PRAKTIKUM 10: REPORT INVESTIGATION

Pertemuan ke : 10

Total Alokasi Waktu : 90 menit
- Materi : 15 menit
- Pre-Test : 15 menit
- Praktikum : 45 menit
- Post-Test : 15 menit

Total Skor Penilaian : 100 %
- Pre-Test : 20 %
- Praktik : 30 %
- Post-Test : 50 %

Pemenuhan CPL dan CPMK

CPL-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah
CPMK-04	Mahasiswa mampu membuat report investigator atas penanganan kasus yang melibatkan digital forensik

10.1. TUJUAN DAN INDIKATOR CAPAIAN

Setelah mengikuti praktikum ini mahasiswa diharapkan: (sesuai dengan RPS)
1. Mampu membuat report investigation digital forensik
2. Mampu memaparkan temuan digital evidence

10.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

CPL-07	CPMK-04	Kemampuan mahasiswa dalam menerapkan tempelate pelaporan bukti digital sebagai General Report Tools Investigator

10.3. TEORI PENDUKUNG

Hal terpenting dalam sebuah proses investigasi forensika digital adalah pembuatan laporan. Tentunya karena bersifat resmi dan merujuk pada pedoman penulisan sesuai dengan bahasa awam (agar mudah dimengerti) dan bahasa hukum (untuk melakukan pembuktian), maka beberapa standart penulisan sudah di atur di beberapa negara. salah satunya adalah laporan dari National Institute of Justice, dan juga Standard Operating Procedure 3 tentang pelaporan hasil pemeriksaan digital forensik yang diterbitkan oleh Pusat Laboratorium Forensik Bidang Fisika dan Komputer Forensik.

Pedoman penulisan laporan Digital Forensics

Meskipun bidang Forensik Digital, belakangan ini sudah menjadi tren yang cukup banyak dibicarakan oleh berbagai kalangan, namun masih banyak tugas, pekerjaan dan keterampilan yang perlu di benahi. Salah satunya adalah dalam hal pembuatan laporan. Biar bagaimanapun, meskipun investigasi telah diselesaikan dengan baik. Namun, yang akan berkomnukasi secara umum adalah laporan hasil dari investigasi tersebut.

Analisis yang memukau hanya akan sia-sia bila tidak tepat dalam menyampaikan. Dalam hal ini perlu diketahui bahwa membuat laporan adalah keterampilan yang bisa di asah dan dipelajari.

Berikut ini adalah beberapa hal yang perlu diperhatikan oleh seorang invstigator untuk mempermudah dalam proses pembuatan laporan, yaitu:

1. Jangan menunda pembuatan laporan ; Mulailah laporan Anda, sebelum Anda memulai pemeriksaan Anda. Biasanya ada beberapa informasi yang Anda ketahui sebelum Anda memulai proses pertama penyelidikan. Bahkan walau hanya dengan mengisi nomor seri, informasi kontak, dan meletakkan apa yang Anda ketahui sebelumnya, tidak membuat Anda berhadapan dengan halaman kosong yang menakutkan setelah Anda menyelesaikan proses penyelidikan Anda. Usahakan juga untuk tetap memperbaharui laporan Anda bila melalui langkah demi langkah.
2. Sertakan Analisis ; Jangan hanya melakukan cari dan dan temukan file saja. Namun, biasakan untuk memberikan analisis Anda untuk menambah nilai dari hasil investigasi Anda.
3. Berhati-hati dengan pernyataan "Mutlak" : Jangan menyatakan sesuatu pasti benar, atau tidak pernah terjadi sekalipun Anda meyakini hal tersebut. Karena apabila setelah dilakukan pengujian ternyata menghasilkan kesimpulan yang berlawanan, maka ini bisa menyebabkan kekacauan dalam proses penyelidikan.
4. Membuat Template : Tampelate dapat mempermudah dan menghemat jam kerja. Template juga bisa disesuaikan dengan bahasa dan format standar.

