Hochschule Wismar
Studiengang Master „IT-Sicherheit und Forensik“

PRAKTIKUMSBERICHT

Gruppe HH-01

Modul „Forensik in Betriebs- und Anwendungssystemen“

Eingereicht am: 25. Juli 2019

von: Lobmeyer, Christoph [redacted]
Rogala, Lukas [redacted]
Schulz, Claudia [redacted]

Inhalt

1 Einführung / Untersuchungsauftrag

Der Hobby IT-Administrator “Günther Kastenfrosch” hatte in seinem Bekanntenkreis gehört, dass der von Windows installierte Virenscanner „Windows Defender“ sein System verlangsamt. Nach einer Recherche im Internet deaktivierte er den Windows Defender auf seinem PC mit dem Betriebssystem Windows 7.

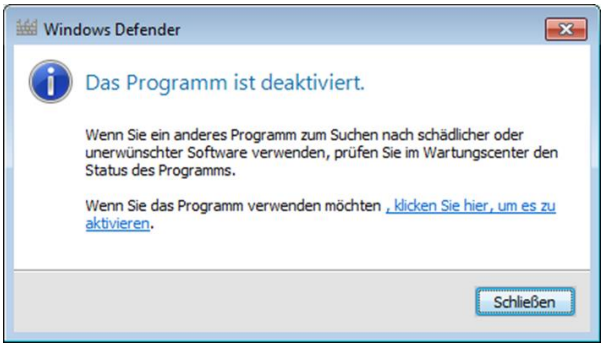


Abbildung 1: Windows Defender deaktiviert

Einige Tage später bekam Herr Kastenfrosch eine E-Mail von dem Absender „Internet Security Center“, die ihn darauf hinwies, dass sein E-Mailkonto „gehacked“ wurde. Zeitgleich gab der Inhalt der E-Mail einen Hinweis darauf, wie der Betroffene Abhilfe schaffen könne und baute unter Verweis auf die „DSGVO“ Zeitdruck auf. Nach 24 Stunden solle sich der Aufwand laut E-Mail immens erhöhen. Zuletzt folgte noch ein Hinweis, dass der Benutzer „je nach Browser“ ein Plugin installieren müsse. Da die E-Mail als Anrede Herrn Kastenfrosch namentlich ansprach, hielt er sie für seriös.

Abbildung 2: E-Mail mit Hinweis auf ein gehacktes E-Mailkonto

Nachdem er die URL aufrief, wurde ihm tatsächlich eine Mitteilung angezeigt, in der er aufgefordert wurde ein Plugin zu installieren. Durch den Zeitdruck ließ er sich dazu verleiten, der E-Mail und dem Text zu vertrauen und das angebotene Plugin herunterzuladen sowie auszuführen. Kurze Zeit später bemerkte er, dass sein Computer ungewöhnlich aktiv wurde und sich das System anschließend deutlich verlangsamte. Kurz darauf wurde ihm allerdings eine Text-Datei präsentiert, die ihm mitteilte, dass sein System verschlüsselt sei und erst nach Zahlung eines entsprechenden Lösegelds wieder freigegeben würde. Seit diesem Moment kann er nicht mehr auf die Daten auf seinem PC zugreifen.

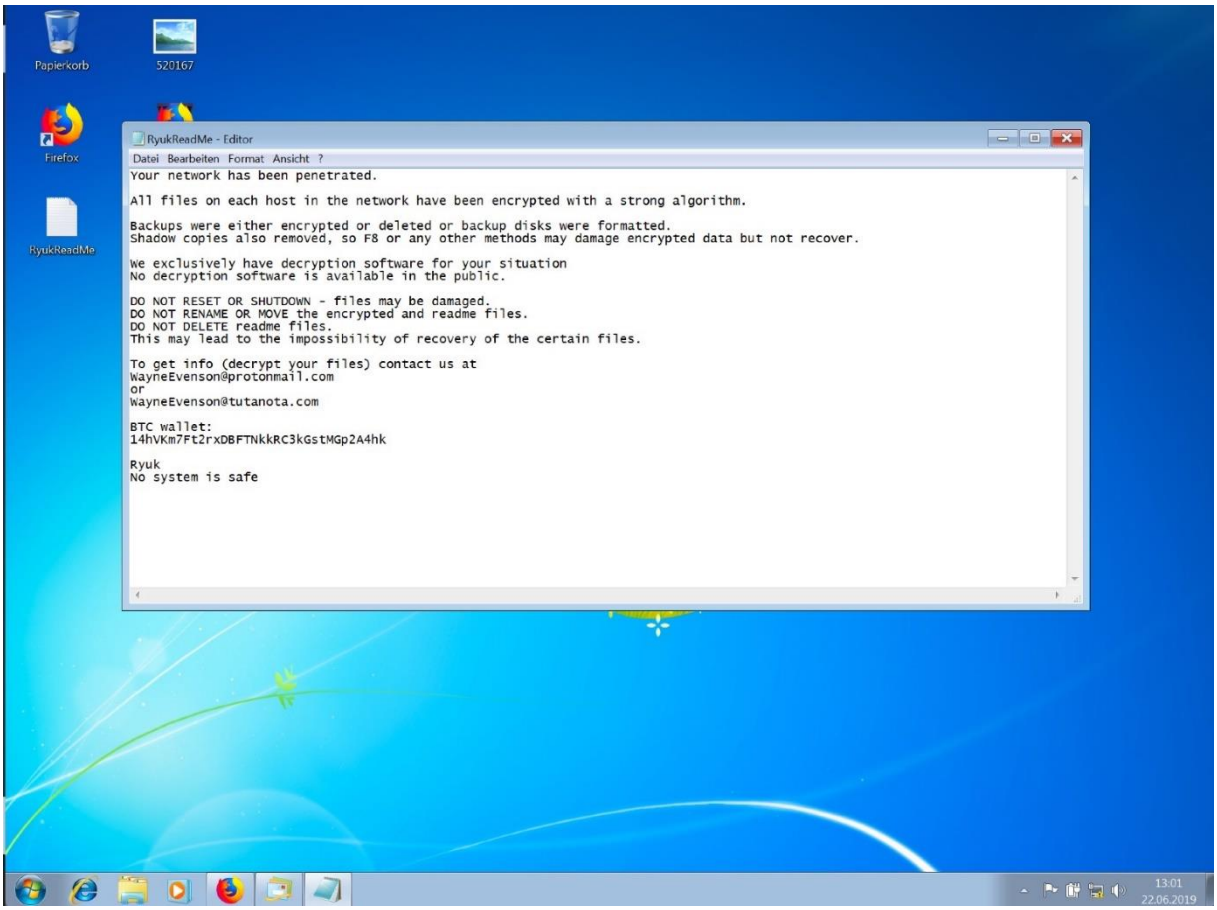


Abbildung 3: Screenshot vom Betroffenen Client-System

Nachdem er den PC heruntergefahren hatte, wendete er sich an einen befreundeten IT-Forensiker um von ihm Unterstützung zu erhalten.

2 Planung

Als Forensiker ist der Bekannte von Herrn Kastenfrosch auf forensische Datensicherungen und Untersuchungen vorbereitet. Hierzu hat er fach- und toolspezifische Schulungen und Fortbildungen besucht, sowie eine Systemumgebung geschaffen, auf der er ohne hohes Risiko forensische Untersuchungen vornehmen kann.

Die Untersuchungsumgebung besteht aus einem virtualisierten Analysesystem, welches mit Windows 10 (Version 1607) betrieben wird. Auf diesem System sind sowohl Anwendungen wie X-Ways Forensics (Version 19.6 SR-1), SQLite Forensic Explorer (Version 2.0) wie auch RegRipper (Version 2.8) installiert. Bereitgestellt wird diese Umgebung über eine Netzwerkverbindung; der Server ist in gesicherten Räumlichkeiten aufgestellt. Aufgrund der Tatsache, dass die Daten der Kunden häufig sensibel sind, ist der Zugriff auf den Server über einen Benutzernamen und ein Passwort abgesichert.

