Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Digitale Forensik - Übungen

Bachelorstudiengang IT Security
Modul Digitale Forensik – Übungen
Sommersemester 22

Diese Übungen stellen die praktische Umsetzung der im theoretischen Teil vermittelten Inhalte dar. Nach der Bearbeitung der Aufgaben können Sie die wichtigsten forensischen Untersuchungen durchführen und die ermittelten Ergebnisse selbstständig beurteilen. Achten Sie darauf eine nachvollziehbare Dokumentation Ihrer Arbeit anzufertigen. Diese benötigen Sie später bei der Bearbeitung der Prüfungsaufgaben.

Übung 1: Digitale Forensik 2
Übung 2: Datenträgerforensik 3
Übung 3: Betriebssystemforensik 5
Übung 4: Anwendungsforensik 6
Übung 5: Systemanalyse [Exkurs] 7
Übung 6: Spezialdisziplinen [Exkurs] 9
Forensic Challenges [Exkurs] 10

Virtuelles Labor

Zur Bearbeitung der Übungen wird in diesem Modul ein virtuelles Labor verwendet. Es basiert auf zwei virtualisierten Betriebssystemen, einmal ein Windows 10 System WINDOWS und einmal eine Linux-Kali-Distribution LINUX. Auf beiden Systemen sind bereits die geläufigsten Tools für die forensische Untersuchung vorinstalliert. Damit können direkt die Übungen bearbeitet werden, ohne dass eine langwierige Einrichtung der Anwendungen erfolgen muss. Beide Systeme sind auf möglichst einfach Bedienung hin optimiert und nicht sicher konfiguriert, daher sollten sie nicht direkt mit dem Internet verbunden werden. Die virtuellen Maschinen benötigen die Software VMware Workstation Player mindestens in der Version 15.

Kali-Linux LINUX

Unter „I:\INF\TI\Veranstaltungen\Malik\Virtuelle Maschinen\“ liegt ein angepasstes Kali Linux-System. Dieses können Sie über die Datei „HSAS_LINUX.vmx“ mit dem VMWare Player starten. Das „kali“ Passwort lautet „kali“.

Windows 10 WINDOWS

Unter „I:\INF\TI\Veranstaltungen\Malik\Virtuelle Maschinen\“ liegt ein angepasstes Windows-System. Dieses können Sie über die Datei „HSAS_WINDOWS.vmx“ mit dem VMWare Player starten. Der Admin-Benutzer hat kein Passwort.

Forensic Explorer & Magnet AXIOM

Auf dem Windows System sind die kostenpflichtigen Versionen Anwendungen Forensic Explores und Magnet AXIOM installiert. Sie benötigt den Zugang zu einem Lizenzserver und funktioniert daher nur im Netz der Hochschule. Sollten Sie die VM auf Ihrem privaten Rechner einsetzen, können eine VPN Verbindung für den Zugang zum Lizenzserver nutzen.

Übung 1: Digitale Forensik

Übung 1.1: Zeitstempel LINUX/WINDOWS

Dateien besitzen Zeitstempel, die angeben wann einen Datei erstellt, zuletzt geändert und zuletzt geöffnet worden ist. Recherchieren Sie, wie diese Zeitstempel unter Windows und Linux ausgelesen werden können. Recherchieren Sie anschließend nach Anwendungen, mit denen Sie die Zeitstempel ändern können.

a) Welche Zeitstempel stellt Windows bzw. Linux zur Verfügung?

b) Gibt es neben den „üblichen“ Zeitstempeln noch weitere Informationen zu Zeitinformationen, die interessant sein könnten?

c) Recherchieren Sie eine Anwendung, mit der Sie die Zeitstempel ändern können.

Übung 1.2: Zeitstempel

Verwenden Sie für diese Aufgabe das Windows-System der Hochschule. Erstellen Sie drei leere Text-Dateien – z.B. test1.txt, test2.txt und test3.txt. Kopieren Sie die erste Datei auf ein anderes Laufwerk und benennen diese um – z.B. test4.txt. Verschieben Sie die Datei anschließend wieder zurück. Nehmen Sie nun die zweite Datei und verschieben diese auf ein externes Laufwerk und verschieben Sie anschließend wieder zurück. Nehmen Sie nun die dritte Datei und verschieben diese auf ein internes Laufwerk und verschieben Sie diese Datei anschließend wieder zurück.

a) Stellen Sie tabellarisch alle Zeitstempel für alle vier Dateien dar. Wodurch wird die Zeit eines Systems beeinflusst?