Berikut ini adalah contoh template penyusunan laporan untuk digital forensik yaitu ;

a. Title Page- ini dapat mencakup informasi seperti nama kasus, tanggal, nama penyidik, dan informasi kontak.
b. Table of Contents (ToC)- ini tidak diperlukan untuk laporan singkat. Namun, jika laporan Anda panjang dan / atau pecah menjadi beberapa bagian yang berbeda, TOC termasuk dapat membantu pembaca.
c. Executive Summary – Termasuk penting untuk laporan, ini memungkinkan pembaca untuk mendapatkan tampilan yang mudah dipahami dari temuan penting tanpa harus menyelidiki secara spesifik.
d. Objectives - Bagian ini sangat penting untuk disertakan jika Anda diminta untuk melakukan penyelidikan yang ditargetkan.
e. Evidence Analyzed- ini harus mencakup nomor seri, nilai hash (MD5, SHA, dll), dan informasi jika diketahui. Jika foto itu diambil di tempat kejadian, Anda mungkin bisa melampirkannya di sini.
f. Steps Taken– Rincikanlah. Termasuk perangkat lunak dan perangkat keras yang digunakan. Jangan lupa untuk menyertakan nomor versi.
g. Relevant Findings- membuat sub kategori laporan apabila diperlukan, seperti: Documents of Interest; Internet Activity; Software of Note; USB Devices, dsb.
h. Timeline - sebuah laporan akan lebih baik bila disertakan timeline. Timeline yang baik dapat membantu mengkomunikasikan informasi yang ingin disampaikan oleh seorang investigator.
i. Conclusion - utamakan hal-hal penting, biasanya dalam bentuk daftar temuan secara ringkas
j. Signature - sertakan bagian tanda tangan yang dapat dicetak dan ditandatangani.
k. Exhibits - sertakan bagian tanda tangan yang dapat dicetak dan ditandatangani.

10.4. HARDWARE DAN SOFTWARE

Alat dan bahan yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Autopsy Windows

10.5. PRE-TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

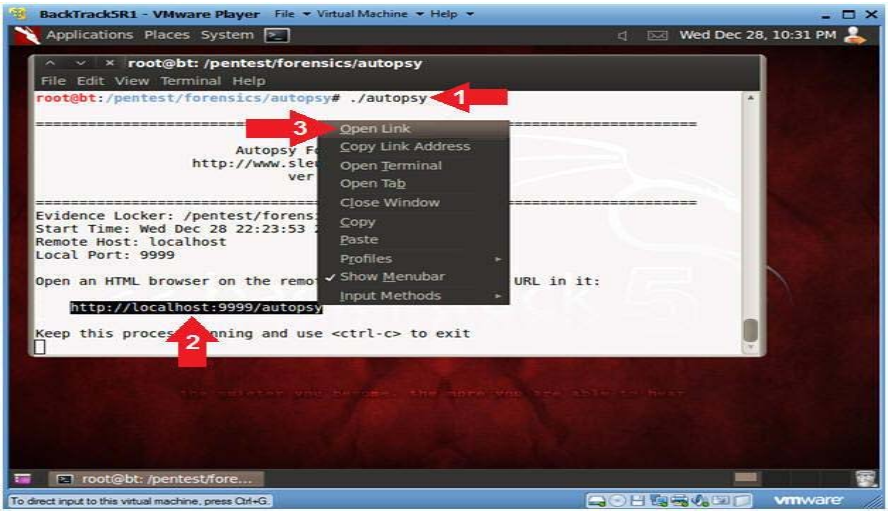
No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-04	Apa tujuan dari dibuatnya report investigation dalam sebuak investigasi digital forensik?	50
2.	CPL-07	CPMK-04	Apa sajo komponen report investigasi terkait 5W+1H?	50