Da es sich im hier vorliegenden Fall um eine forensische Untersuchung bei einem Malwareverdacht handelt, muss der Analyst vorbereitet sein, weitere Untersuchungen mit öffentlichen Tools durchzuführen. Hierfür muss er über die notwendigen Kenntnisse von typischen Angriffsvektoren und dazugehöriger Artefakte verfügen.

Um jederzeit eine standardisierte und qualitätsgesicherte Vorgehensweise sicherzustellen, nutzt der Analyst sogenannte „Standard Operating Procedures“ (SOP). Hierbei werden immer wieder auftretende Routinetätigkeiten in einen festen Ablauf gebracht, damit keine Aspekte vergessen werden. Für diese Untersuchung sind folgende SOP einschlägig:

- Durchführung einer Datensicherung
- Export der Registry
- Aufbereitung einer Timeline

Weitere Maßnahmen, die im Rahmen der Untersuchung durchgeführt werden, lassen sich nicht standardisieren. Hier kommt auf es auf den individuellen Fall an. Hierfür ist das o. g. Hintergrundwissen des Analysten erforderlich.

3 Datensicherung und Vorbereitung

Zur Analyse des Vorfalls muss im ersten Schritt eine Kopie der Quelldaten erstellt werden, um eine Verfälschung der Beweise auszuschließen. Dazu wird in der Regel die betroffene Festplatte ausgebaut und über einen Writeblocker an das vorbereitete Forensik-System angeschlossen. Hier wird über die anerkannte Software „FTK Imager“ in der Version 4.2.0.13 ein bitweises 1:1 Abbild des Datenträgers erstellt, mit dem weitergearbeitet werden kann.

3.1 Vorbereitung

Zur Datensicherung wird das betroffene System physisch geöffnet und die eingebaute Festplatte entfernt. Eine weitere Festplatte kann im Gehäuse nicht gefunden werden. Üblicherweise nutzt der Forensiker einen Writeblocker mit, den er im weiteren Verlauf verwendet, um die Festplatte an sein Forensik-System anzuschließen und die Daten nicht zu verfälschen.

Anmerkung: Da die Fallstudie in einem virtualisierten Umfeld aufgebaut wurde, wurde zusätzlich zur Original-Platte (vermutlich infiziert) eine weitere virtuelle Festplatte eines Windows 10 Systems in die infizierte Virtuelle Maschine eingebunden. Anschließend wurde der infizierte Rechner mit dem nicht infizierten System gestartet.

3.2 Image-Erstellung mittels FTK Imager

Im Zuge der Datensicherung wird von der vorhandenen Festplatte ein bitweises 1:1-Abbild erstellt, um mit diesem arbeiten zu können. Hierfür wird das unter Forensikern anerkannte Windows-Programm „FTK Imager“ der Firma AccessData eingesetzt.

In den nachfolgenden Unterpunkten wird explizit aufgeschlüsselt, welche Schritte zur Erstellung des Abbilds durchgeführt wurden.

3.2.1 Einlesen der Festplatte als Image

Nachdem das Programm gestartet ist, kann über den Menüpunkt „File“ > „Add Evidence Item“ ein Laufwerk oder Teile eines Laufwerks eingelesen und im Anschluss als Image exportiert werden.

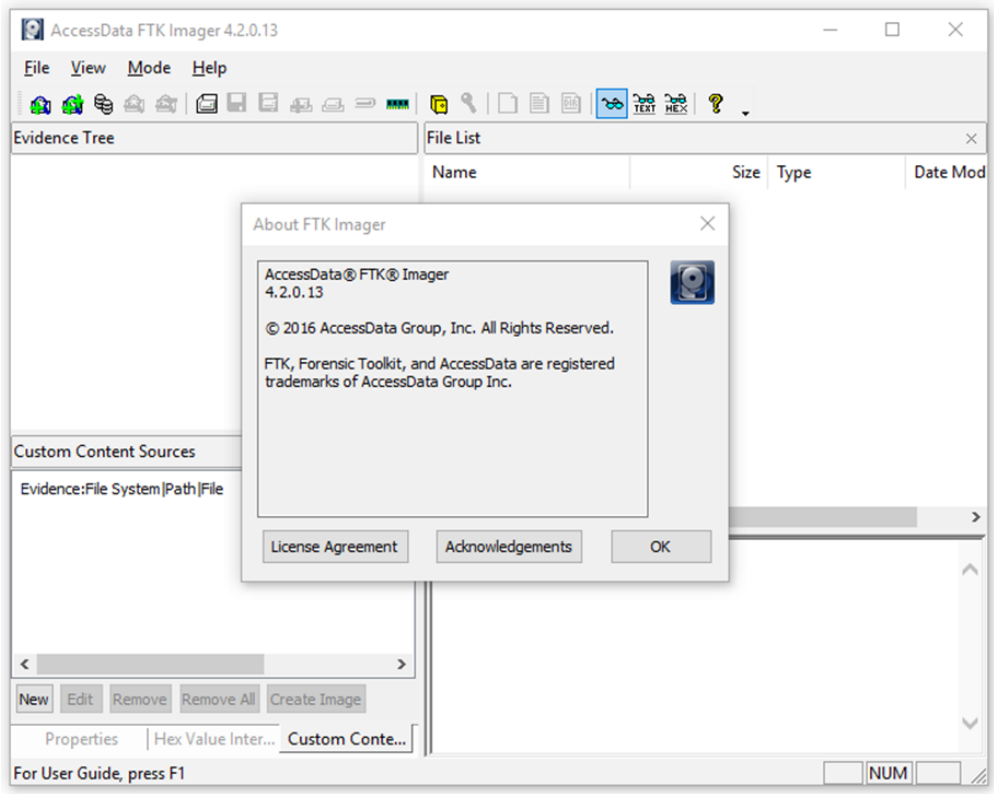


Abbildung 4: FTK Imager - Übersicht und Version

Im darauffolgenden Fenster ist die Option „Physical Drive“ auszuwählen, da so die gesamte Festplatte als 1:1-Abbild eingelesen wird und dadurch in der späteren Analyse auch die Möglichkeit besteht, bereits gelöschte Dateien wiederherzustellen oder versteckte Partitionen zu finden.

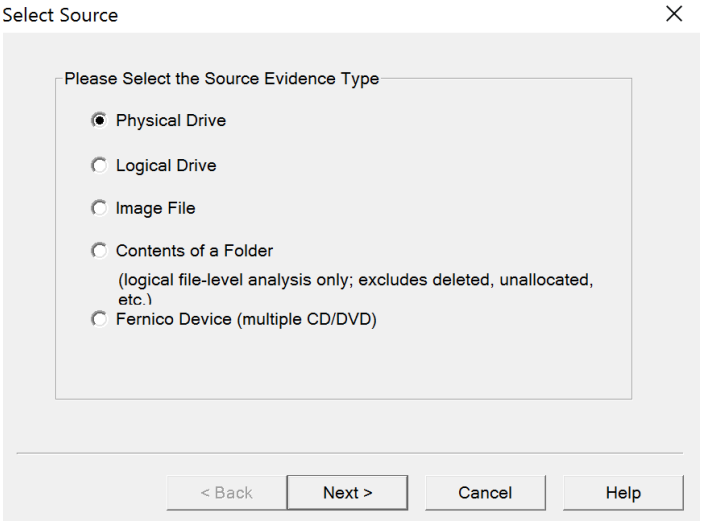


Abbildung 5: FTK Imager - Auswahl Evidence Type

Mit dieser Auswahl fragt die Software nach der konkreten Quelle. Hier wird nun aus einer Liste der angeschlossenen Laufwerke die kompromittierte Festplatte ausgewählt und mit einem Klick auf „Finish“ in die Software eingelesen.

