Web
Mail
Email
Webmail
Voip
Share
Chat
Shell
Undecoded
enhance
Email to <raj_deol2002in@yahoo.co.in>
Subject: SMTP
Sender: Gurpartap Singh <gurpartap@patriots.in>
Recipient: <raj_deol2002in@yahoo.co.in>
Date: Mon, 5 Oct 2009 11:36:07 +0530
Username:
Password:
EML file: email.eml
Info: info.xml
Hello
I send u smtp pcap file
Find the attachment
GPS

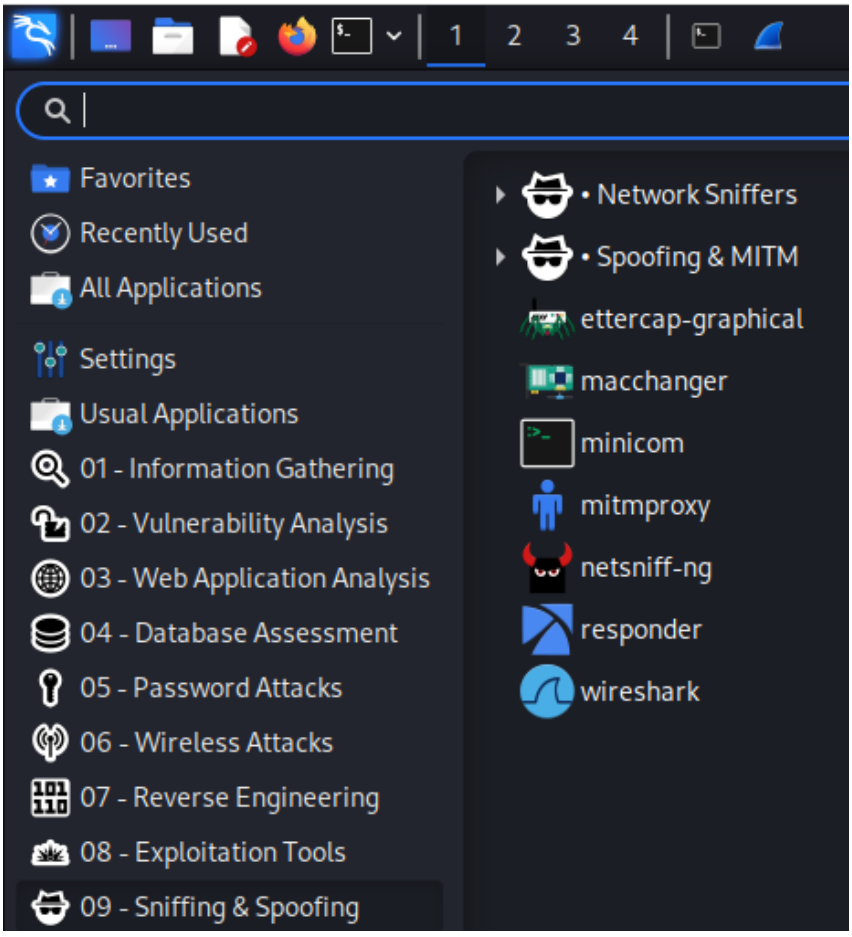

Session Data
Case and Session name CFSIVoice2023 -> CFSIVoiceAnalysis2023
Cap. Start Time 2014-01-01 19:23:46
Cap. End Time 2014-01-01 19:24:00
Status DECODING COMPLETED
Hosts
Filter

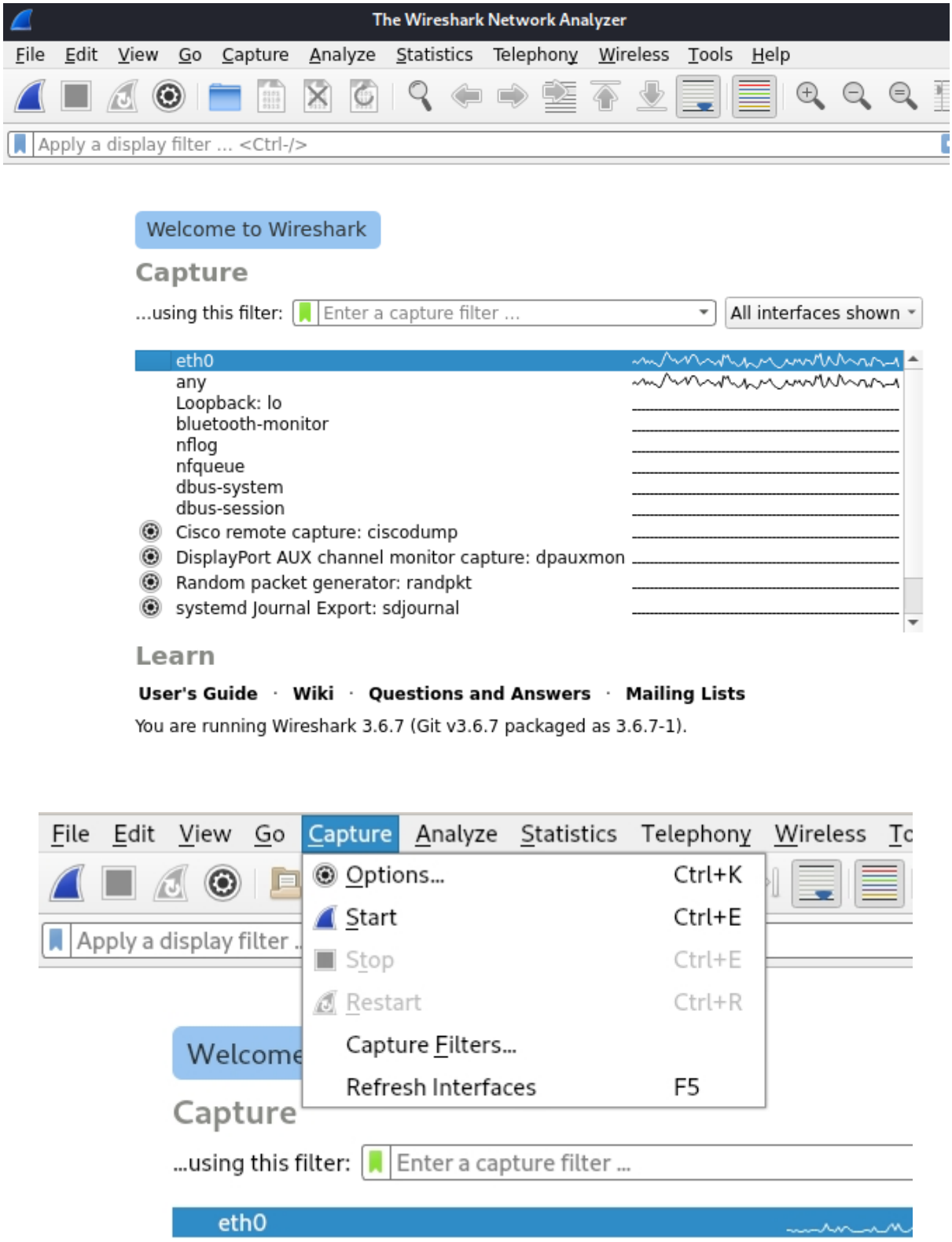

Case
Graphs
Web
Mail
Voip
Sip
Rtp
Search:
Go
Date
From
To
Duration
2014-01-01 19:23:51
"0360653674" <sip:+33360653674@
<sip:147@ims.mnc010.mcc208.3gpp
0:0:5
Previous
1 of 1


Date: 2014-01-01 19:23:51
From: "0360653674" <sip:+33360653674@ims.mnc010.mcc208.3gppnetwork.org
To: <sip:147@ims.mnc010.mcc208.3gppnetwork.org
Duration: 0:0:5
Commands: cmd.txt
Info: info.xml
A plugin is needed to display this content.
Install plugin...

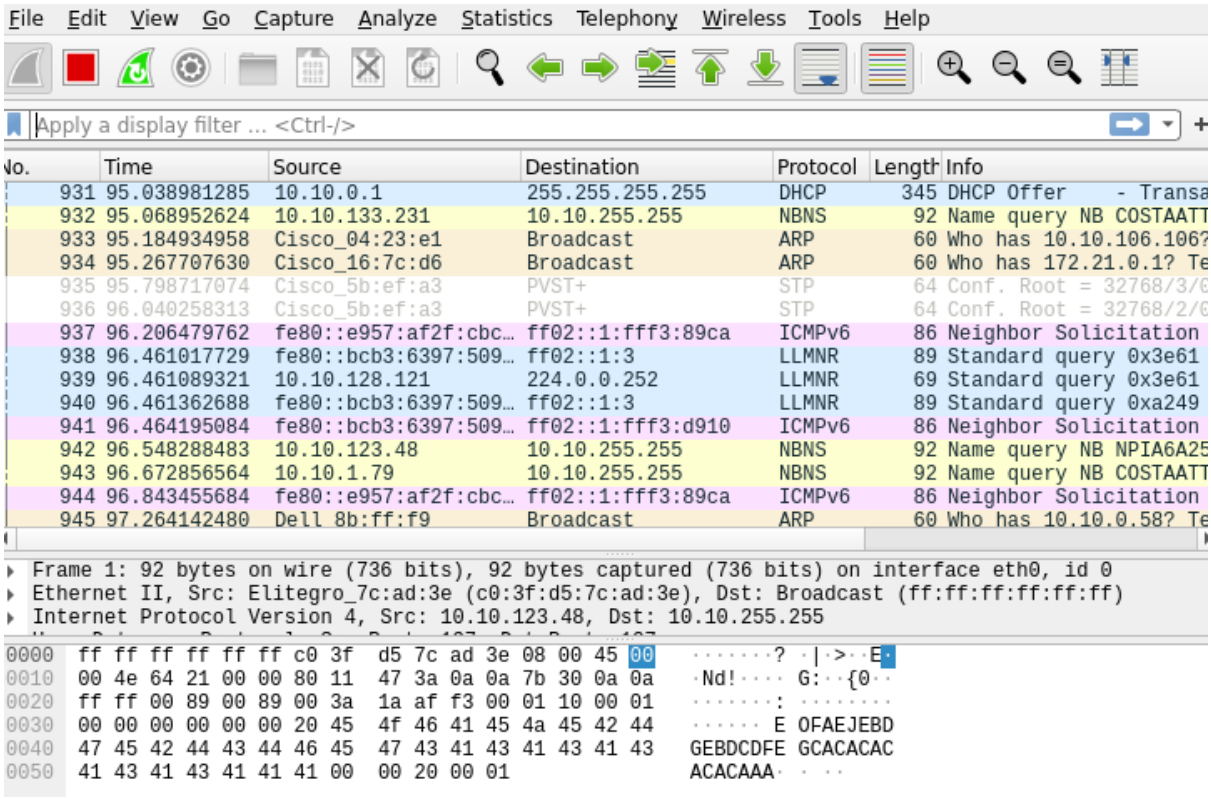
Chapter 16: Network Forensic Analysis Tools

