FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Forensische Untersuchung virtueller Maschinen

Remigius Kaminski

Lehrgebiet Datennetze, IT-Sicherheit und IT-Forensik

IT Forensik
FH Aachen

Inhaltsverzeichnis

Problemstellung

- Verschiedene Virtualisierungsmöglichkeiten
  - VMware Workstation, Oracle VirtualBox, Microsoft Virtual PC, Parallels
  - Allein VMware hat 10 Virtualisierungslösungen
- Wird eine VM genutzt oder wurde eine genutzt?
- Welche Daten werden wo von der VM gespeichert?

VM = Virtuelle Maschine

Problemstellung

- Live Forensics
  - Speicherzugriffe der VM
  - Netzwerkverkehr von der VM oder Host verursacht
  - Angeschlossene virtuelle Geräte
  - Eindeutige Zuordnung der VM zum Host

- Ist die Maschine physisch oder virtuell?
- Nachweisbarkeit vor Gericht

Problemstellung

Verhandlung aus den USA:

Mr. Defense: Ms. Barrett is there a difference between physical and virtual environments?

Ms. Barrett: Yes

Mr. Defense: Was the environment you examined physical or virtual?

Ms. Barrett: Physical

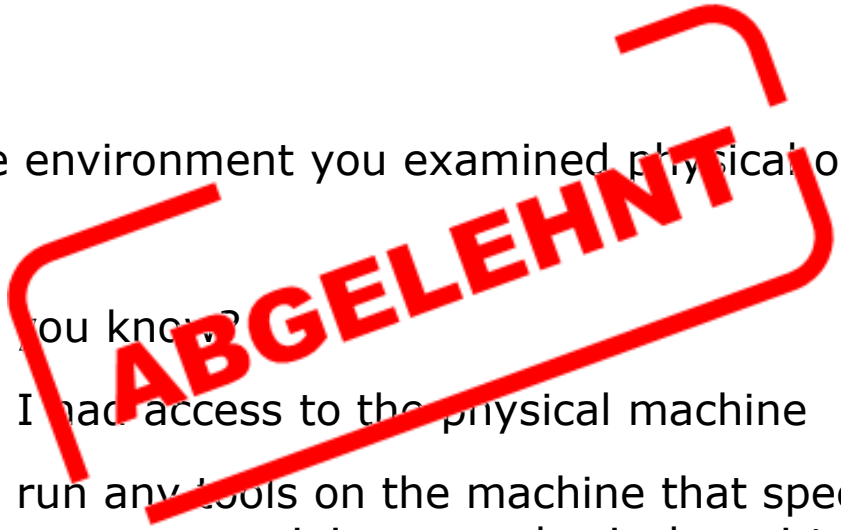
Mr. Defense: How do you know?

Ms. Barrett: Because I had access to the physical machine

Mr. Defense: Did you run any tools on the machine that specifically checked if the environment you were examining was physical or virtual

Ms. Barrett: No

Mr. Defense: If you did not use a tool to validate the environment, how can you say for sure that the environment was physical



Ansatz

- Möglichst realitätsnah
- Nachvollziehbar und beweisbar
- Vorhandene bereits anerkannte Tools verwenden
- Zwei Fälle
  - Ansatz für Dead Virtual Environment
  - Ansatz für Live Virtual Environment