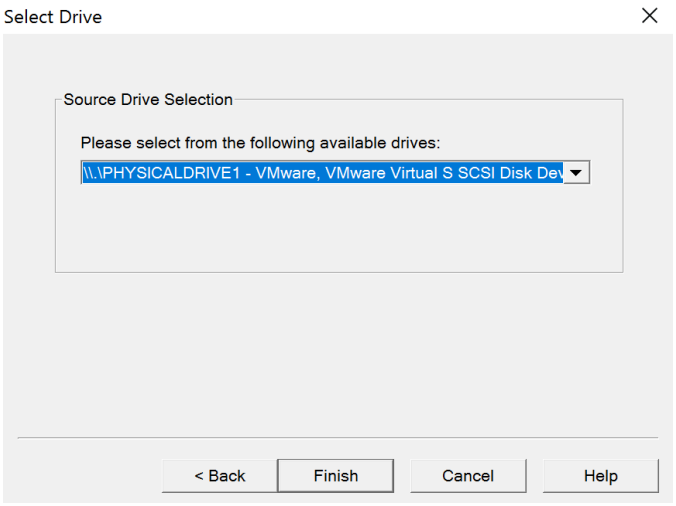


Abbildung 6: FTK Imager - Auswahl des Quell-Laufwerks

3.2.2 Image exportieren

Nachdem der FTK Imager das Laufwerk eingelesen hat wird damit begonnen das Image zu exportieren. Dies geht erneut über den Menüpunkt „File“ > „Create Image“. Im Popup, das daraufhin zu sehen ist, wird zuerst ein Ziel gewählt, an dem das erstellte Image abgelegt wird. Weiterhin muss das Format gewählt werden, in welches das Image exportiert wird. Im vorliegenden Fall wird das Evidence-File-Format (E01) gewählt, da dieses Format in die gewählte Forensik Software X-Ways eingebunden werden kann und gleichzeitig platzsparend ist. Generell muss im Vorfeld abgestimmt werden, welches der möglichen Formate für den konkreten Fall Sinn ergibt und welche Software die gewünschten Aufgaben am besten erledigen kann. Zusätzlich wird die Option „Verify images after they are created“ aktiviert, was einen automatischen Hash-Vergleich von Ziel und Quelle aktiviert.

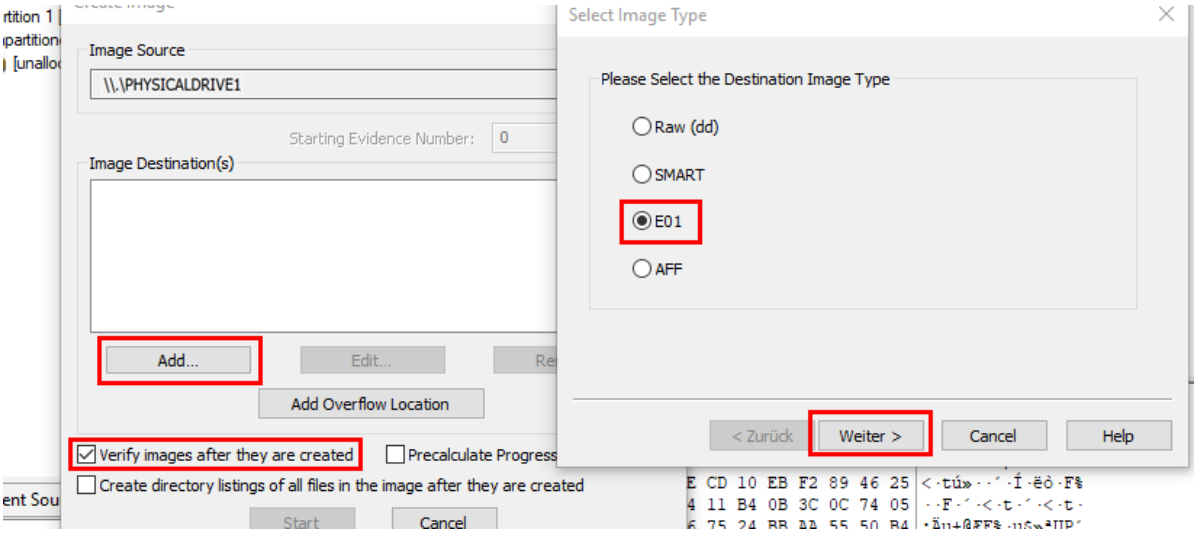


Abbildung 7: FTK Imager - Create Image

Nachdem das Zielformat gewählt ist, werden Metadaten zum Fall abgefragt. Diese werden im E01-File abgelegt und können im Nachgang bei einer möglichen Zuordnung zu einem Fall oder zu einem Beweisstück helfen.

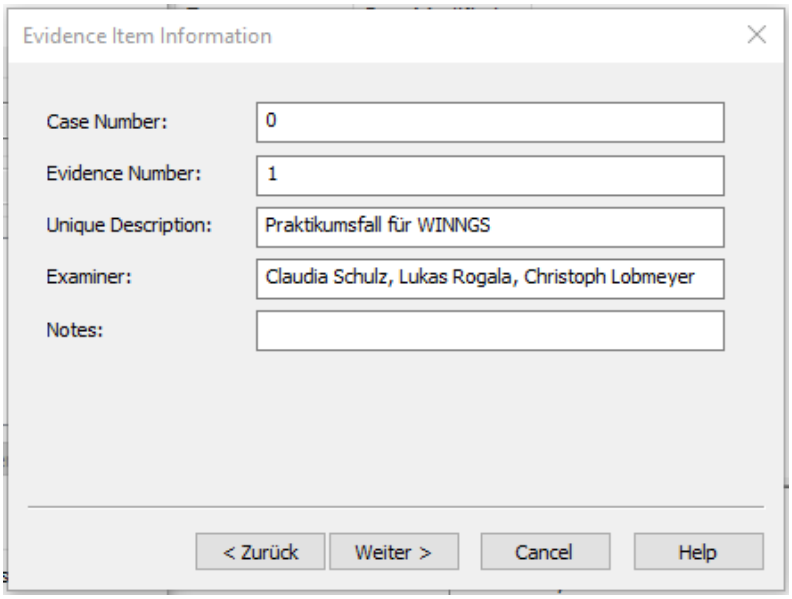


Abbildung 8: FTK Imager - Evidence Item Information

Zuletzt werden der Ziel-Pfad sowie der Dateiname abgefragt, an dem das erstellte Image unter dem zugewiesenen Namen abgelegt werden soll. Nach der Eingabe kann man den Destination-Dialog mit „`Finish`“ bestätigen und im „`Create Image`“-Fenster den Export-Vorgang mit „`Start`“ beginnen.