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.170.105  netmask 255.255.0.0  broadcast 10.10.255.255
        inet6 fe80::71ce:b8aa:c039:d0bd  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:22:46:4f  txqueuelen 1000  (Ethernet)
        RX packets 575  bytes 56599 (55.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 1932 (1.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

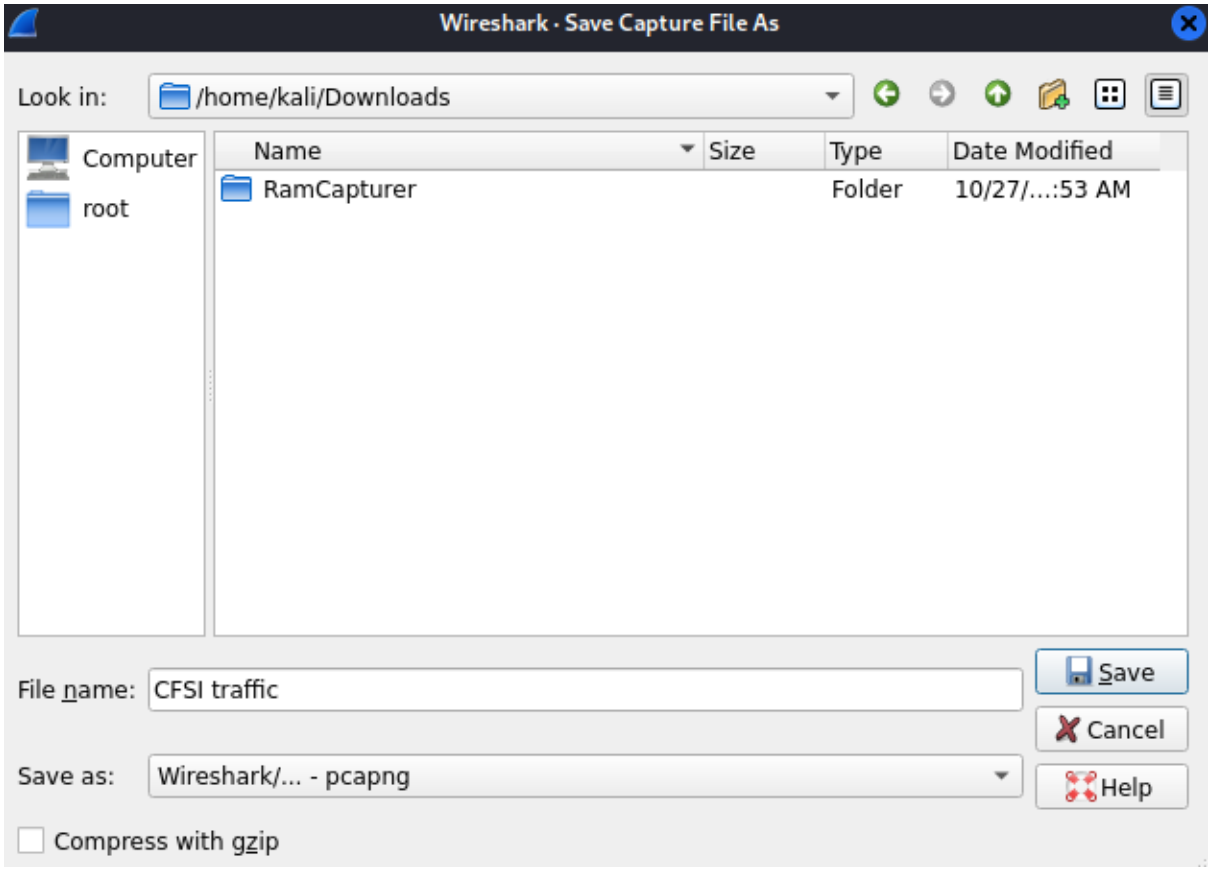


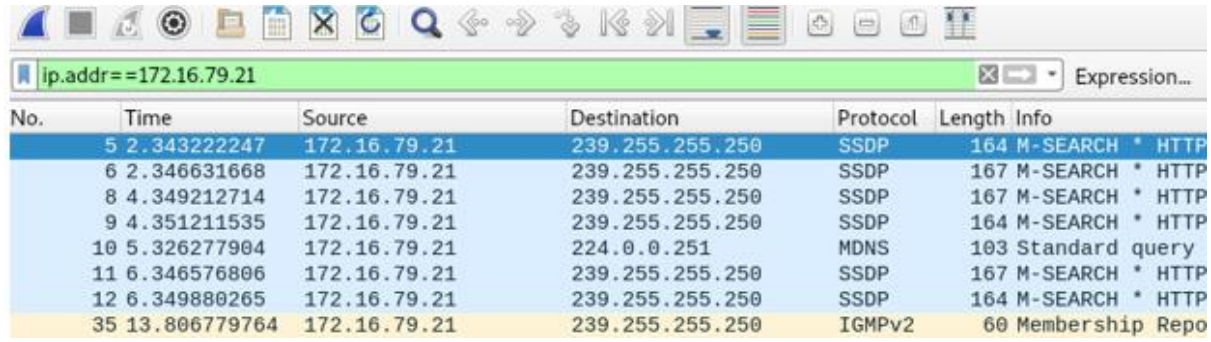

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.6.7 (Git v3.6.7 packaged as 3.6.7-1).

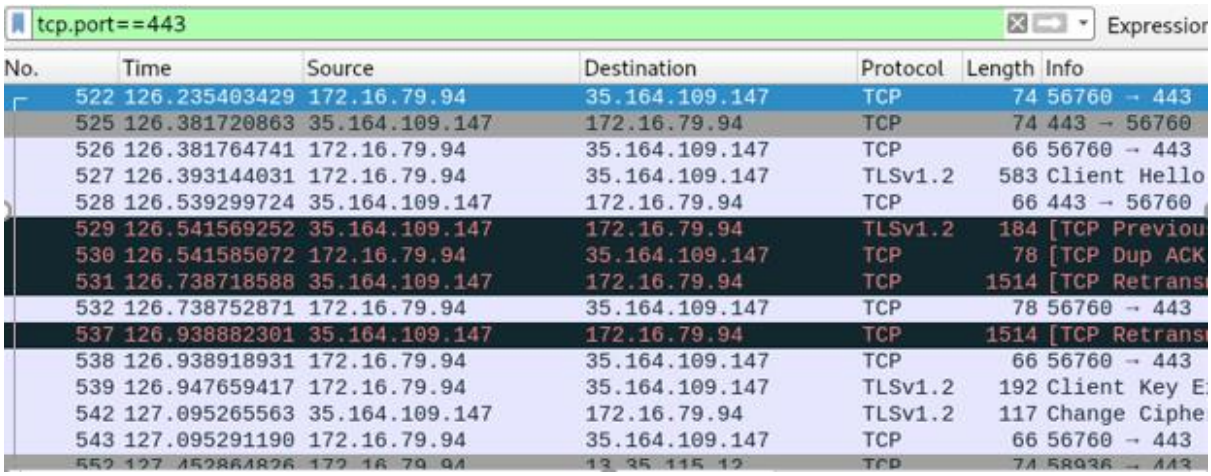
File Edit View Go Capture Analyze Statistics Telephony Wireless To
Options... Ctrl+K
Start Ctrl+E
Stop Ctrl+E
Restart Ctrl+R
Capture Filters...
Refresh Interfaces F5
Apply a display filter ...
Welcome
Capture
...using this filter: Enter a capture filter ...
eth0

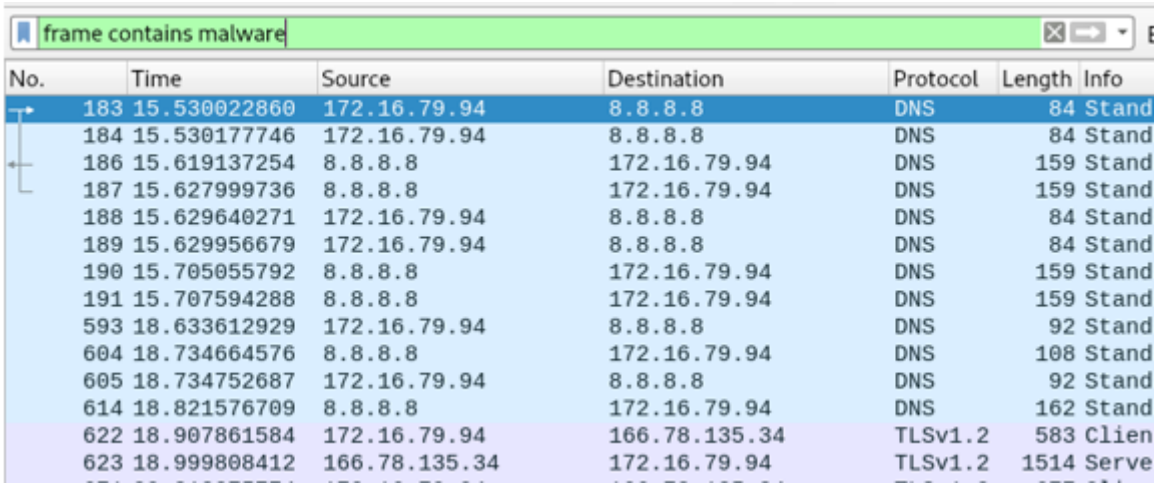

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
931 95.038981285 10.10.0.1 255.255.255.255 DHCP 345 DHCP Offer - Transa
932 95.068952624 10.10.133.231 10.10.255.255 NBNS 92 Name query NB COSTAATT
933 95.184934958 Cisco_04:23:e1 Broadcast ARP 60 Who has 10.10.106.106?
934 95.267707630 Cisco_16:7c:d6 Broadcast ARP 60 Who has 172.21.0.1? Te
935 95.798717074 Cisco_5b:ef:a3 PVST+ STP 64 Conf. Root = 32768/3/0
936 96.040258313 Cisco_5b:ef:a3 PVST+ STP 64 Conf. Root = 32768/2/0
937 96.206479762 fe80::e957:af2f:cbc… ff02::1:fff3:89ca ICMPv6 86 Neighbor Solicitation
938 96.461017729 fe80::bcb3:6397:509… ff02::1:3 LLMNR 89 Standard query 0x3e61
939 96.461089321 10.10.128.121 224.0.0.252 LLMNR 69 Standard query 0x3e61
940 96.461362688 fe80::bcb3:6397:509… ff02::1:3 LLMNR 89 Standard query 0xa249
941 96.464195084 fe80::bcb3:6397:509… ff02::1:fff3:d910 ICMPv6 86 Neighbor Solicitation
942 96.548288483 10.10.123.48 10.10.255.255 NBNS 92 Name query NB NPIA6A25
943 96.672856564 10.10.1.79 10.10.255.255 NBNS 92 Name query NB COSTAATT
944 96.843455684 fe80::e957:af2f:cbc… ff02::1:fff3:89ca ICMPv6 86 Neighbor Solicitation
945 97.264142480 Dell_8b:ff:f9 Broadcast ARP 60 Who has 10.10.0.58? Te
Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface eth0, id 0
Ethernet II, Src: Elitegro_7c:ad:3e (c0:3f:d5:7c:ad:3e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 10.10.123.48, Dst: 10.10.255.255
0000 ff ff ff ff ff ff c0 3f d5 7c ad 3e 08 00 45 00 ·····? ·|·>··E·
0010 00 4e 64 21 00 00 80 11 47 3a 0a 0a 7b 30 0a 0a ·Nd!···· G:··{0··
0020 ff ff 00 89 00 89 00 3a 1a af f3 00 01 10 00 01 ·····: ·····
0030 00 00 00 00 00 00 20 45 4f 46 41 45 4a 45 42 44 ····· E OFAEJEBD
0040 47 45 42 44 43 44 46 45 47 43 41 43 41 43 41 43 GEBDCDFE GCACACAC
0050 41 43 41 43 41 41 41 00 00 20 00 01 ACACAAA· · ··