Übung 1.3: Read-only Zugriff LINUX/WINDOWS

Ein USB-Stick und ein virtuelles Laufwerk sollen beim Anschließen an einen Rechner nicht vollständig gemountet werden, sondern im „nur-lesen“ Modus eingebunden werden. Beschreiben Sie die notwendigen Konfigurationen und erstellen Sie jeweils ein Script um den Vorgang zu automatisieren.

a) Wie erreichen Sie dies unter Linux?

b) Wie erreichen Sie dies unter Windows?

Übung 2: Datenträgerforensik

Übung 2.1: Forensische Sicherung eines Laufwerkes LINUX

Erstellen Sie ein mit dem Tool dd [Howto] ein 50MB großes virtuelles Laufwerk und formatieren Sie diese mit FAT. Verwenden Sie hierfür das Tool mkfs [Howto]. Binden Sie das Laufwerk ein und kopieren Sie anschließend verschiedene, beliebige Dateien auf die Partition.

Erstellen Sie eine forensische Kopie der Partition - verwenden Sie hierfür das Programm dcfldd [Website][Howto]. Beachten Sie dabei, dass das Laufwerk nicht eingebunden sein darf. Der MD5-Hash-Wert der Kopie soll dabei in eine Datei geschrieben werden. Beschreiben Sie Ihr Vorgehen und die verwendeten Befehle. Wie sieht der Befehl aus, wenn Sie das Image in 10 MB große Dateien aufsplitten?

Übung 2.2: Validierung der Kopie LINUX

Validieren Sie den Hash-Wert aus Übung 2.1, indem Sie einen Hashwert des virtuellen Laufwerkes mit dem Programm md5sum erzeugen. Führen Sie anschließend einen automatisierten Vergleich der beiden Hash-Werte durch. Beschreiben Sie Ihr Vorgehen und die verwendeten Befehle.

Übung 2.3: File Carving WINDOWS

Laden Sie das Image „Basic Data Carving Test 1“ herunter und untersuchen Sie es mit der Software Forensic Explorer. Nutzen Sie dazu die Option „File Carve“ [Anleitung S. 344].

a) Welche Dateien sind im Image enthalten?

b) Welche Dateien waren beschädigt und konnten wiederhergestellt werden?

Übung 2.4: Vergleich von Werkzeugen für das Carving WINDOWS/LINUX

Untersuchen Sie, inwieweit verschiedene Tools, Dateien wiederherstellen können (carving/Retrieving files by file header searching) oder Images auch gar nicht lesen können. Vergleichen Sie die Tools *Autopsy (Win)* [Dokumentation], *Forensic Explorer (Win)* [Anleitung S. 344] und *Foremost* (Linux) [Howto | Howto]. Binden Sie das zweite Image (JPEG Search Test #1) mit dem Tool OSFMount unter Windows ein verwenden Sie zusätzlich das Tool Recuva (Win).

Verwenden Sie für die Untersuchung die folgenden zwei Images:
Basic Data Carving Test #2 http://dftt.sourceforge.net/test12/index.html
JPEG Search Test #1 http://dftt.sourceforge.net/test8/index.html

Welche Dateien werden mit dem jeweiligen Carving Tool gefunden?

Übung 2.5: Testszenario für das Carving WINDOWS/LINUX

Überlegen Sie sich einen Testfall, mit dem es möglich ist, File Carving von JPEG-Dateien zu untersuchen. Erstellen Sie dazu ein virtuelles Image und speichern Sie darauf mindestens drei JPEG-Dateien. Löschen Sie nun eine Datei, beschädigen Sie eine weitere Datei (löschen Sie dazu einen Teil des Bildes mit einem HEX- oder Text-Editor) und entfernen Sie von der dritten Datei den Datei-Header (öffnen Sie dazu das Image in einem Hex-Editor und bearbeiten es).

Realisieren und überprüfen Sie den Testfall. Beschreiben Sie Ihr Vorgehen.