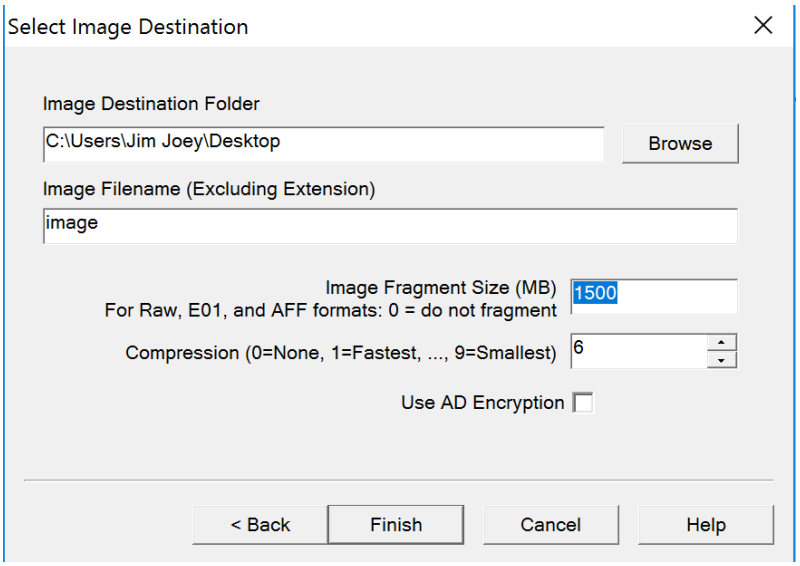


Abbildung 9: FTK Imager - Select Image Destination

Im Anschluss wird das Abbild gemäß den gewählten Einstellungen erstellt. Dieser Schritt kann je nach Größe sowie Festplattenanbindung bzw. Geschwindigkeit der Quelle mehr oder weniger Zeit in

Anspruch nehmen. Da die zu kopierende Festplatte eine Größe von 20 GB hat, kann der Vorgang in knapp 10 Minuten abgeschlossen werden.

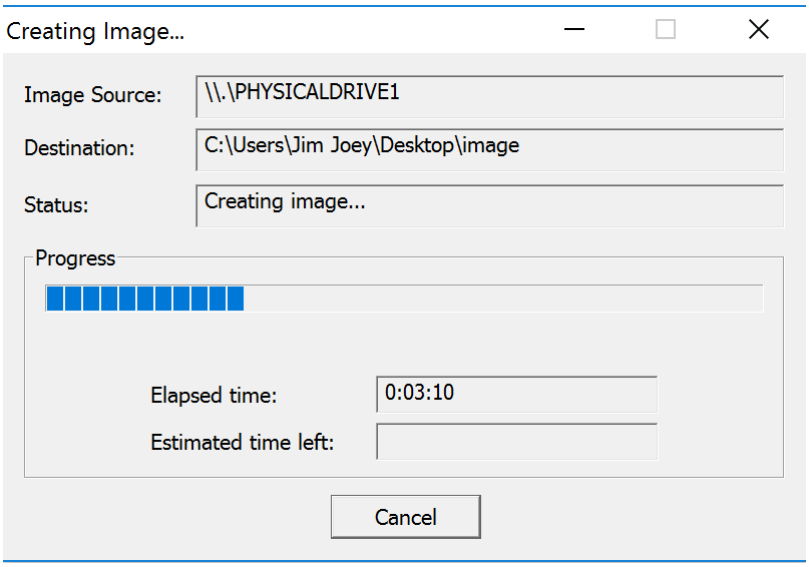


Abbildung 10: FTK Imager - Creating Image

3.2.3 Hashes generieren und vergleichen

Da die Funktion „`Verify images after they are created`“, siehe Abbildung 7: FTK Imager - Create Image, aktiviert wurde, startet der FTK `Imager` nach der Erstellung des Abbilds automatisch damit die Hashes des erstellten Images zu berechnen und mit dem Ausgangs-Hash der Quelle zu vergleichen. Dieser Vorgang nimmt je nach Image-Größe ebenfalls einige Zeit in Anspruch - im konkreten Fall sind dies knapp 5 Minuten.

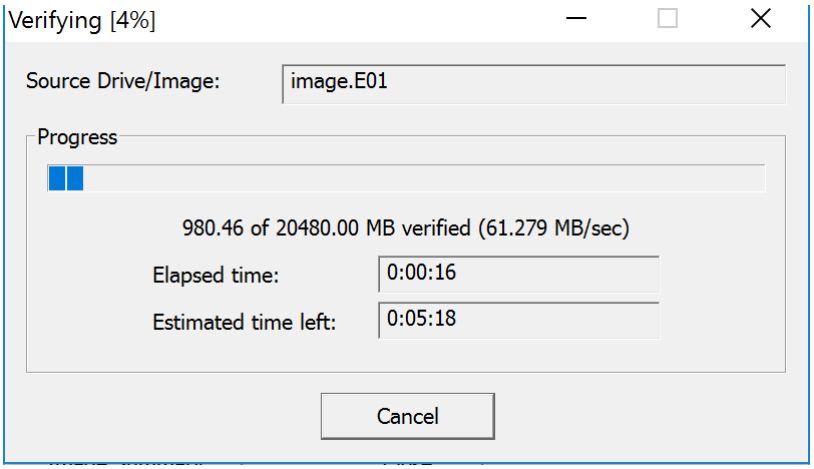


Abbildung 11: FTK Imager - Hashes berechnen und prüfen

Als letzten Schritt der Image-Erstellung gibt FTK `Imager` eine Übersicht der Image-Generierung inkl. berechneter MD5- sowie SHA1-Hashes der Quelle sowie des generierten Images aus. Sollten die Hashes nicht übereinstimmen, würde das Programm eine entsprechende Fehlermeldung ausgeben.

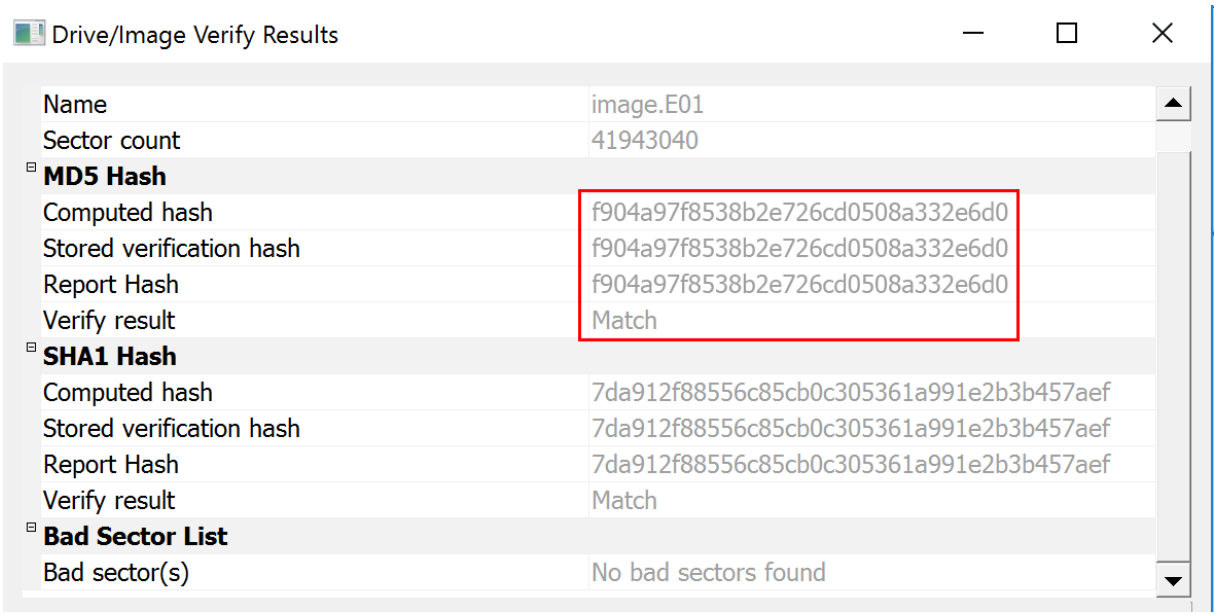


Abbildung 12: FTK Imager - Verify Results

Der generierte MD5-Hash wird auf dem Beweissicherungsprotokoll notiert und für spätere Vergleiche, zum Beispiel nach dem Import in der Forensik-Software, verwendet.

Anmerkung: In einem tatsächlichen forensischen Szenario würde die Sicherung (z.B. über einen RAID1-Verbund) doppelt erfolgen: Es würde eine Arbeitskopie und eine Beweissicherungskopie erstellt werden.