10.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

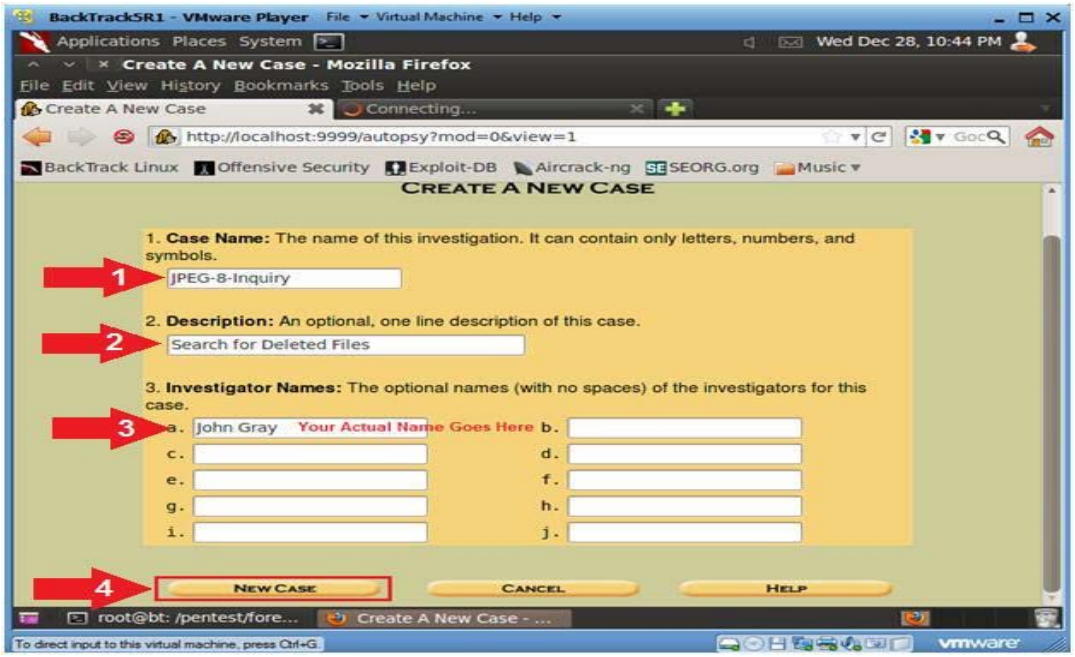
No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-04	Selesaikan langkah praktikum berikut ini!	Screen Shot Hasil praktikum	100

Browser Forensik Autopsy memungkinkan Anda untuk melakukan penyelidikan forensik digital. Ini adalah antarmuka grafis untuk The Sleuth Kit dan alat lainnya. Panduan ini mencakup informasi tentang penggunaan Autopsy versi 3 pada Windows.