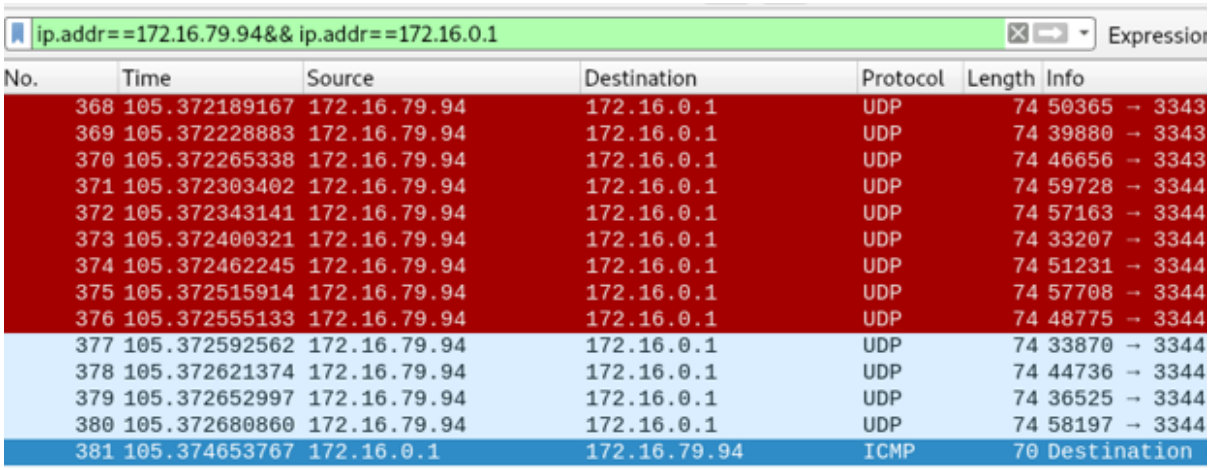

File Edit View

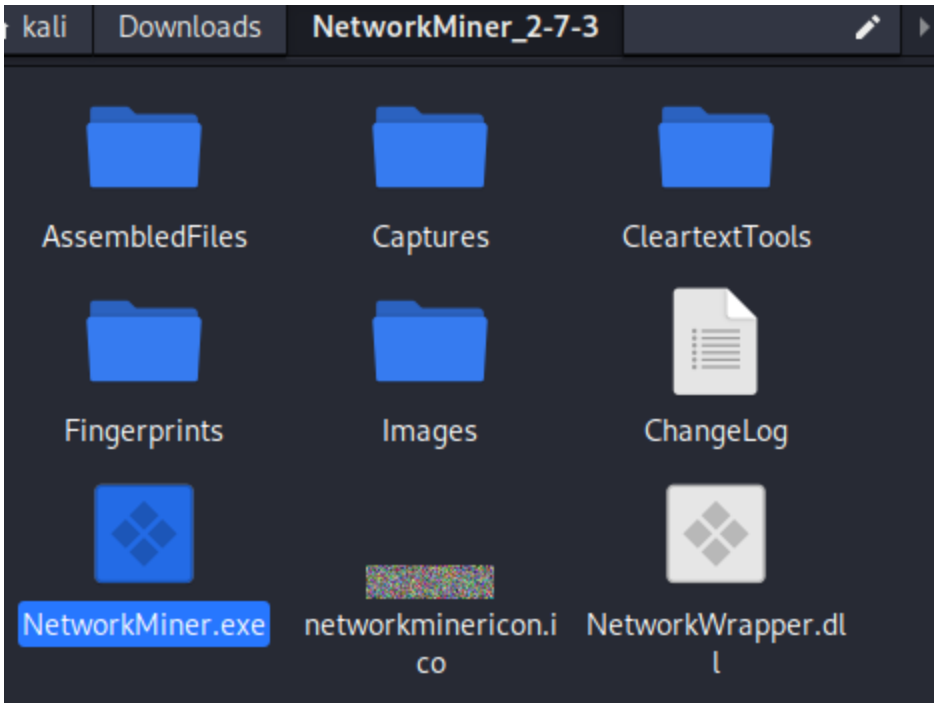

Wireshark · Save Capture File As
Look in:
/home/kali/Downloads
Computer
root
Name
Size
Type
Date Modified
RamCapturer
Folder
10/27/...:53 AM
File name:
CFSI traffic
Save
Cancel
Save as:
Wireshark/... - pcapng
Help
Compress with gzip

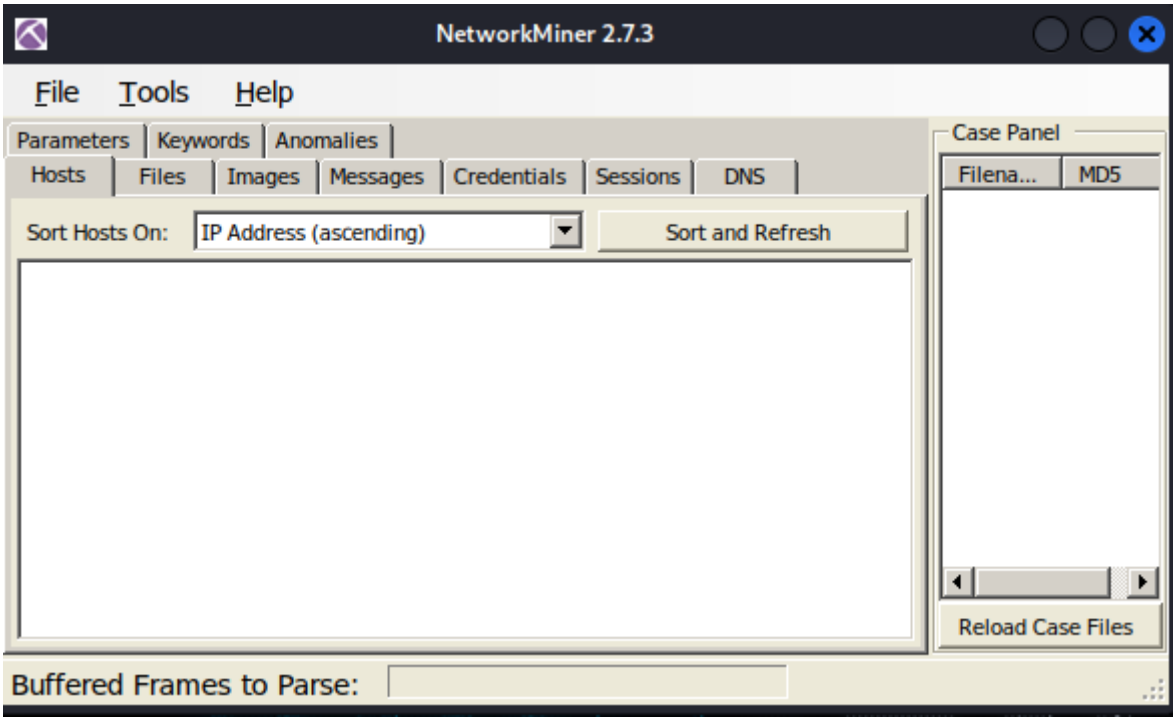

ip.addr==172.16.79.21
Expression...
No. Time Source Destination Protocol Length Info
5 2.343222247 172.16.79.21 239.255.255.250 SSDP 164 M-SEARCH * HTTP
6 2.346631668 172.16.79.21 239.255.255.250 SSDP 167 M-SEARCH * HTTP
8 4.349212714 172.16.79.21 239.255.255.250 SSDP 167 M-SEARCH * HTTP
9 4.351211535 172.16.79.21 239.255.255.250 SSDP 164 M-SEARCH * HTTP
10 5.326277904 172.16.79.21 224.0.0.251 MDNS 103 Standard query
11 6.346576806 172.16.79.21 239.255.255.250 SSDP 167 M-SEARCH * HTTP
12 6.349880265 172.16.79.21 239.255.255.250 SSDP 164 M-SEARCH * HTTP
35 13.806779764 172.16.79.21 239.255.255.250 IGMPv2 60 Membership Repo