3.3 Hochladen in ein Forensik-System

Zuletzt wird das erstellte E01-File in ein Windows Forensik-System hochgeladen, auf dem das Analyse-Tool „`X-Ways Forensics`“ in der Version `19.6 SR-1` zur Verfügung steht. Damit lässt sich das Image einlesen, analysieren und auswerten. Diese Schritte werden in den nachfolgenden Kapiteln beschrieben.

4 Aufbereitung des Systems

Das Image wird in X-Ways Forensics geladen und zur weiteren Untersuchung aufbereitet. Hierfür werden die von X-Ways bereitgestellten Aufbereitungsfunktionen genutzt. Besonders relevant ist hier das sogenannte „File-Carving“, also das Untersuchen von nicht allokiertem Festplattenspeicher auf ehemals dort vorhandene Dateien, sowie die Extraktion von Metadaten und Inhalten (z.B. E-Mails) aus den zur Verfügung stehenden Daten.

4.1 Neuen Case erstellen

Über das Hauptmenü wird ein neuer Fall erstellt (Case Data > File > Create New Case). Dafür sind der Speicherpfad sowie verschiedene Metadaten wie ein Falltitel und zusätzliche Informationen wie die (optionale) Beschreibung plus Informationen der Untersuchenden anzugeben.

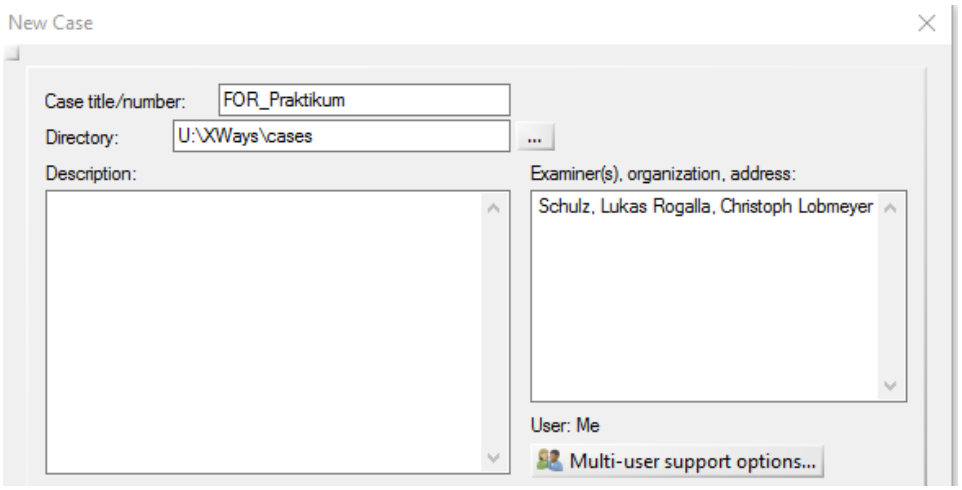


Abbildung 13: X-Ways - Case erstellen

4.2 Image-Datei einlesen

Sobald der Fall erstellt ist muss das hochgeladene Image in den Fall eingelesen werden. Diese Funktion wird über den Menüpunkt Case Data > File > Add Image gestartet.

4.3 Integrität über MD5-Hash überprüfen

Um die Integrität der Daten sicherzustellen wird der Hash des eingelesenen Images an dieser Stelle berechnet und mit dem Hash der Ausgangsdatei vergleichen. Dies wird über den Dialog „Properties > Verify Hash“ realisiert. Ein Vergleich mit *Abbildung 12: FTK Imager - Verify Results* zeigt, dass das Image korrekt hochgeladen und hinzugefügt wurde.

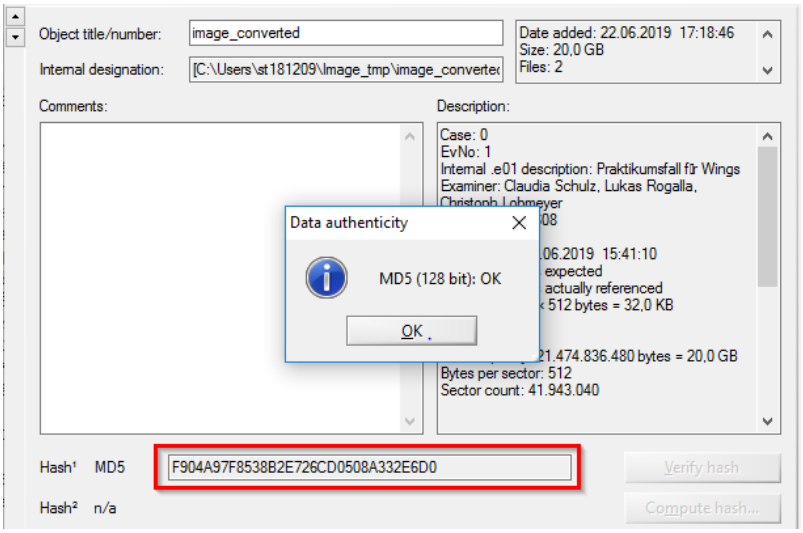


Abbildung 14: Verify Hash mit MD5

4.4 Aufbereitung der Daten mit X-Ways (Refine Volume Snapshot)

Über die Optionen von „`Refine Volume Snapshot`“ wird festgelegt, welche Aufbereitungsoptionen von `X-Ways` für die Aufbereitung des Festplattenimages angewendet werden sollen. Die Aktivierung einiger dieser Funktionen sorgt im Nachgang für ein weiteres Optionsfeld bzw. Popup. Nachfolgend die Dokumentation der Felder und der damit konfigurierten Aufbereitungsschritte.