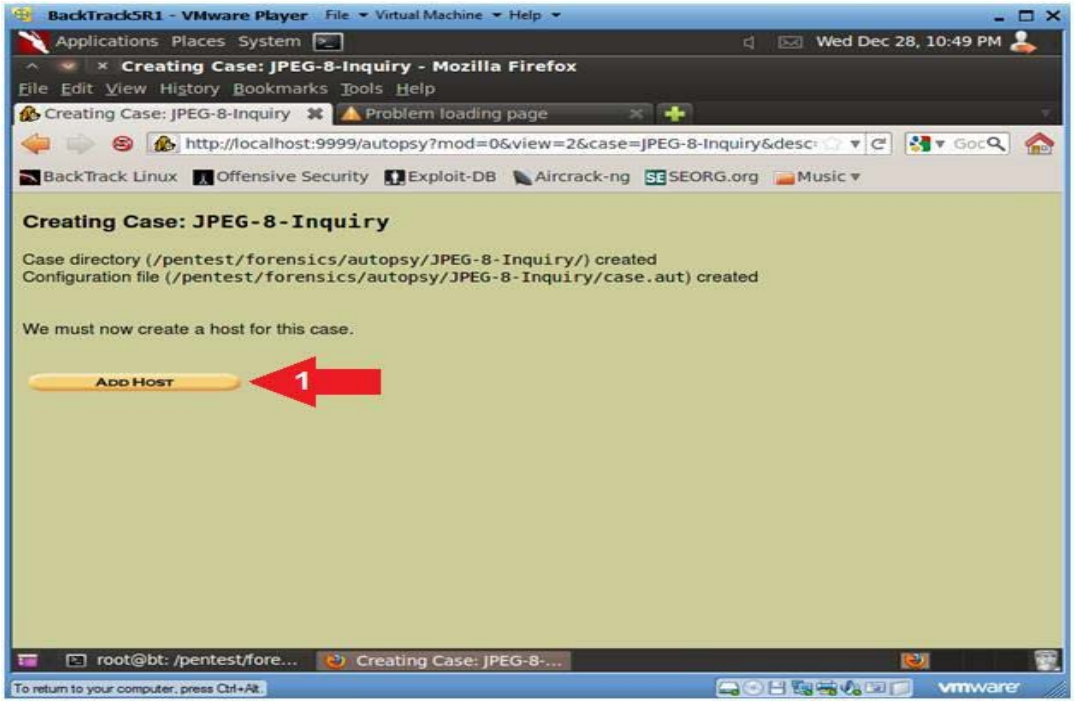


Gambar 10.1 Autopsy Browser.

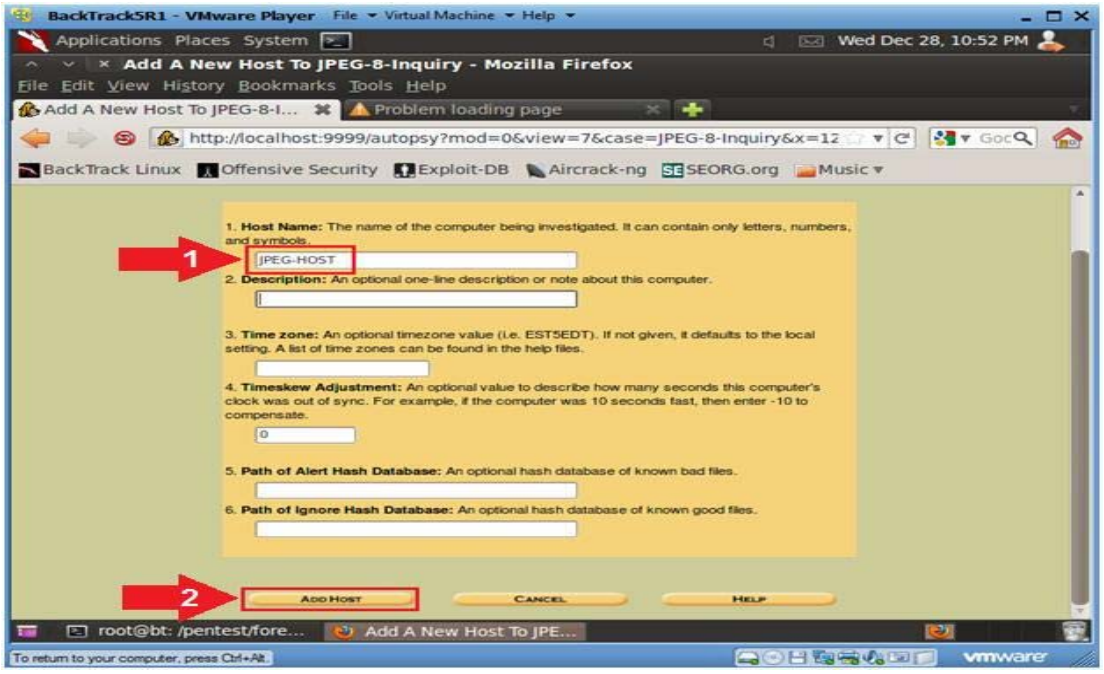
Gambar 10.2 Autopsy New Case.