Übung 2.6: EnCase, Metadaten und Zusatzinformationen WINDOWS/LINUX

Führen Sie eine Analyse der Datei uebung_2-6.E01 (diese ist auf ILIAS zu finden) mit einem Tool Ihrer Wahl durch. Prüfen Sie zu Beginn die Integrität des Images. Inwieweit unterscheidet sich der im E01-Format vorliegende Hash mit dem des ursprünglichen Images? Wie können Sie sich diesen Unterschied erklären?
Lesen Sie daraufhin die dateiformatspezifischen Metadaten aus. Lassen sich die Autoren der Dateien ermitteln? Führen Sie anschließend eine Schlüsselwortsuche durch. In diesem Beispiel wird vermutet, dass der Ort eines Treffens in einer der Dateien auf der SD-Karte enthalten ist. Im Bilderordner befindet sich eine thumbs.db-Datei. Prüfen Sie, ob alle Dateien, für die Vorschaubilder existieren, noch vorhanden sind.

Übung 2.7: Vertiefte Analyse – Teil 1 LINUX

In den nachfolgenden Übungen soll das auf Ilias bereitgestellte Abbild einer Festplatte untersucht werden, deren Inhalt nicht näher beschrieben ist. Verwenden Sie hierfür die Werkzeuge des Sleuth Kits. Die Verwendung von Autopsy bzw. des Autopsy Forensic Browsers ist hier nicht vorgesehen. Für die Ausarbeitung sind jeweils die verwendeten Werkzeuge mit den entsprechenden Parametern und die geforderten Ergebnisse entsprechend der Aufgabenstellung anzugeben.

a) Verwenden Sie das Datenträgerwerkzeug mmls, um die Partitionstabelle des Images auszulesen. Wie viele Partitionen befinden sich auf dem Abbild? Welche Dateisysteme verwenden die einzelnen Partitionen? Verwenden Sie gegebenenfalls TestDisk, um die Korrektheit der Partitionstabelle zu überprüfen.

b) Mit den Informationen aus der vorherigen Übung können Sie nun die Analyse der Dateisysteme durchführen. Verwenden Sie das Werkzeug fsstat unter Berücksichtigung des passenden Offsets. Geben Sie die von Ihnen verwendeten Programmaufrufe für die einzelnen Partitionen an.

c) Listen Sie die Dateien und Verzeichnisse der einzelnen Dateisysteme auf. Nennen Sie in Ihrer Ausarbeitung neben den gefundenen Dateien und Verzeichnissen auch das verwendete TSK-Werkzeug und die übergebenen Parameter.

d) [Exkurs] Mit den Inodes der Daten aus der vorherigen Übung und dem Werkzeug istat können Sie sich nun detaillierte Informationen über einzelne Dateien ausgeben lassen. Führen Sie die notwendigen Schritte exemplarisch an einer Datei durch und geben Sie den verwendeten Programmaufruf sowie die Ausgabe in Ihrer Ausarbeitung an.

Übung 2.8: Vertiefte Analyse – Teil 2 WINDOWS

Für die Lösung der nachfolgenden Übungsaufgaben müssen Sie Autopsy unter Windows verwenden. Erstellen Sie einen neuen Fall und fügen Sie dem Fall einen Host und das bereitgestellte Image bei. Über die „Case Gallery“ können nun die einzelnen Partitionen betrachtet und analysiert werden. Nutzen Sie das Case-Management von Autopsy für diese Übung, sodass die einzelnen Analyseschritte gut dokumentiert sind. Dies Aufgaben sollen Ihnen vor allem den Unterscheid zu Sleuth Kit aufzeigen, daher sind nicht alle Aufgaben direkt lösbar.

a) Wie viele Partitionen hat das Image? Vergleichen Sie Ihre Ergebnisse mit denen aus Übung 2.7. Werden alle Partitionen in Autopsy korrekt angezeigt?

b) Welche allgemeinen Informationen können Sie über die Dateisysteme herausfinden (zum Beispiel: Dateisystem, Volume Name, letzter Schreibzugriff und letzter Zeitpunkt, zu dem die Partition gemounted wurde)?

c) Geben Sie für jeweils eine beliebige Datei pro Dateisystem den Dateinamen, das Dateiformat, die Dateigröße und den Dateiinhalt an. Einige Dateitypen enthalten Metadaten, die am Anfang der Datei positioniert sind. Über die ASCII-Strings-Anzeige von Autopsy können diese Informationen problemlos ausgelesen werden. Welche Dateitypen mit Metadaten können Sie in dem Image finden?

d) Erstellen Sie über Autopsy eine Zeitachse der Dateiaktivitäten für die einzelnen Partitionen. In welchen Zeiträumen fanden die Aktivitäten statt?