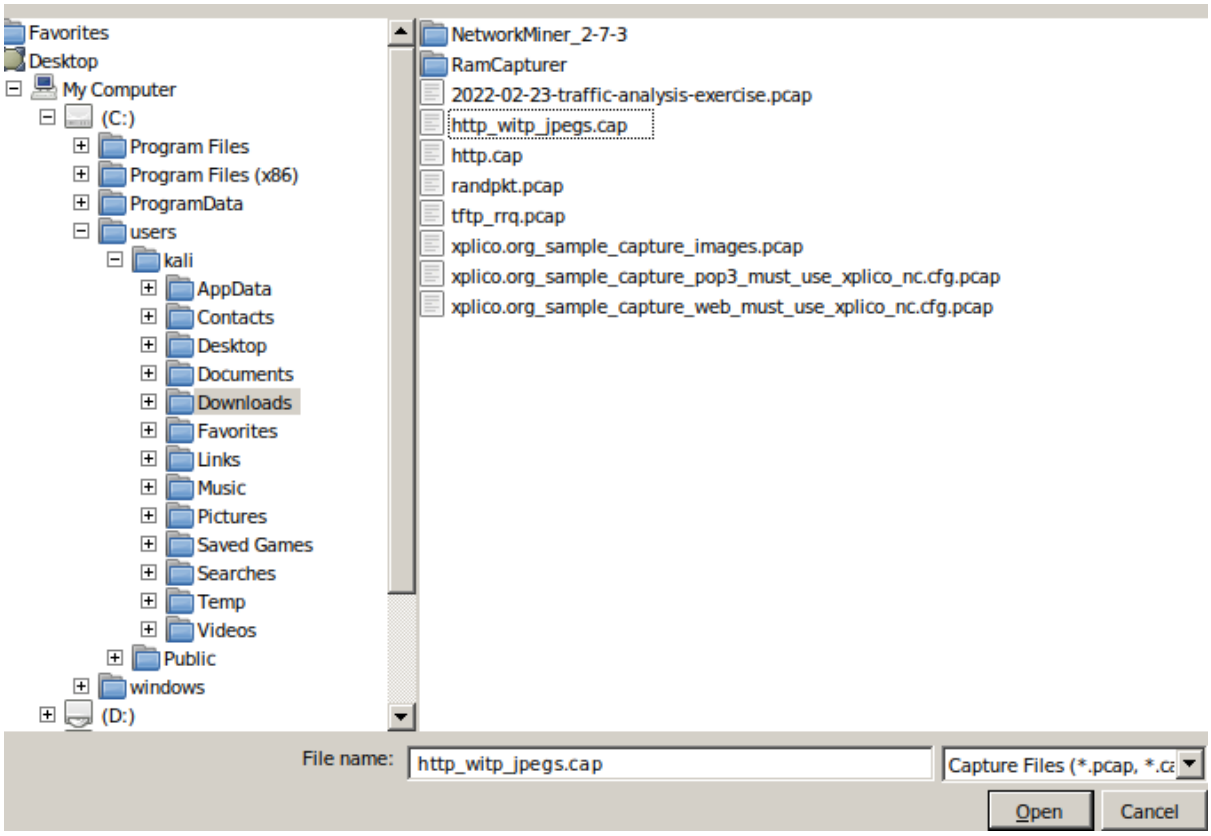

tcp.port==443
Expressior
No. Time Source Destination Protocol Length Info
522 126.235403429 172.16.79.94 35.164.109.147 TCP 74 56760 → 443
525 126.381720863 35.164.109.147 172.16.79.94 TCP 74 443 → 56760
526 126.381764741 172.16.79.94 35.164.109.147 TCP 66 56760 → 443
527 126.393144031 172.16.79.94 35.164.109.147 TLSv1.2 583 Client Hello
528 126.539299724 35.164.109.147 172.16.79.94 TCP 66 443 → 56760
529 126.541569252 35.164.109.147 172.16.79.94 TLSv1.2 184 [TCP Previou
530 126.541585072 172.16.79.94 35.164.109.147 TCP 78 [TCP Dup ACK
531 126.738718588 35.164.109.147 172.16.79.94 TCP 1514 [TCP Retrans
532 126.738752871 172.16.79.94 35.164.109.147 TCP 78 56760 → 443
537 126.938882301 35.164.109.147 172.16.79.94 TCP 1514 [TCP Retrans
538 126.938918931 172.16.79.94 35.164.109.147 TCP 66 56760 → 443
539 126.947659417 172.16.79.94 35.164.109.147 TLSv1.2 192 Client Key E
542 127.095265563 35.164.109.147 172.16.79.94 TLSv1.2 117 Change Ciphe
543 127.095291190 172.16.79.94 35.164.109.147 TCP 66 56760 → 443

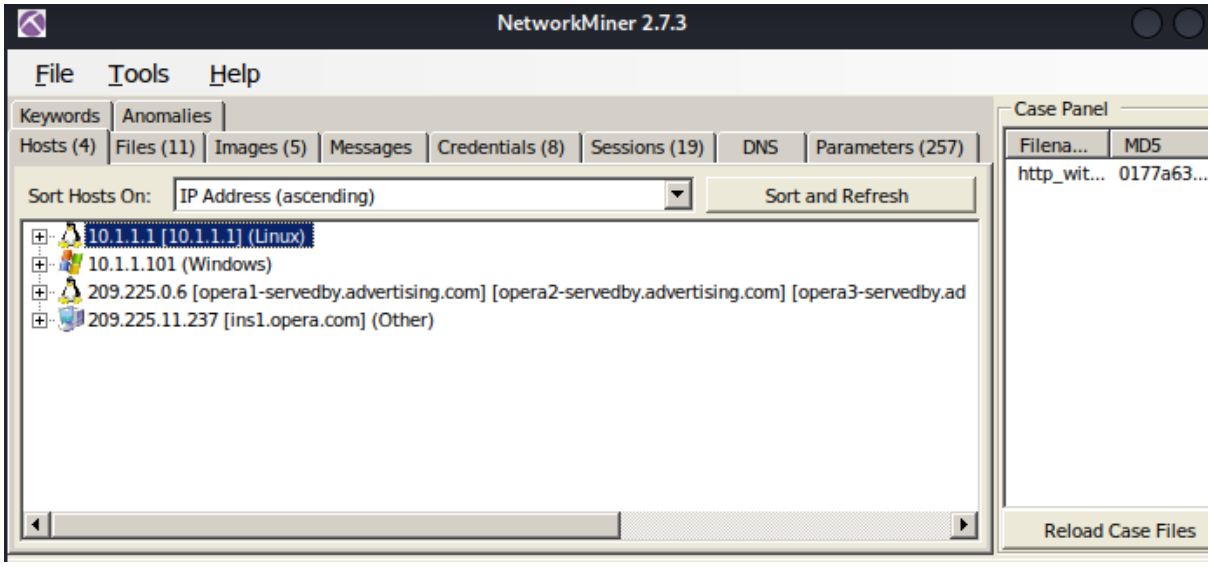

frame contains malware
No. Time Source Destination Protocol Length Info
183 15.530022860 172.16.79.94 8.8.8.8 DNS 84 Stand
184 15.530177746 172.16.79.94 8.8.8.8 DNS 84 Stand
186 15.619137254 8.8.8.8 172.16.79.94 DNS 159 Stand
187 15.627999736 8.8.8.8 172.16.79.94 DNS 159 Stand
188 15.629640271 172.16.79.94 8.8.8.8 DNS 84 Stand
189 15.629956679 172.16.79.94 8.8.8.8 DNS 84 Stand
190 15.705055792 8.8.8.8 172.16.79.94 DNS 159 Stand
191 15.707594288 8.8.8.8 172.16.79.94 DNS 159 Stand
593 18.633612929 172.16.79.94 8.8.8.8 DNS 92 Stand
604 18.734664576 8.8.8.8 172.16.79.94 DNS 108 Stand
605 18.734752687 172.16.79.94 8.8.8.8 DNS 92 Stand
614 18.821576709 8.8.8.8 172.16.79.94 DNS 162 Stand
622 18.907861584 172.16.79.94 166.78.135.34 TLSv1.2 583 Clien
623 18.999808412 166.78.135.34 172.16.79.94 TLSv1.2 1514 Serve

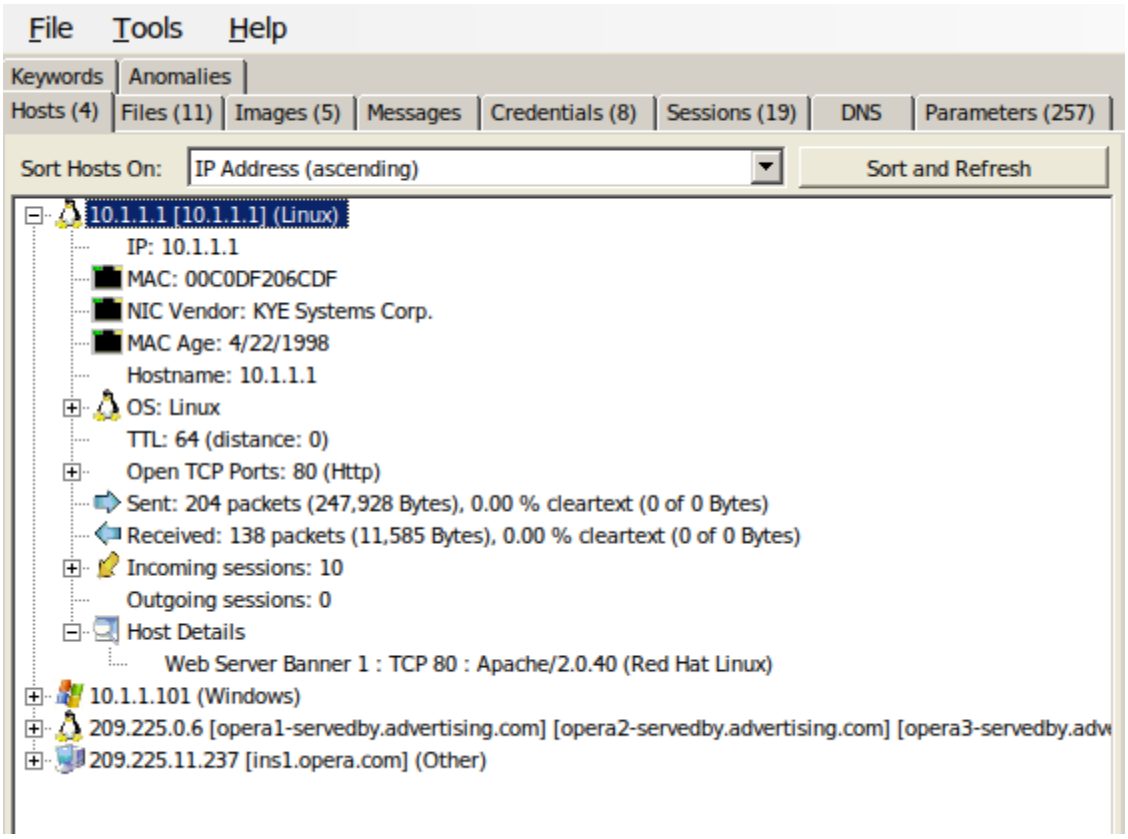

ip.addr==172.16.79.94&& ip.addr==172.16.0.1
Expressio
No. Time Source Destination Protocol Length Info
368 105.372189167 172.16.79.94 172.16.0.1 UDP 74 50365 → 3343
369 105.372228883 172.16.79.94 172.16.0.1 UDP 74 39880 → 3343
370 105.372265338 172.16.79.94 172.16.0.1 UDP 74 46656 → 3343
371 105.372303402 172.16.79.94 172.16.0.1 UDP 74 59728 → 3344
372 105.372343141 172.16.79.94 172.16.0.1 UDP 74 57163 → 3344
373 105.372400321 172.16.79.94 172.16.0.1 UDP 74 33207 → 3344
374 105.372462245 172.16.79.94 172.16.0.1 UDP 74 51231 → 3344
375 105.372515914 172.16.79.94 172.16.0.1 UDP 74 57708 → 3344
376 105.372555133 172.16.79.94 172.16.0.1 UDP 74 48775 → 3344
377 105.372592562 172.16.79.94 172.16.0.1 UDP 74 33870 → 3344
378 105.372621374 172.16.79.94 172.16.0.1 UDP 74 44736 → 3344
379 105.372652997 172.16.79.94 172.16.0.1 UDP 74 36525 → 3344
380 105.372680860 172.16.79.94 172.16.0.1 UDP 74 58197 → 3344
381 105.374653767 172.16.0.1 172.16.79.94 ICMP 70 Destination


kali
Downloads
NetworkMiner_2-7-3
AssembledFiles
Captures
CleartextTools
Fingerprints
Images
ChangeLog
NetworkMiner.exe
networkminericon.ico
NetworkWrapper.dll


NetworkMiner 2.7.3
File
Tools
Help
Parameters
Keywords
Anomalies
Hosts
Files
Images
Messages
Credentials
Sessions
DNS
Sort Hosts On:
IP Address (ascending)
Sort and Refresh
Case Panel
Filena...
MD5
Reload Case Files
Buffered Frames to Parse:


Favorites
Desktop
My Computer
(C:)
Program Files
Program Files (x86)
ProgramData
users
kali
AppData
Contacts
Desktop
Documents
Downloads
Favorites
Links
Music
Pictures
Saved Games
Searches
Temp
Videos
Public
windows
(D:)
NetworkMiner_2-7-3
RamCapturer
2022-02-23-traffic-analysis-exercise.pcap
http_witp_jpegs.cap
http.cap
randpkt.pcap
tftp_rrq.pcap
xplico.org_sample_capture_images.pcap
xplico.org_sample_capture_pop3_must_use_xplico_nc.cfg.pcap
xplico.org_sample_capture_web_must_use_xplico_nc.cfg.pcap
File name:
http_witp_jpegs.cap
Capture Files (*.pcap, *.ca
Open
Cancel


NetworkMiner 2.7.3
File Tools Help
Keywords Anomalies
Hosts (4) Files (11) Images (5) Messages Credentials (8) Sessions (19) DNS Parameters (257)
Sort Hosts On: IP Address (ascending) Sort and Refresh
10.1.1.1 [10.1.1.1] (Linux)
10.1.1.101 (Windows)
209.225.0.6 [opera1-servedby.advertising.com] [opera2-servedby.advertising.com] [opera3-servedby.ad
209.225.11.237 [ins1.opera.com] (Other)
Case Panel
Filena... MD5
http_wit... 0177a63...
Reload Case Files


File Tools Help
Keywords Anomalies
Hosts (4) Files (11) Images (5) Messages Credentials (8) Sessions (19) DNS Parameters (257)
Sort Hosts On: IP Address (ascending) Sort and Refresh
10.1.1.1 [10.1.1.1] (Linux)
IP: 10.1.1.1
MAC: 00C0DF206CDF
NIC Vendor: KYE Systems Corp.
MAC Age: 4/22/1998
Hostname: 10.1.1.1
OS: Linux
TTL: 64 (distance: 0)
Open TCP Ports: 80 (Http)
Sent: 204 packets (247,928 Bytes), 0.00 % cleartext (0 of 0 Bytes)
Received: 138 packets (11,585 Bytes), 0.00 % cleartext (0 of 0 Bytes)
Incoming sessions: 10
Outgoing sessions: 0
Host Details
Web Server Banner 1 : TCP 80 : Apache/2.0.40 (Red Hat Linux)
10.1.1.101 (Windows)
209.225.0.6 [opera1-servedby.advertising.com] [opera2-servedby.advertising.com] [opera3-servedby.adv
209.225.11.237 [ins1.opera.com] (Other)

Hosts (4) | Files (11) | Images (5) | Messages | Credentials (8) | Sessions (19) | DNS | Parameters (257) | Keywords | Anomalies

Filter keyword: Case sensitive ExactPhrase Any column Clear Apply

Frame ...	Filename	Extens...	Size	Source host	S. port	Destination host
4	index.html	html	160 B	10.1.1.1 [10.1.1.1] (Linux)	TCP 80	10.1.1.101 (Windows)
16	xcms.asp.vnd.xacp	xacp	433 B	10.1.1.101 (Windows)	TCP 3179	209.225.11.237 [ins1.opera.com] (Other
31	index.html	html	4 323 B	10.1.1.1 [10.1.1.1] (Linux)	TCP 80	10.1.1.101 (Windows)
48	bg2.jpg	jpg	8 281 B	10.1.1.1 [10.1.1.1] (Linux)	TCP 80	10.1.1.101 (Windows)
50	sydney.jpg	jpg	9 045 B	10.1.1.1 [10.1.1.1] (Linux)	TCP 80	10.1.1.101 (Windows)
157	dagbok.html	html	416 B	10.1.1.1 [10.1.1.1] (Linux)	TCP 80	10.1.1.101 (Windows)
215	dagbok.html	html	1 263 B	10.1.1.1 [10.1.1.1] (Linux)	TCP 80	10.1.1.101 (Windows)
227	dagbok.html	html	2 232 B	10.1.1.1 [10.1.1.1] (Linux)	TCP 80	10.1.1.101 (Windows)
240	DSC07858.JPG	jpg	8 963 B	10.1.1.1 [10.1.1.1] (Linux)	TCP 80	10.1.1.101 (Windows)
241	DSC07859.JPG	jpg	10 730 B	10.1.1.1 [10.1.1.1] (Linux)	TCP 80	10.1.1.101 (Windows)
278	DSC07858.JPG	jpg	191 515 B	10.1.1.1 [10.1.1.1] (Linux)	TCP 80	10.1.1.101 (Windows)

File Tools Help

Hosts (4) | Files (11) | Images (5) | Messages | Credentials (8) | Sessions (19) | DNS | Parameters (257) | Keywords


bg2.jpg
512x512, 8 281 B


sydney.jpg
500x89, 9 045 B


DSC07858.JPG
180x240, 8 963 B


DSC07859.JPG
180x240, 10 730 B


DSC07858.JPG
960x1280, 191 515 B

```
┌──(kali㉿kali)-[~]
└─$ sudo git clone https://github.com/Srinivas11789/PcapXray.git
[sudo] password for kali:
Cloning into 'PcapXray' ...
remote: Enumerating objects: 1704, done.
remote: Counting objects: 100% (15/15), done.
remote: Compressing objects: 100% (11/11), done.
remote: Total 1704 (delta 3), reused 9 (delta 2), pack-reused 1689
Receiving objects: 100% (1704/1704), 115.75 MiB | 1.14 MiB/s, done.
Resolving deltas: 100% (975/975), done.
```

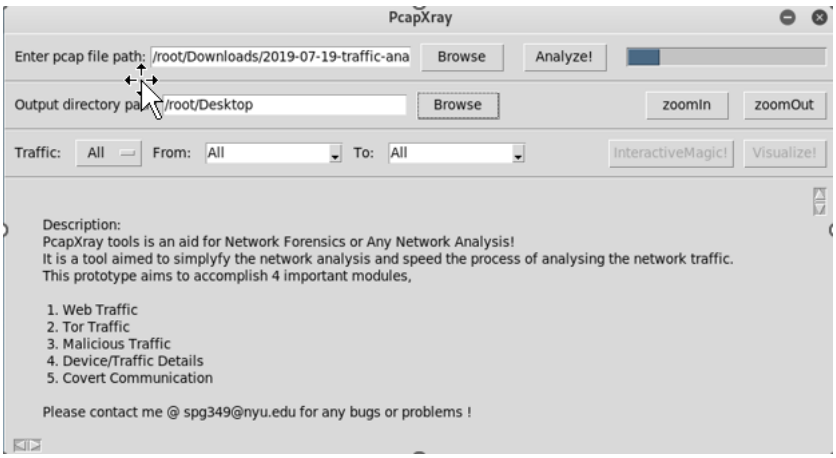
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install graphviz
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
```

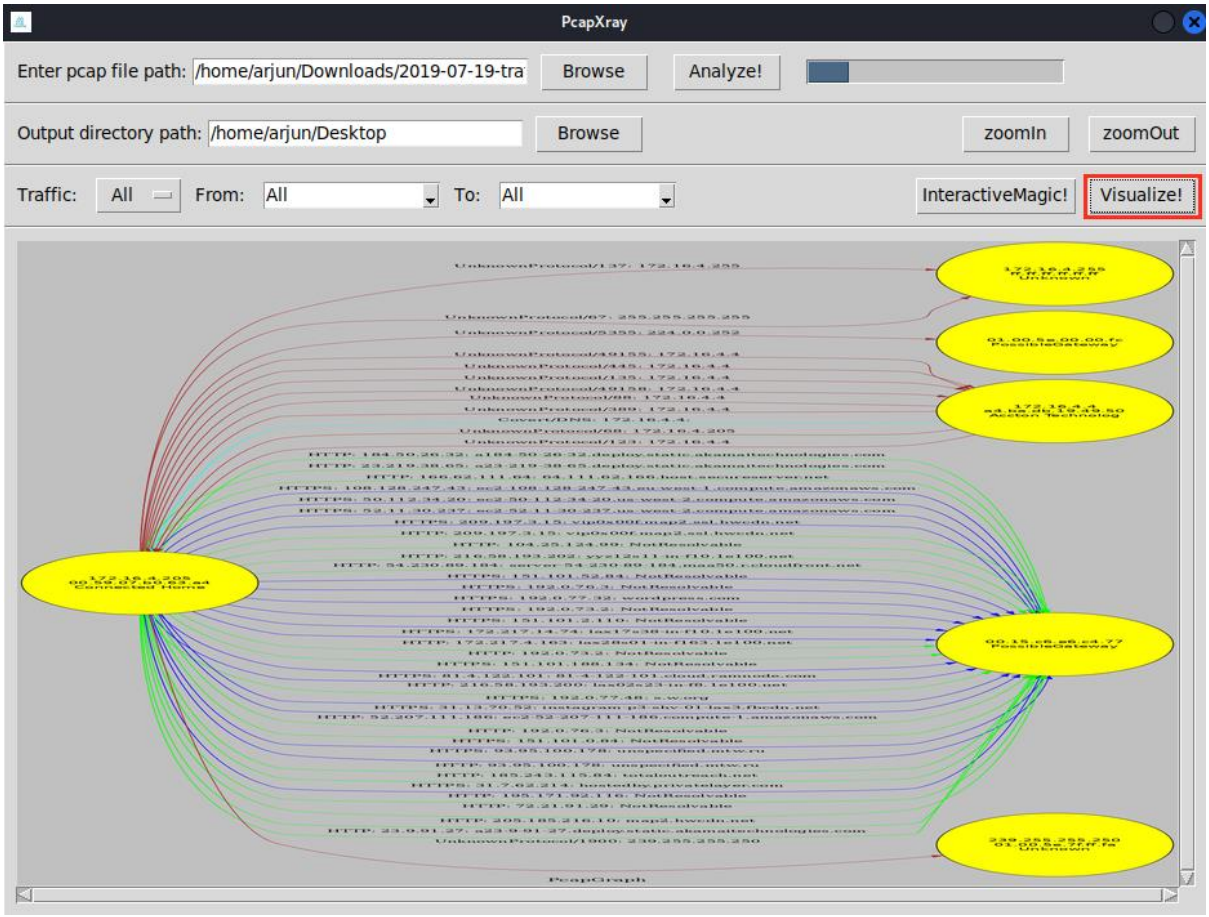
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install python3-pil python3-pil.imagetk
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  libev4 libfmt8 libhttp-server-simple-perl libilmbase25 liblerc3 libopenexr25
  libpoppler118 libpython3.9-minimal libpython3.9-stdlib libsvtav1enc0 libwebsockets16
  linux-image-5.18.0-kali5-amd64 python3-dataclasses-json python3-limiter
  python3-marshmallow-enum python3-mypy-extensions python3-responses python3-spyse
  python3-token-bucket python3-typing-inspect python3.9 python3.9-minimal
```