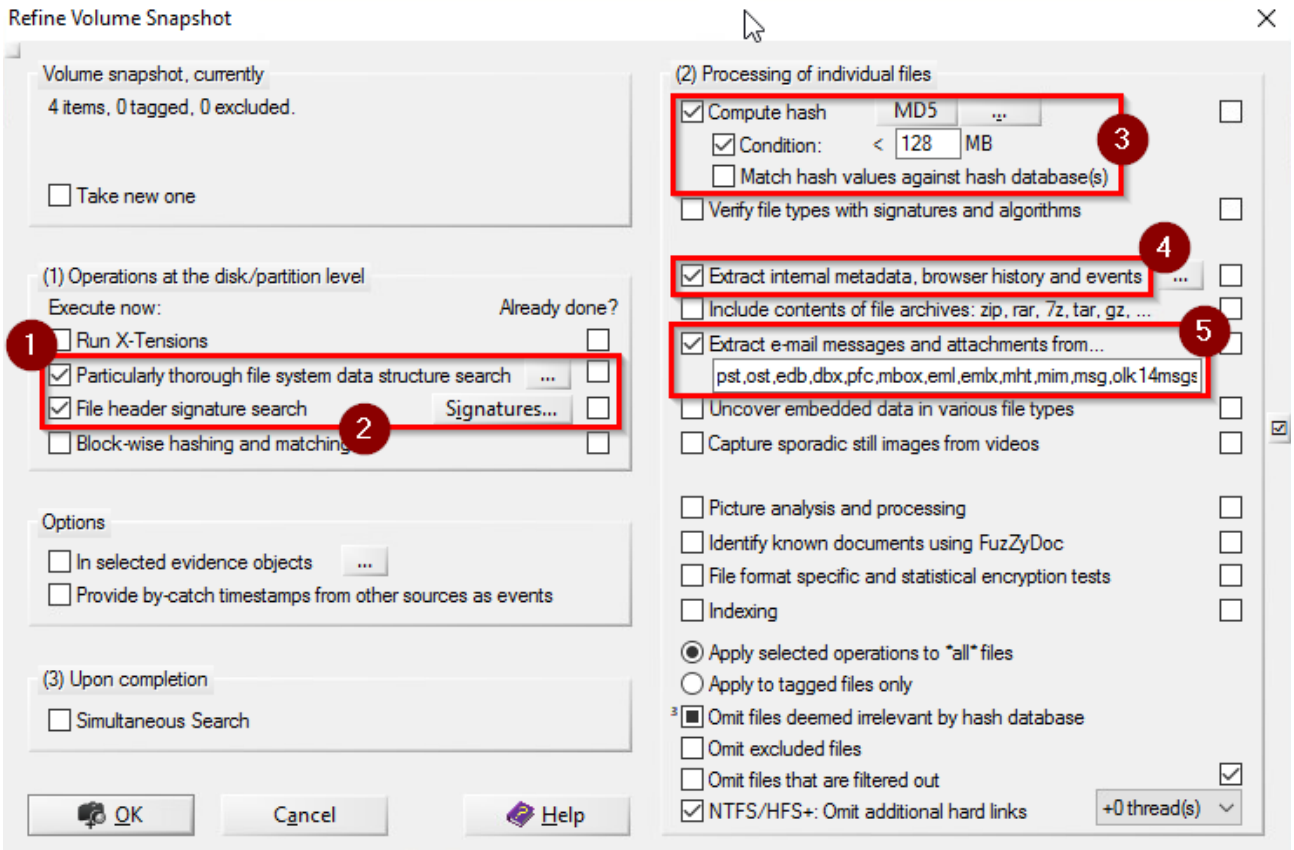


Abbildung 15: Refine Volume Snapshot

4.4.1 Particularly thorough file system data structure search (1)

Diese Funktion aktiviert die Auswertung von „`Volume Shadow Copies`“, also von Dateikopien, die das Dateisystem für verschiedene Zwecke (z.B. Backups) anlegt. Die Option „`Avoid identical SC previous versions`“ bewirkt, dass die Dateiversionen in den Shadow Copies verglichen werden. Jede Version wird nur einmal extrahiert. Mit der Option „`Include files whose clusters are unknown`“ werden auch solche Dateien angezeigt, bei denen nicht mehr klar ist, wo diese gespeichert sind. Hier werden dann nur noch die Metadaten angezeigt.

Über die Beschreibung „`List earlier names/paths`“ werden Verweise auf alte Dateinamen und Dateiorte (bei identischen Dateien) herausgearbeitet.

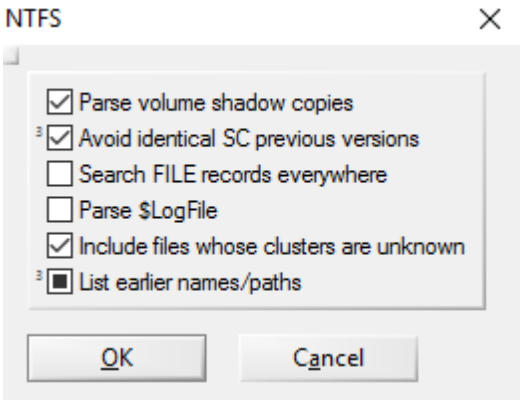


Abbildung 16: NTFS settings

4.4.2 File header signature search (2)

Über die Checkbox „`File Header Search`” wird dafür gesorgt, dass vom Dateisystem freigegebener Festplattenplatz nach den nachfolgend gewählten Dateitypheadern durchsucht wird („Carving“) und somit möglicherweise bereits gelöschte Dateien (bzw. genauer gesagt als gelöscht markierte Dateien) aufgefunden werden können. Im Detail-Optionsfeld werden alle bekannten Formate von E-Mails sowie im Oberpunkt „Programme“ ausführbare Dateien der windowsspezifischen Programme aktiviert, da es sich bei dem vorliegenden Fall um eine Analyse eines mutmaßlichen IT-Sicherheitsvorfalls handelt und E-Mails ein häufiger Angriffsvektor auf Benutzer sind.

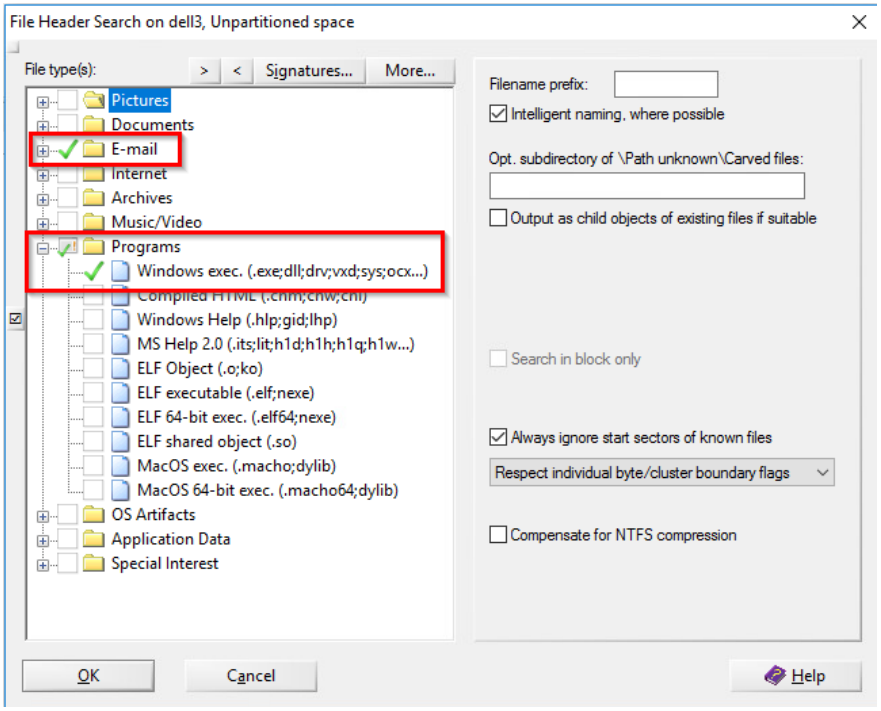


Abbildung 17: File Header Search

4.4.3 Compute Hash (3)

Über diese Option wird festgelegt, dass X-Ways zu jeder Datei einen Hash generiert, den man für weitere Zwecke wie z.B. den Abgleich mit Datenbanken verwenden kann. Sollten Listen von bekanntermaßen gutartigen Dateien (z.B. des Betriebssystems) vorliegen, können diese Dateien bereits aus dem Untersuchungsfokus genommen werden. Dadurch reduziert sich die Datenmenge, die untersucht werden muss. Auch der umgekehrte Weg ist möglich: Sind bereits Hashes von Schadsoftware bekannt, so könnten diese ebenfalls leichter gefunden und als relevant markiert werden. Um Ressourcen zu schonen wird MD5 verwendet und Dateien mit mehr als 128MB übersprungen. Üblicherweise hat Malware eine deutlich geringere Größe.

4.4.4 Extract internal metadata, browser history and events (4)

Da bei der geschilderten Problembeschreibung davon auszugehen ist, dass das System über eine Nutzereingabe kompromittiert wurde, werden E-Mail und Browser - Haupteinfallstor für Schadsoftware - als mutmaßlicher Einstiegspunkt definiert. Um Browseraktivitäten aufzubereiten wird die Option „Extract internal metadata, browser history and events“ aktiviert und im nachfolgenden Detail-Fenster die hierfür benötigten Dateitypen ausgewählt.