Übung 3: Betriebssystemforensik

Übung 3.1: Logfile-Analyse LINUX

Untersuchen Sie eine LinuxVM mittels des Programms logwatch[Howto] über einen selbst gewählten Zeitraum. Protokollieren Sie die Ausgabe und beschreiben Sie jede der ausgegebenen Kategorien mit ein paar Sätzen, indem Sie darlegen, welche Informationen in diesem Bereich ausgegeben werden.

Installation unter Kali: apt update | apt install logwatch

Übung 3.2: Webserver LINUX

Auf dem Kali Linux ist ein Webserver eingerichtet. Analysieren Sie die installierte Web-Anwendung und beschreiben Sie kurz ihre Funktionsweise. Recherchieren Sie, welche Dateien für eine forensische Auswertung interessant sind und analysieren Sie diese. Beantworten Sie zudem die Frage welcher Nutzer zu welchem Zeitpunkt Zugriff auf welche Dateien hatte.

Übung 3.3: Hive-Files Analyse WINDOWS

Auf Ilias finden Sie Hive-Files, die einem System entnommen wurden. Verwenden Sie den Forensic Registry Editor (fred) und den Forensic Explorer, um diese Dateien zu analysieren und beantworten Sie die folgenden Fragen:

1) Welchem Verzeichnis wurden diese Dateien vermutlich entnommen und um welche Hive-Files handelt es sich?

2) In welchem Hive-File finden sich Informationen zu den angelegten Benutzern? Wie lauten die Benutzer? Nennen Sie außerderdem zu jedem Account die Zeitstempel des letzten Logins und der Passwortänderung.

3) Welche Software wurde auf dem System installiert?

4) Welche Informationen können Sie über die angeschlossenen USB-Speichermedien finden?

Übung 4: Anwendungsforensik

Übung 4.1: Firefox Web-Browser WINDOWS

Rufen Sie mit dem Web-Browser mehrere Websites auf, um Einträge in den Datenbanken zu generieren. Ein kleiner Tipp: Große Nachrichtenportale laden viele verschiedene Quellen und sind hier sehr ergiebig. Führen Sie zusätzlich weitere Aktionen durch: Erstellen Sie von einigen Seiten Bookmarks und löschen Sie einige davon wieder, laden Sie eine Datei herunter, füllen Sie ein Formular aus und schicken Sie dieses ab. Melden Sie sich bei einer Seite an und speichern Sie das Passwort.

Analysieren Sie anschließend den Profil-Ordner von Firefox und untersuchen Sie, ob Sie die unternommenen Schritte nachvollziehen können. Verwenden Sie dazu die Software *DB Browser for SQLite*.

Einführung: Mozilla Firefox Forensics – Usage of Sqlite File in Investigation

https://www.acquireforensics.com/services/tech/mozilla-firefox.html

Übung 4.2: Web Forensics - Cache WINDOWS

Setzen Sie Ihren Firefox Web-Browser komplett zurück und löschen Sie alle Daten. Rufen Sie nun den nachfolgenden Link auf und besuchen Sie der Reihe nach all drei Demos.

Link: https://lab.scheible.it/web-forensics/cachemanipulation/

Analysieren Sie nach jedem Aufruf, welche Daten im Cache abgelegt wurden. Nutzen Sie dazu die Anwendung MZCacheView von NirSoft. Welche Informationen bzw. Dateien finden Sie? Erstellen Sie einen tabellarischen Vergleich der drei Demos.

Übung 4.3: Web Forensics - Downloads WINDOWS

Setzen Sie Ihren Firefox Web-Browser komplett zurück und löschen Sie alle Daten. Rufen Sie nun den nachfolgenden Link auf und besuchen Sie alle Unterseiten.

Link: https://lab.scheible.it/web-forensics/jsdownloader/

Untersuchen Sie, welche Netzwerkübertragungen beiden Seitenaufrufen durchgeführt werden/ wurden. Nutzen Sie dazu die in Firefox integrierten Entwicklerwerkzeuge (Reiter Netzwerkanalyse). Welche Übertragungen sind erkennbar und wie werden die Downloads gestartet?