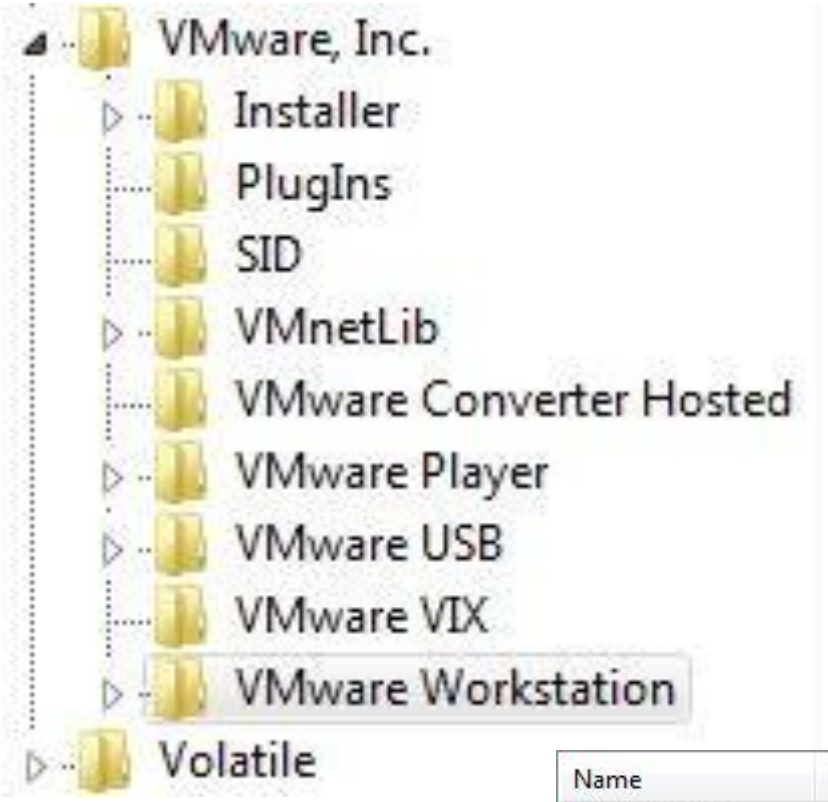
Ansatz – Dead Virtual Environment

- Verdächtiger Host läuft oder ist aus
- Woran erkenne ich das VM vorhanden?
  - Wurde die VM auf den Host eingespielt oder kopiert?
  - Footsteps vorhanden
- Wo befindet sich die VM?
  - Auf Festplatte oder einem USB-Stick
- Verbindung zwischen Host und VM
  - Wenn auf USB-Stick VM gefunden
- Weitere Informationen über die VM
  - Statusänderungen der VM

Ansatz – Live Virtual Environment

- Host und VM laufen
- Physisch oder virtuell
- Genutzte Snapshot Dateien
  - Gibt es Exporte von VM Dateien
  - Letzte Statusänderungen VM
  - Vergleich 2 Snapshot Dateien ohne Hashes
- Wurde VM auf dem Host angelegt oder importiert?

Bisherige Ergebnisse



Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
InstallPath	REG_SZ	C:\Program Files (x86)\VMware\VMware Workstation\
InstallPath64	REG_SZ	C:\Program Files (x86)\VMware\VMware Workstation\x64\
ProductCode	REG_SZ	{A3FF5CB2-FB35-4658-8751-9EDE1D65B3AA}
ProductVersion	REG_SZ	7.1.1.282343

Bisherige Ergebnisse

- Datei .vmdk
- VM ist nativ virtualisiert
- Kein Snapshot vorhanden
- Datenträgerkonfiguration
- Dateiname
- Festplatten-Geometrie
- ID der VMDK Datei

```
rFile version=1
encoding="window
s-1252" CID=31be
418b parentCID=f
fffffff isNative
Snapshot="no" cr
eateType="monoli
thicSparse"  # E
xtent descriptio
n RW 20971520 SP
ARSE "Windows XP
 Professional.vm
dk"  # The Disk
Data Base  #DDB
 ddb.adapterType
 = "buslogic" dd
b.geometry.secto
rs = "56" ddb.ge
ometry.heads = "
255" ddb.geometr
y.cylinders = "1
468" ddb.uuid =
"60 00 C2 95 94
81 11 1e-6c 2d 5
b 32 5c 78 8c 7d
" ddb.longConten
tID = "2dffb6961
b7d797d9f55808d3
1be418b" ddb.vir
tualHWVersion =
"7" ddb.toolsVer
sion = "8323"
```

FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Vielen Dank für Ihre Aufmerksamkeit

Haben Sie noch Fragen?

IT Forensik
FH Aachen