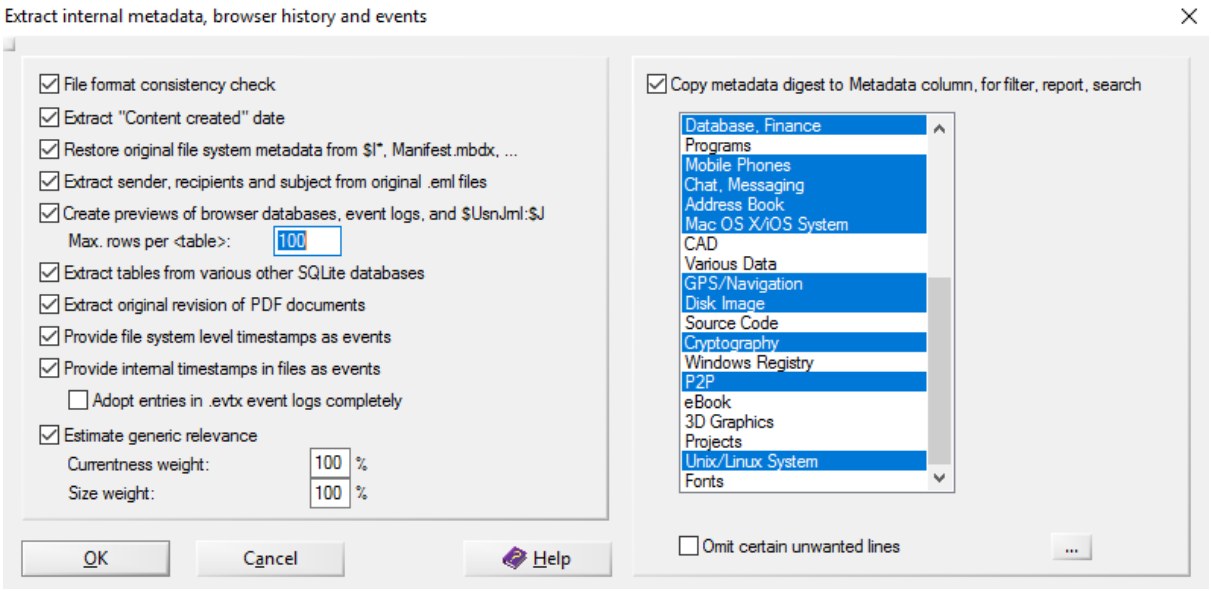


Abbildung 18: Extract internal metadata, browser history and events

4.4.5 Extract e-mail messages and attachments from… (5)

Zuletzt wird die Option „`Extract e-mail messages`“ aktiviert, da eine E-Mail eines der Haupteinfallstore für Schadsoftware ist. Dadurch werden aus den proprietären E-Mail-Datenbanken (z.B. *.pst-Dateien) die E-Mails samt ihren Metadaten extrahiert. Würde dieser Schritt entfallen, würde man nur die Datenbank als Gesamtes finden, ohne die darin enthaltenen E-Mails und der dazugehörigen Metadaten.

4.5 Aufbereitung durchführen

Nachdem die Konfiguration durchgeführt wurde, werden die vorgegebenen Analyseschritte mit einem Klick auf „OK“ sequenziell durchgeführt. Bei dem vorliegenden Image dauert der Vorgang etwa 15 Minuten. Während des Durchlaufens der Analyseschritte wird durch `X-Ways` eine interne Datenbank aufgebaut, sodass die Untersuchung anschließend auf dieser Datenbank erfolgt. Dies gilt, solange nicht der Inhalt der eigentlichen Dateien untersucht wird.

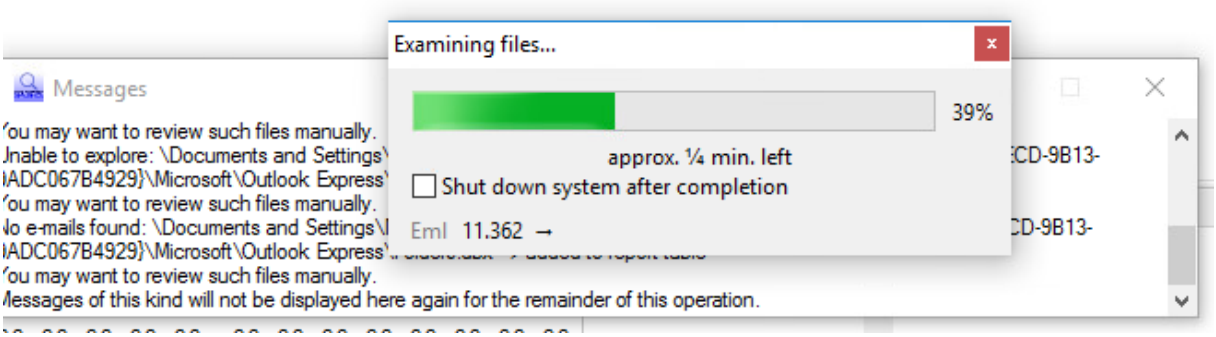


Abbildung 19: Untersuchung des Images

5 Untersuchungsschritte

Nachdem die Dateien von X-Ways eingelesen sind kann im weiteren Verlauf in die nähere Analyse und Auswertung der gesammelten Daten eingestiegen und so der Vorfall rekonstruiert werden.

5.1 Identifikation des Systems

Vor der eigentlichen Analyse des Systems, muss dieses zunächst zweifelsfrei identifiziert werden, um sicherzustellen, dass das korrekte IT-System analysiert wird. Dies geschieht bei Windows-Systemen in der Regel über die Analyse einiger Registry-Schlüssel (genaueres Vorgehen siehe Systeminformationen aus der Registry).

Dort werden eindeutige Kennzeichen des IT-Systems extrahiert. Gegenstand der hier dokumentierten forensischen Untersuchung ist das folgende System:

Kennzeichen	Wert
Hostname	WIN-BS9RVGO8L4V
Zeitzone	MESZ
IP-Adresse	192.168.2.129
Angemeldete Benutzer	„Günther Kastenfrosch“
Betriebssystem	Windows 7 Professional

5.2 Untersuchung der Ursache

Da, wie in Kapitel 4.4.4 und 4.4.5 beschrieben, davon auszugehen ist, dass das System durch eine Nutzerinteraktion kompromittiert wurde beginnt die Suche in Windows „Users“-Verzeichnis. Auf dem System wird nur ein persönlicher Benutzerordner („Günther Kastenfrosch“) gefunden, der als Ausgangspunkt der Suche gewählt wird. Um alle Unterordner in die Suche einzuschließen, muss der Ordner im linken Dateibaum mit der rechten Maustaste ausgewählt werden; ein kleines Icon neben dem Ordnernamen zeigt an, dass die Unterordner mit dargestellt werden.

In dieser Ansicht springt sofort eine Datei mit dem Namen „RyukReadMe.txt“ in den Fokus. Diese Datei ist vielfach auf dem Client-System vorhanden und beinhaltet einen Text, der typisch für einen sogenannten „Erpressungstrojaner“ ist. Der Inhalt der TXT-Datei kann über die „Preview“ im unteren Fenster eingesehen werden.