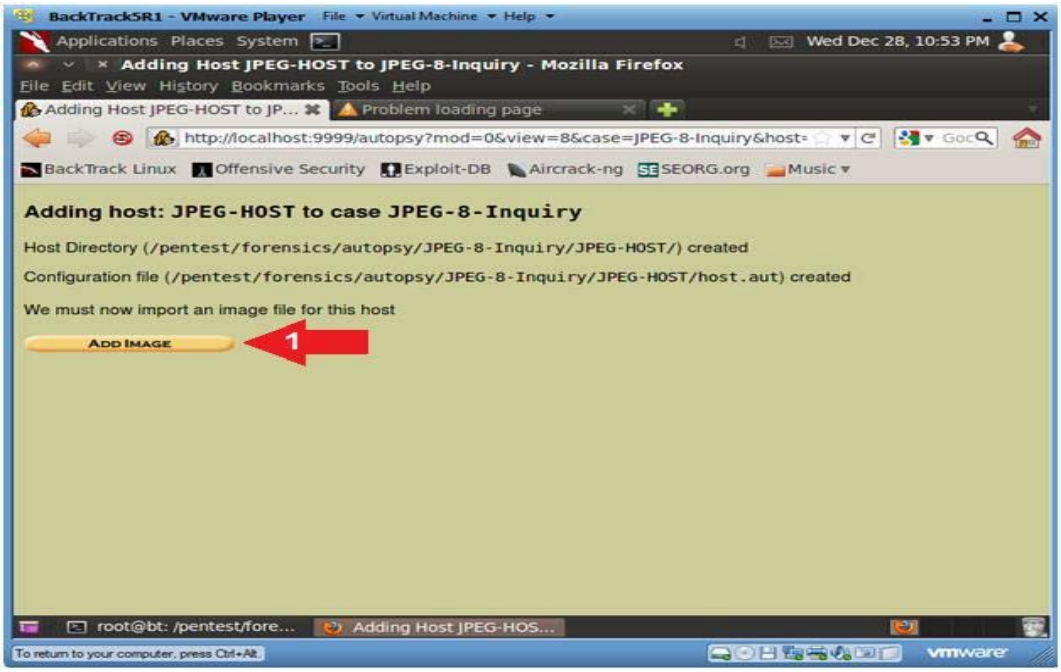
Gambar 10.3 Autopsy Create New Case.



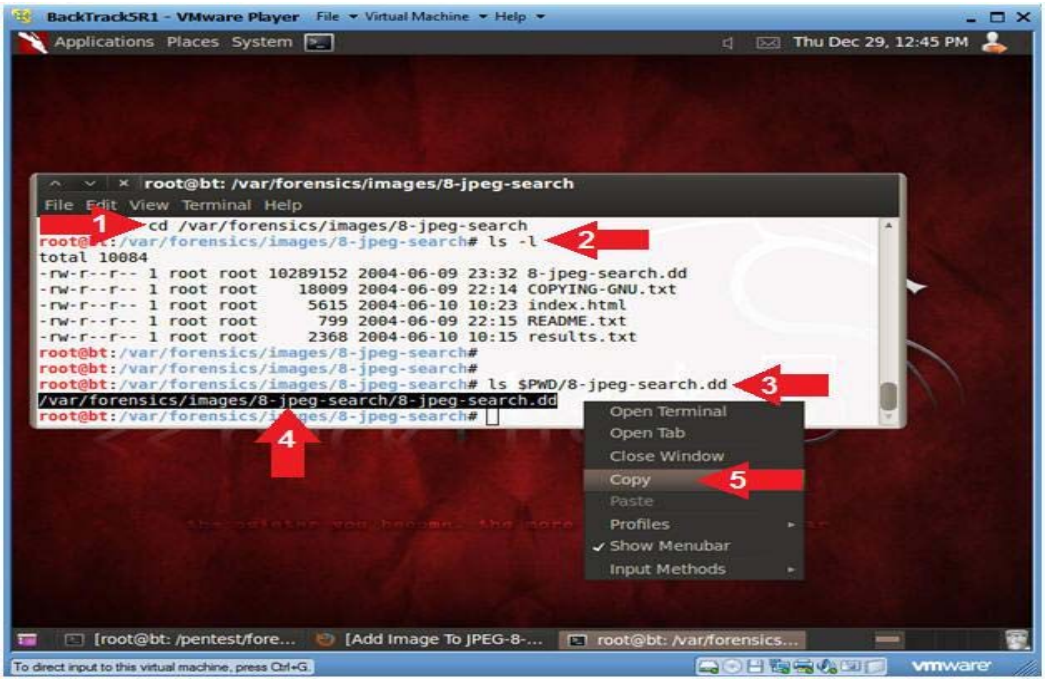
Gambar 10.4 Autopsy Create New Case Sample.