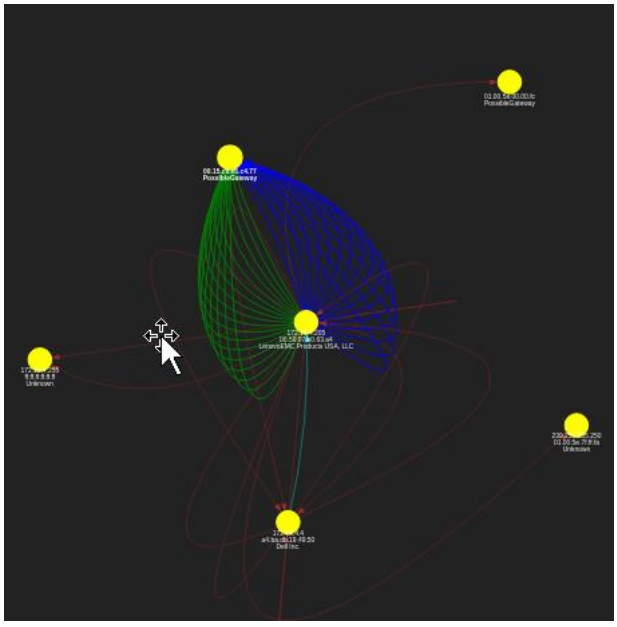
```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop    Downloads   Music     Pictures  Templates  Videos
Documents  get-pip.py  PcapXray  Public    tmp

┌──(kali㉿kali)-[~]
└─$ cd PcapXray

┌──(kali㉿kali)-[~/PcapXray]
└─$ ls
_config.yml  Dockerfile  logo.png   requirements.txt  Samples  Test
Design       LICENSE     README.md  run.sh            Source
```

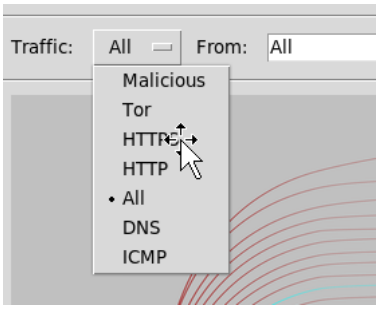
```
┌──(kali㉿kali)-[~/PcapXray]
└─$ pip3 install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: scapy in /usr/lib/python3/dist-packages (from -r requirem
ents.txt (line 4)) (2.4.5+g9420c22)
Collecting pyshark
  Downloading pyshark-0.5.3-py3-none-any.whl (41 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 41.1/41.1 kB 398.6 kB/s eta 0:00:00
Requirement already satisfied: ipwhois in /usr/lib/python3/dist-packages (from -r requir
ements.txt (line 12)) (0.15.1)
```

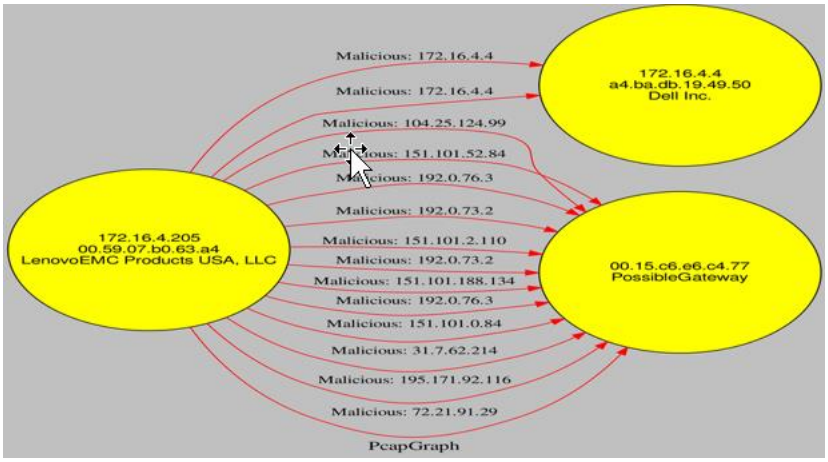
```
┌──(kali㉿kali)-[~/PcapXray]
└─$ python3 Source/main.py
```

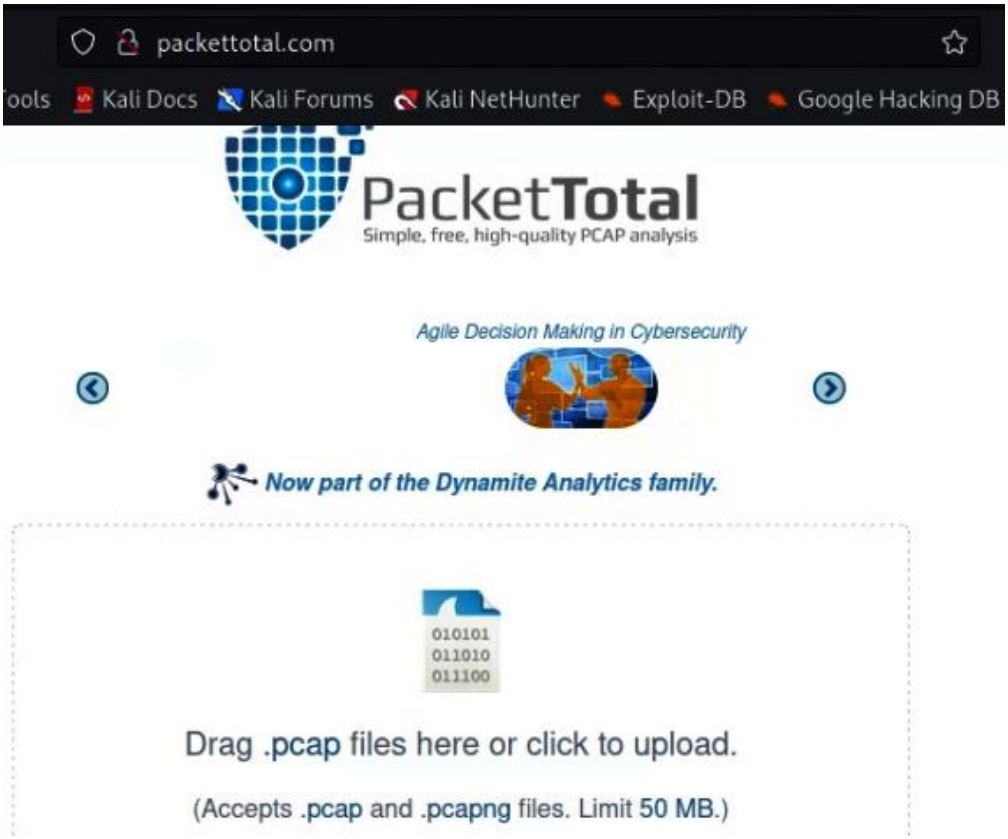


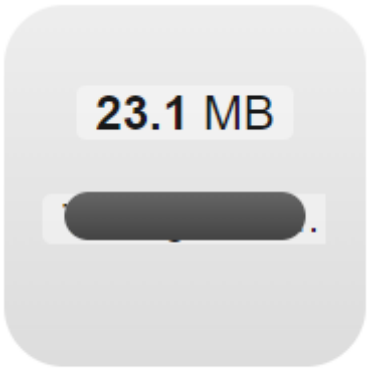

PcapXray
Enter pcap file path: /home/arjun/Downloads/2019-07-19-tra
Browse
Analyze!
Output directory path: /home/arjun/Desktop
Browse
zoomIn
zoomOut
Traffic:
All
From:
All
To:
All
InteractiveMagic!
Visualize!
PcapGraph

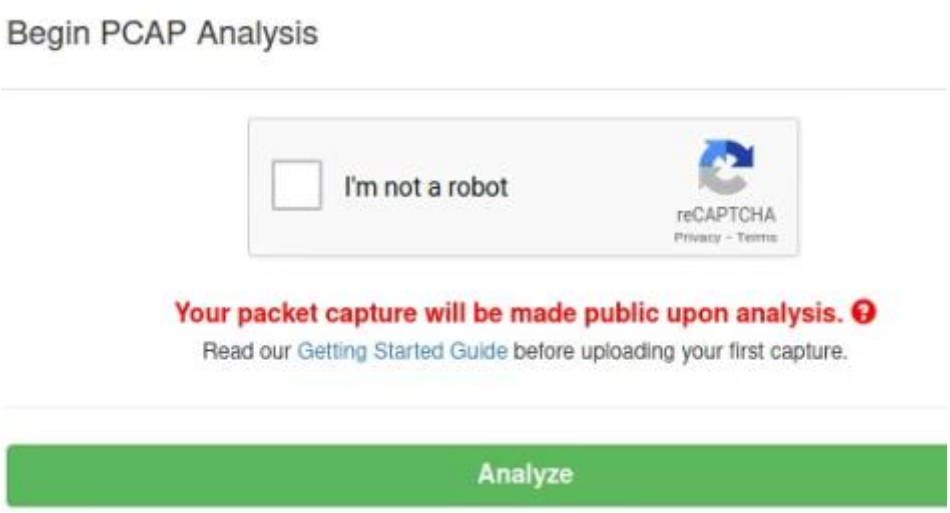



Traffic:
All
From:
All
Malicious
Tor
HTTPS
HTTP
All
DNS
ICMP


Malicious: 172.16.4.4
Malicious: 172.16.4.4
Malicious: 104.25.124.99
Malicious: 151.101.52.84
Malicious: 192.0.76.3
Malicious: 192.0.73.2
Malicious: 151.101.2.110
Malicious: 192.0.73.2
Malicious: 151.101.188.134
Malicious: 192.0.76.3
Malicious: 151.101.0.84
Malicious: 31.7.62.214
Malicious: 195.171.92.116
Malicious: 72.21.91.29
172.16.4.4
a4.ba.db.19.49.50
Dell Inc.
172.16.4.205
00.59.07.b0.63.a4
LenovoEMC Products USA, LLC
00.15.c6.e6.c4.77
PossibleGateway
PcapGraph


packettotal.com
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
PacketTotal
Simple, free, high-quality PCAP analysis
Agile Decision Making in Cybersecurity
Now part of the Dynamite Analytics family.
010101
011010
011100
Drag .pcap files here or click to upload.
(Accepts .pcap and .pcapng files. Limit 50 MB.)