Übung 4.4: Web Forensics – HTTP Header WINDOWS

Rufen Sie nun den nachfolgenden Link auf und besuchen Sie der Reihe nach alle Unterseiten.

Link: https://lab.scheible.it/web-forensics/httpheaders/

Untersuchen Sie, welche Auswirkung die verschiedenen HTTP Header auf die Spuren im Cache habe. Werden alle Daten wie bekannt gespeichert? Welche zusätzlichen Einträge können durch HTTP Header angelegt werden?

Übung 5: Systemanalyse [Exkurs]

Übung 5.1: Versteckte Zugangsdaten [EXKURS]

Es ist bekannt, dass die Zugangsdaten zu Rechnern auf den Volumen IBM-P3-Ext3g.dd in Dateien des Verzeichnisses /accounts/ in den Dateien user1.txt bis user10.txt sowie in Metadaten enthalten sind.

Der Inhalt der Dateien user1.txt bis user5.txt enthält Zugangscodes zu 5 Rechnern. Der Inhalt dieser Dateien ist folgendermaßen aufgebaut:

- Rechnername: IWW-XWi (letzte Ziffer i wie useri.txt)
- Allgemeines Kennwort: xw1234
- User: Admin
- pwd: (keines)

TeamViewerID: s. Inode 1100i (letzte Ziffer i wie useri.txt)

Die TeamViewerID für den Rechner IWW-XWi ist im Inode 1100i gespeichert, allerdings codiert.

Die Codierung, die auf die TeamViewerID angewendet wurde, ist in einer gelöschten Datei user?.txt angegeben. Alternative, aber nicht angewendete Codierungen, sind in den Dateien user7.txt bis user10.txt zu sehen.

- In welcher Reihenfolge wurden die Dateien user1.txt bis user10.txt vermutlich erzeugt oder modifiziert? Sie können als Anhaltspunkte die Timestamps/ Zeitstempel, die Journaleinträge sowie die Allokation heranziehen.
- Wie sind Sie vorgegangen, um die gelöschte Datei user?.txt zu suchen und auszuwerten? Was ist die angewendete Codierung?
- Wie lauten die codierten und decodierten TeamViewerIDs?

Übung 5.2: Hirschhornsalz-Affäre [EXKURS]

In einer Stadt wurde Ende 2012 eine Untersuchung im Zusammenhang mit Drogenhandel durchgeführt. Die bekannte, stark süchtig machende Substanz Hirschhornsalz wurde in größeren Mengen von Lebkuchen gefunden. In diesem Zusammenhang wurde gegen den Händler Egon Kräuterling sowie gegen den Bürgermeister der Stadt, Karl König sowie gegen Beamte der Stadtverwaltung ermittelt.

Zwei Pressemitteilungen dazu:

Pressemitteilung vom 24.12.2012:
Drogenhändler Egon Kräuterling flüchtig. Große Mengen an Hirschhorn-Drogen gefunden. Die Ermittlungen laufen.
Staatsanwalt Weißwas

Pressemitteilung vom 27.12.2012:
In Sachen Drogenhändler Egon Kräuterling. Die Ermittlungen sollen klären, ob korrupte Beamte involviert sind. Evtl. wird ein städtischer Untersuchungsausschuss eingesetzt: Wer-wusste-wann-was.
Staatsanwalt Weißwas

Die Asservate *ntfs-egon-01b.001* und *ntfs-karl-02a.001* wurden von zwei USB-Sticks sichergestellt (die Abbilder werden bereitgestellt). Zunächst sollen die $logfiles nicht berücksichtigt werden.

a) Verschaffen Sie sich einen Überblick über die Asservate:
   I Welche Dateien und Ordner befinden sich auf den Asservaten?
   II Welche gelöschten Dateien sind zu finden und ggf. wiederherstellbar?
   III Welche Dateien erscheinen für die Ermittlung relevant?

b) Erstellen Sie eine Timeline aller relevanten Dateien anhand der Zeitstempel MAC (aus STANDARD_INFORMATION und FILENAME) sowie der MFT-Einträge und ggf. aus INDEX_ALLOCATION.
I Welche relevanten Sachzusammenhänge sind zwischen den in den Dateien enthaltenen Informationen (scheinbar oder aber tatsächlich) zu erkennen?
II Gibt es Hinweise auf gefälschte Zeitstempel und falls ja, welche?