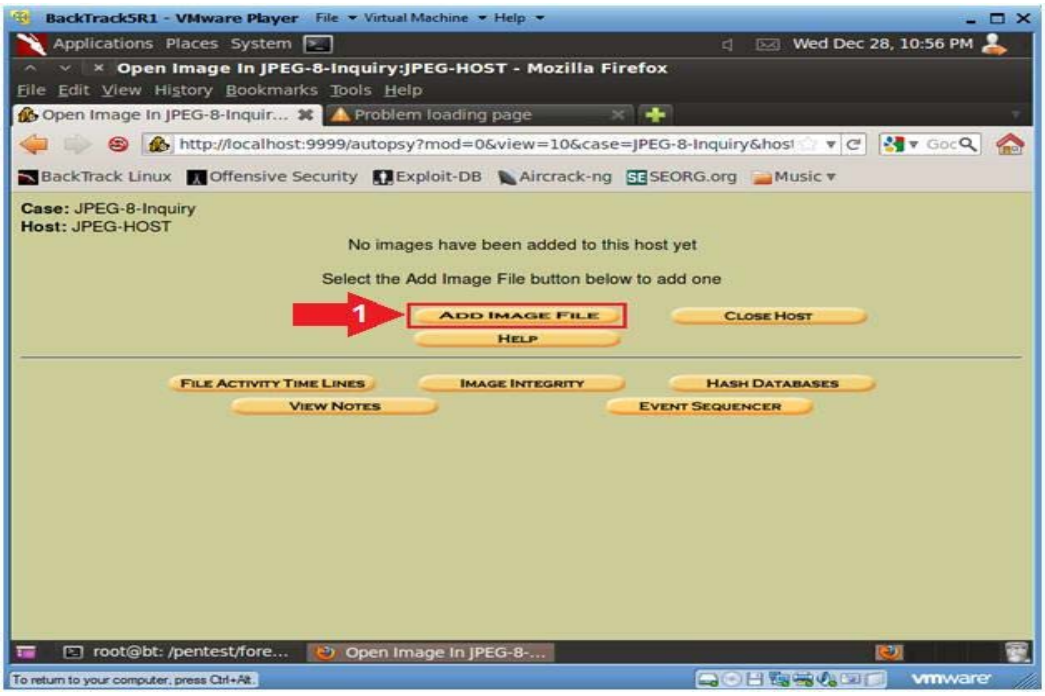
Gambar 10.5 Autopsy Create New Case.