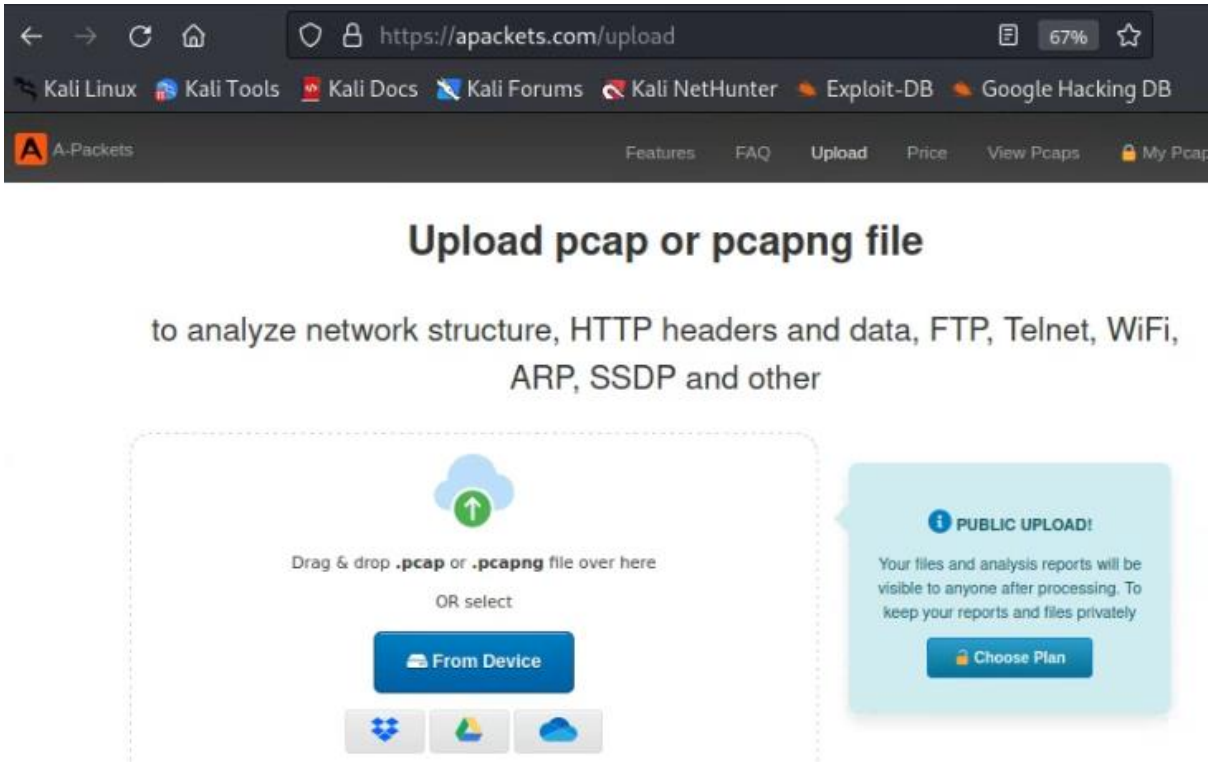
Suspicious Activity | Connections | DHCP | DNS | HTTP | SSL Certificates | PKI (X.509) | Transferred Files | Dynamic Protocol Detection | Strange Activity | Similar Packet Captures

Search in results

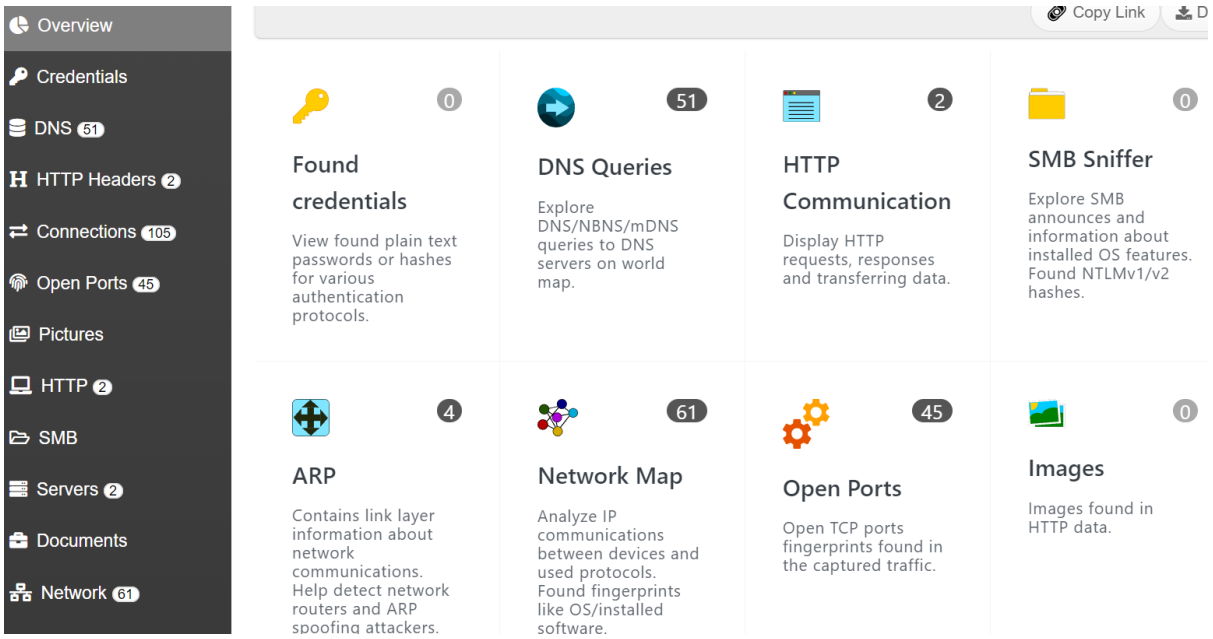
Timestamp	Connection ID	Alert Type	Alert Message	Alert Sub-message	Sender IP	Sender Port	Target IP	Target Port
2022-07-19 14:35:29 Z	null	HTTP::SQL_Injection_Attacker	An SQL injection attacker was discovered!	null	null	null	null	null
2022-07-19 14:35:29 Z	null	HTTP::SQL_Injection_Victim	An SQL injection victim was discovered!	null	null	null	null	null

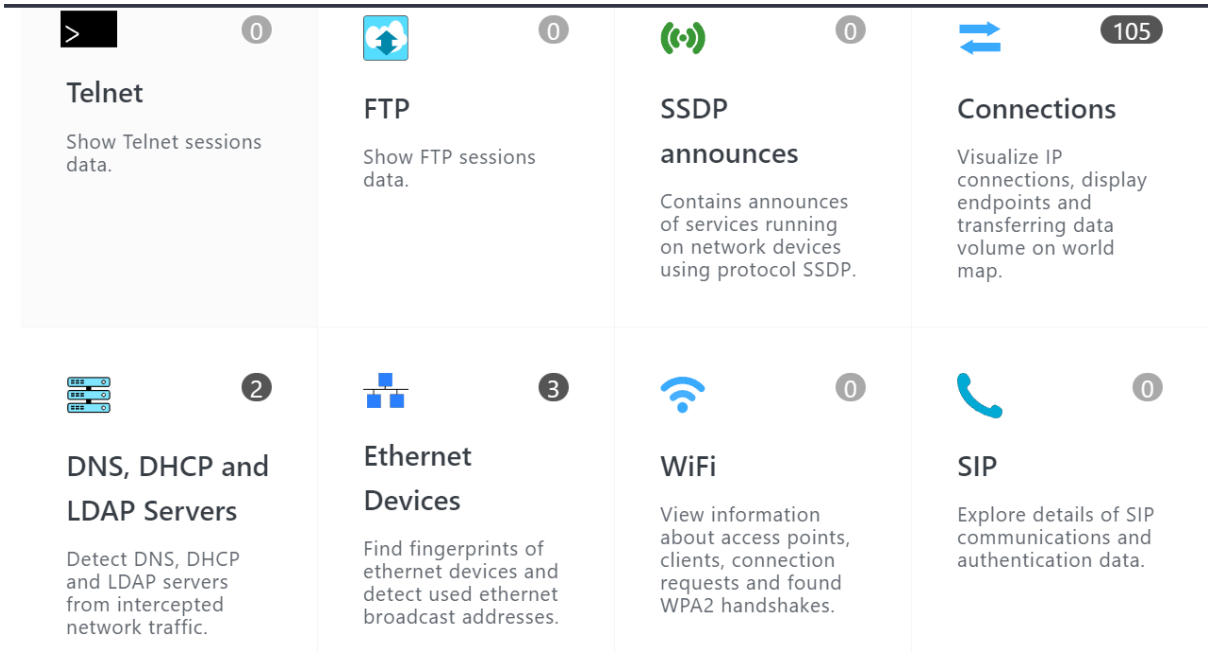
Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port
2022-07-19 14:31:39 Z	CjKhTiYtXfiJypHhh	192.168.0.107	43464	34.120.208.123	443
2022-07-19 14:31:44 Z	C9ALdu4mwoHrXrrzS1	192.168.0.107	50352	192.168.0.1	53
2022-07-19 14:31:44 Z	C4bfnLptmEs2cdaDk	192.168.0.107	41694	192.168.0.1	53
2022-07-19 14:31:44 Z	CAyfHJ3mkRJzmDFsz5	192.168.0.107	34111	192.168.0.1	53
2022-07-19 14:31:44 Z	CvD6Ch274v58IivWbe	192.168.0.107	33979	192.168.0.1	53
2022-07-19 14:31:44 Z	CtL6NN2j2LgQStBkta	192.168.0.107	40948	192.168.0.1	53
2022-07-19 14:31:44 Z	CCLc4h1YfZqh6G9aqd	192.168.0.107	33948	192.168.0.1	53
2022-07-19 14:31:44 Z	CWk7IV2jORbzvbPojd	192.168.0.107	52392	192.168.0.1	53
2022-07-19 14:31:44 Z	CahuXd1EZvgn7TGxUd	192.168.0.107	41469	192.168.0.1	53
2022-07-19 14:31:44 Z	COgVX33g5LuDzfVxSa	192.168.0.107	58661	192.168.0.1	53

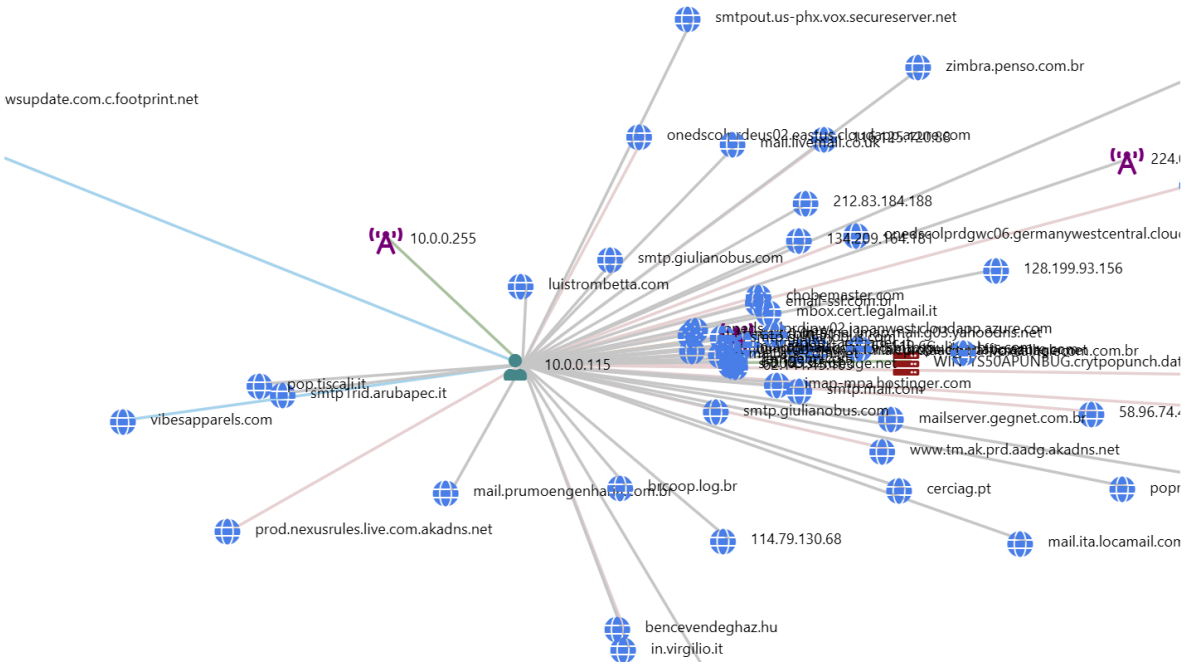
CVEPdp3kiK5C5SO25b	192.168.0.108	5353	224.0.0.251	5353	DNS_RR_unknown_type
CVEPdp3kiK5C5SO25b	192.168.0.108	5353	224.0.0.251	5353	dns_unmatched_reply