Nun sollen zusätzlich die $logfiles berücksichtigt werden.

Hinweis: Im Asservat ntfs-egon-01.001 ist $logfile aus technischen Gründen erst ab Eintrag 24A40 nutzbar.

c) Welche Zusammenhänge sind aus den $logfiles zusätzlich zu den bisher eruierten ersichtlich?

Karl König behauptet, er hätte erst im Jahr 2013 von den Vorwürfen gegen Egon Kräuterling erfahren, bis dahin habe er gutgläubig dessen Produkte gekauft.

d) Welche Inhalte und welche Zeitstempel müssten verändert werden, so dass diese Behauptung wahr sein könnte?
Hinweis: Es dürfen keine Dateien gelöscht werden und die inhaltlichen Änderungen sollen so klein wie möglich sein.

Übung 6: Spezialdisziplinen [Exkurs]

Übung 6.1: Multimediaforensik - Bildmanipulationen LINUX/WINDOWS

Auf Ilias stehen zwei Abbildungen zur Verfügung, beide wurden mit Bildbearbeitungstools bearbeitet. Finden Sie heraus welche Bereiche bearbeitet wurden.

a) Verwenden Sie die beiden Online-Tools Forensically (https://29a.ch/photo-forensics/) und FotoForensics (https://fotoforensics.com/) zur Analyse der Fotos.

b) Installieren Sie die auf Java basierende Open Source Software ImageJ (https://imagej.net) und führen Sie damit die Untersuchung erneut durch.

Übung 6.2: Live Analyse [EXKURS] LINUX

Starten Sie die das virtualisierte Windows System im VMware Player und öffnen Sie einige Programme wie den Firefox Web-Browser. Öffnen Sie anschließend auf dem Host-System den Ordner C:\VM_BSN1W\DF\Win7. Erstellen Sie eine Kopie der Datei mit der Dateiendung *.vmem*. Dabei handelt es sich um das Abbild des virtuellen Arbeitsspeichers des virtualisierten Windows Systems.

Untersuchen Sie dieses Abbild zum einen mit der Software Forensic Explorer und zum anderen mit der Software Volatility unter Kali Linux. Welche Informationen können Sie aus diesem Speicherabbild gewinnen?

Einführung: Memory Forensics and Analysis Using Volatility

http://resources.infosecinstitute.com/memory-forensics-and-analysis-using-volatility/

Forensic Challenges [Exkurs]

Sollten Sie bereits alle Aufgaben gelöst haben oder schneller sein als andere, können Sie diese Exkurse lösen. Es handelt sich hierbei um Aufgaben, die von anderen Einrichtungen öffentlich bereitgestellt werden. Diese Liste wird kontinuierlich erweitert.

Exkurs 1: FDFRWS EU 2017: Forensik Rodeo

Im Rahmen der Konferenz DFRWS EU 2017, die in Überlingen stattfand, wurde ein Forensik Rodeo veranstaltet. Dabei erhielten die Teilnehmer ein vorbereitetes Image eines Rechners. Das Ziel war während der Abendveranstaltung das Geheimnis dieses Rechners zu entschlüsseln und die Fragen zu beantworten.

Über die folgende Links können die Images und die entsprechenden Dateien heruntergeladen werden:

https://hs-as.de/rodeo/dfrws-rodeo.zip
https://hs-as.de/rodeo/dfrws-rodeo.zip.md5
https://hs-as.de/rodeo/dfrws-rodeo.zip.sha256
https://hs-as.de/rodeo/References_Reading-Material.txt
https://hs-as.de/rodeo/The-Case_The-Task.txt

Das Passwort für die ZIP-Datei lautet: Gal1le0#2017

Exkurs 2: Ann's Aurora - An Advanced Persistent Threat based challenge

Bei diesem Szenario geht es darum, dass ein Angreifer versuchte mit einer spear phising Attacke Zugriff auf ein System zu erlangen um Dokumente zu entwenden. Diese Herausforderung ist eine sehr nützliche Fallstudie, um bösartige Netzwerkangriffe zu untersuchen.

https://digital-forensics.sans.org/community/challenges

Weitere Herausforderungen: Test Images and Forensic Challenges

https://www.forensicfocus.com/images-and-challenges