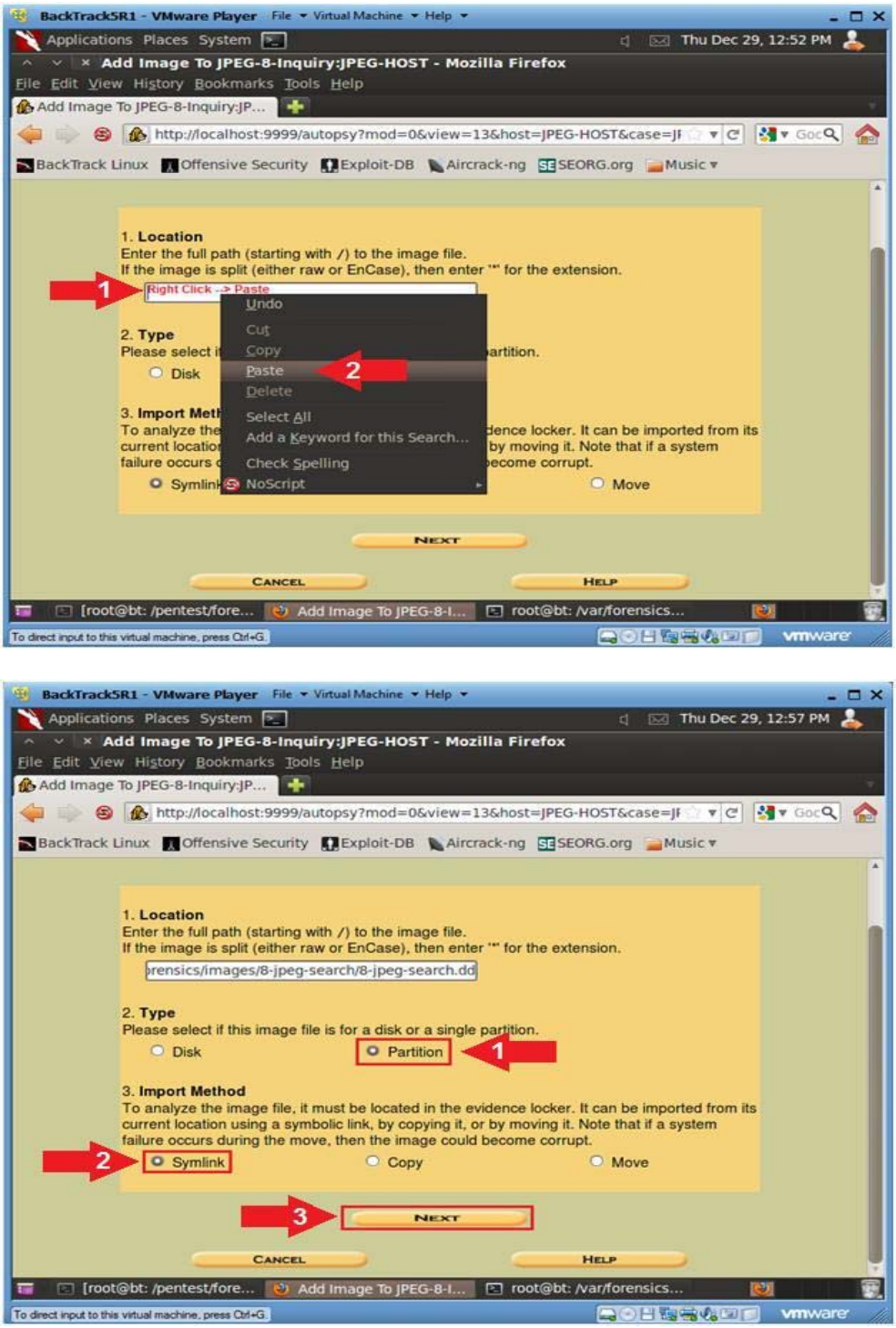
Gambar 10.6 Autopsy Add Image File.



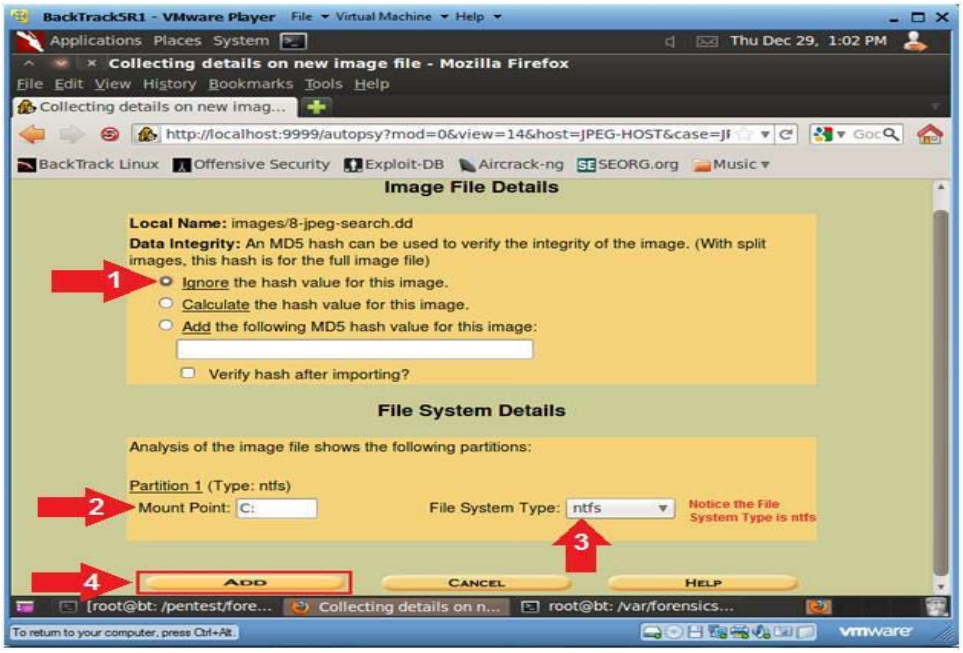
Gambar 10.7 Directory DD Linux.