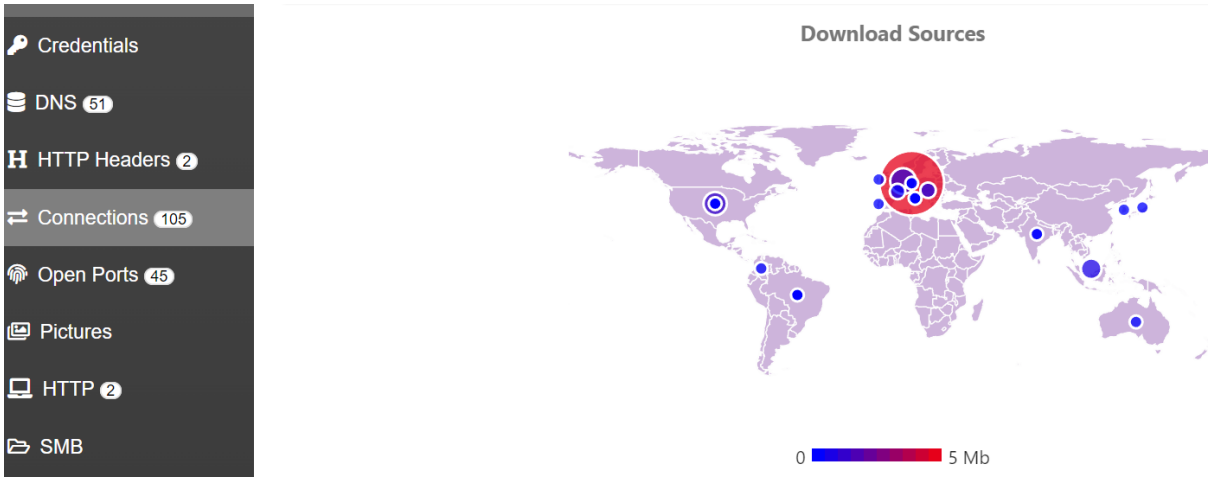


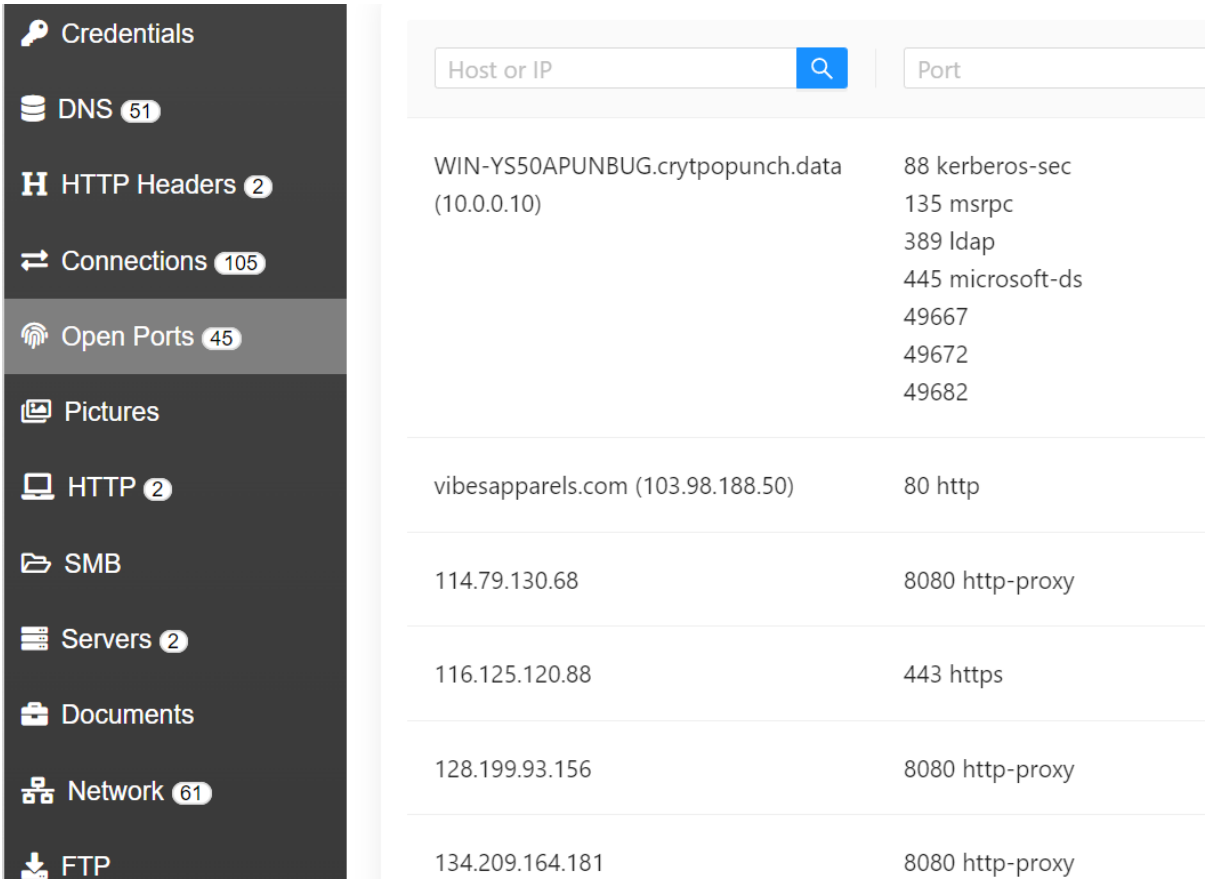
Processing **2022-06-07-Emotet-epoch5-infection-with-Cobalt-Strike-and-spambot-activity.pcap** completed, view report

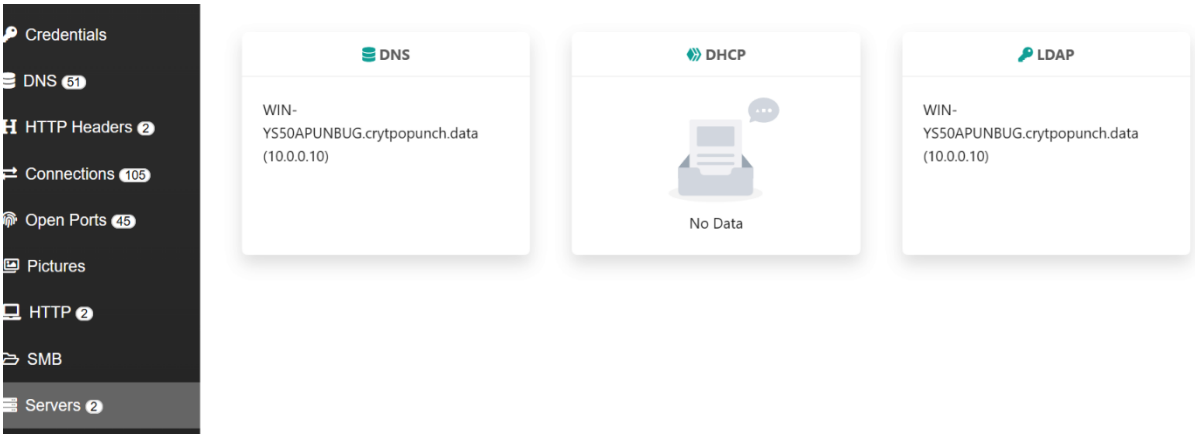





smtpout.us-phx.vox.secureserver.net
zimbra.penso.com.br
wsupdate.com.c.footprint.net
212.83.184.188
10.0.0.255
smtp.giulianobus.com
128.199.93.156
luistrombetta.com
mbox.cert.legalmail.it
10.0.0.115
pop.tiscali.it
smtp1rid.arubapec.it
vibesapparels.com
smtp.giulianobus.com
mailserver.gegnet.com.br
www.tm.ak.prd.aadg.akadns.net
cerciag.pt
mail.prumoengenharia.com.br
brcoop.log.br
prod.nexusrules.live.com.akadns.net
114.79.130.68
mail.ita.locamail.com
bencevendeghaz.hu
in.virgilio.it


Credentials
DNS 51
HTTP Headers 2
Connections 105
Open Ports 45
Pictures
HTTP 2
SMB
Download Sources
0
5 Mb


Credentials
DNS 51
HTTP Headers 2
Connections 105
Open Ports 45
Pictures
HTTP 2
SMB
Servers 2
Documents
Network 61
FTP
Host or IP
Port
WIN-YS50APUNBUG.crytpopunch.data (10.0.0.10)
88 kerberos-sec
135 msrpc
389 ldap
445 microsoft-ds
49667
49672
49682
vibesapparels.com (103.98.188.50)
80 http
114.79.130.68
8080 http-proxy
116.125.120.88
443 https
128.199.93.156
8080 http-proxy
134.209.164.181
8080 http-proxy


Credentials
DNS 51
HTTP Headers 2
Connections 105
Open Ports 45
Pictures
HTTP 2
SMB
Servers 2
DNS
WIN-YS50APUNBUG.crytpopunch.data (10.0.0.10)
DHCP
No Data
LDAP
WIN-YS50APUNBUG.crytpopunch.data (10.0.0.10)

IP	DNS Server	Names
10.0.0.115	WIN-YS50APUNBUG.crytpopunch.data (10.0.0.10)	chobemaster.com bencevendeghaz.hu vibesapparels.com nexusrules.officeapps.live.com v10.events.data.microsoft.com ecs.office.com login.microsoftonline.com self.events.data.microsoft.com wpad.crytpopunch.data Non-Existent Domain WIN-YS50APUNBUG.crytpopunch.data lentgenn.com _ldap._tcp.Default-First-Site-Name._sites.WIN-YS50APUNBUG.CRYPTOPUNCH.DATA Non-Existent Domain _ldap._tcp.WIN-YS50APUNBUG.CRYPTOPUNCH.DATA Non-Existent Domain _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.crytpopunch.data CRYPTOPUNCH.crytpopunch.data Non-Existent Domain settings-win.data.microsoft.com ctldl.windowsupdate.com smtp.pec.aruba.it Non-Existent Domain mail.vermessung-jankowski.de Non-Existent Domain smtp.gegnet.com.br mbox.cert.legalmail.it mail.gmail.com Non-Existent Domain