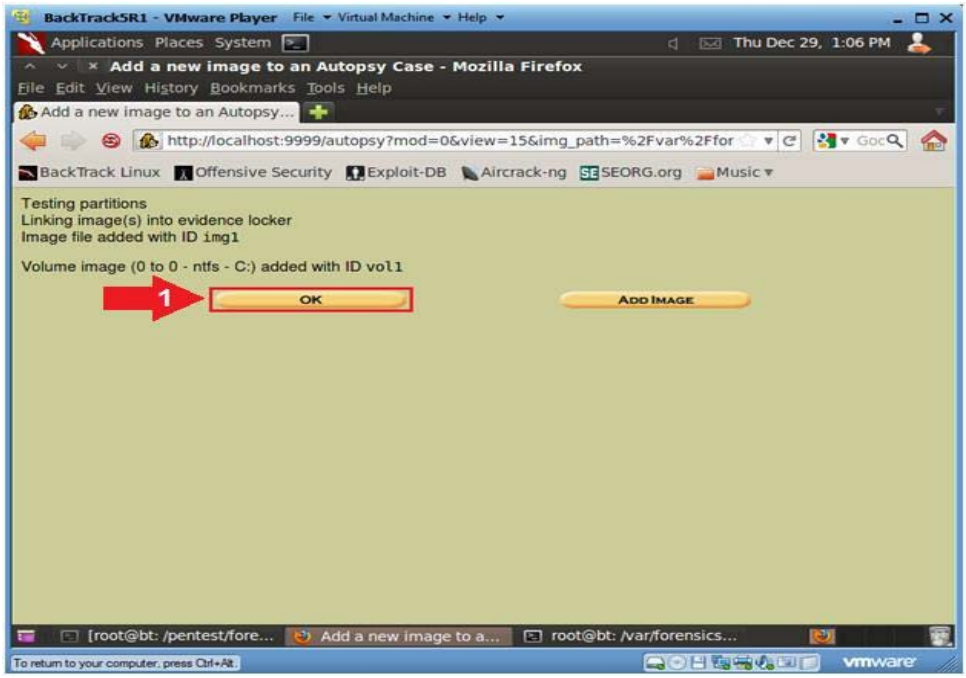


Gambar 10.8 Autopsy Add Image DD.



Gambar 10.9 Autopsy Add Image Location & Partition.


BackTrack5R1 - VMware Player
Applications Places System
Thu Dec 29, 1:02 PM
Collecting details on new image file - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Collecting details on new imag...
http://localhost:9999/autopsy?mod=0&view=14&host=JPEG-HOST&case=J
BackTrack Linux Offensive Security Exploit-DB Aircrack-ng SEORG.org Music
Image File Details
Local Name: images/8-jpeg-search.dd
Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)
1
Ignore the hash value for this image.
Calculate the hash value for this image.
Add the following MD5 hash value for this image:
Verify hash after importing?
File System Details
Analysis of the image file shows the following partitions:
Partition 1 (Type: ntfs)
2
Mount Point: C:
File System Type: ntfs
Notice the File System Type is ntfs
3
4
ADD
CANCEL
HELP
[root@bt: /pentest/fore...
Collecting details on n...
root@bt: /var/forensics...
To return to your computer, press Ctrl+Alt
vmware


BackTrack5R1 - VMware Player
Applications Places System
Thu Dec 29, 1:06 PM
Add a new image to an Autopsy Case - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Add a new image to an Autopsy...
http://localhost:9999/autopsy?mod=0&view=15&img_path=%2Fvar%2Ffor
BackTrack Linux Offensive Security Exploit-DB Aircrack-ng SEORG.org Music
Testing partitions
Linking image(s) into evidence locker
Image file added with ID img1
Volume image (0 to 0 - ntfs - C:) added with ID vol1
1
OK
ADD IMAGE
[root@bt: /pentest/fore...
Add a new image to a...
root@bt: /var/forensics...
To return to your computer, press Ctrl+Alt
vmware