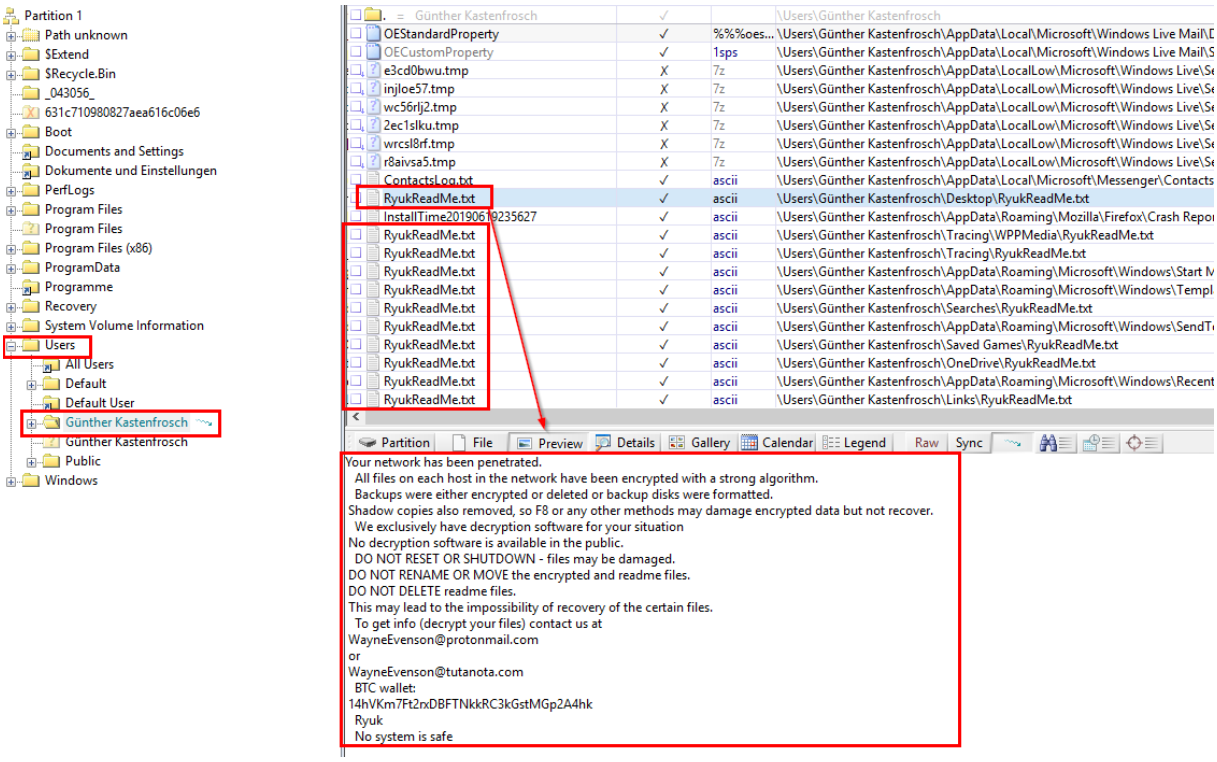


Abbildung 20: Untersuchung des Benutzer-Verzeichnisses

Um den Vorgang besser nachvollziehen zu können ist es wichtig zu prüfen, welche Aktionen seitens des Systems um diese Datei geschehen sind. X-Ways extrahiert in der Analysephase mehrere Timestamps die wir hierzu verwenden können. Sinnvoll ist an dieser Stelle eine Sortierung nach „Record changed“, da jede Änderung an den Metadaten der Datei betrachtet werden muss, um z.B. auch Anpassungen an Betriebssystemdateien oder Benutzerberechtigungen zu erkennen. An dieser Stelle wird die wichtige Information notiert, dass am 22.06.2019 um 12:57 MESZ etwas am System passiert ist und es zu prüfen gilt, was um diesen Timestamp herum Interessantes geschehen ist.

Full path	Type	Size	Created	Modified	Record changed
\Users		1,2 GB	14.07.2009 05:20:08,8 +2	28.05.2019 20:27:52,6 +2	28.05.2019 20:27:52,6 +2
\Users\Günther Kastenfrosch		1,1 GB	28.05.2019 20:27:52,6 +2	22.06.2019 12:57:00,7 +2	22.06.2019 12:57:00,7 +2
\Users\Günther Kastenfrosch\RyukReadMe.txt	ascii	0,8 KB	22.06.2019 12:57:00,7 +2	22.06.2019 12:57:00,7 +2	22.06.2019 12:57:00,7 +2
\Users\Günther Kastenfrosch\AppData\Roaming\RyukReadMe.txt	ascii	0,8 KB	22.06.2019 12:57:00,7 +2	22.06.2019 12:57:00,7 +2	22.06.2019 12:57:00,7 +2
\Users\Günther Kastenfrosch\AppData\RyukReadMe.txt	ascii	0,8 KB	22.06.2019 12:57:00,7 +2	22.06.2019 12:57:00,7 +2	22.06.2019 12:57:00,7 +2
\Users\Günther Kastenfrosch\AppData\Local\Microsoft\RyukReadMe...	ascii	0,8 KB	22.06.2019 12:57:00,7 +2	22.06.2019 12:57:00,7 +2	22.06.2019 12:57:00,7 +2
\Users\Günther Kastenfrosch\AppData\Local\Microsoft\Credentials\...	ascii	0,8 KB	22.06.2019 12:57:00,7 +2	22.06.2019 12:57:00,7 +2	22.06.2019 12:57:00,7 +2

Abbildung 21: Timestamp der RyukReadMe.txt

Als nächster Schritt wird die Menge an Daten eingeschränkt, indem ein Filter auf die Spalte „Record Changed“ gesetzt wird. Es wird sich auf die Zeit ab 12:50 Uhr MESZ bis zum Tagesende des o.g. Tages konzentriert, um alle Ereignisse bis zum Herunterfahren des Systems anzuzeigen. Nachdem der Filter aktiv ist werden die verbliebenen Objekte nach dem Timestamp sortiert.

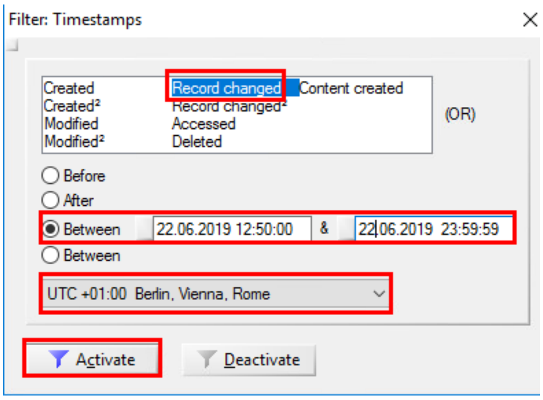
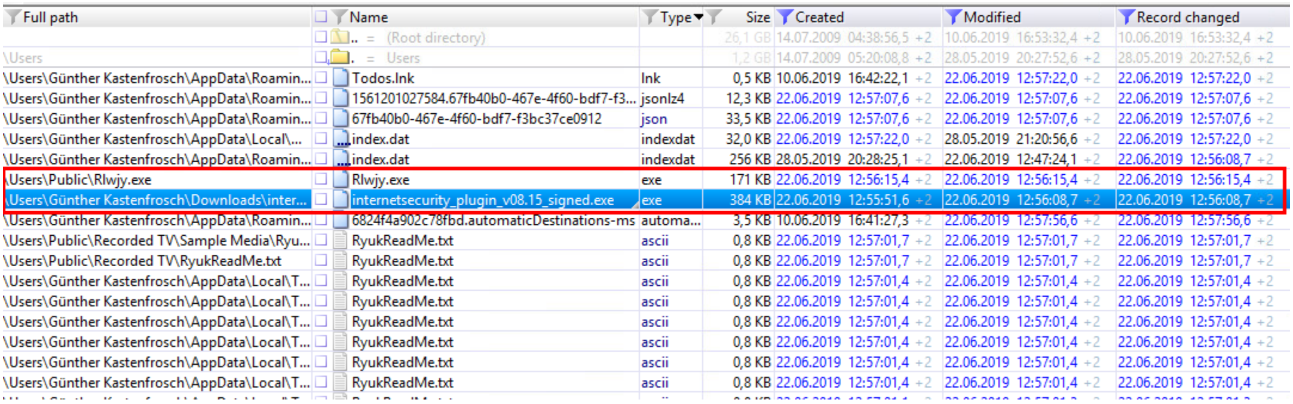


Abbildung 22: Datenmenge nach Timestamp einschränken

Nachdem die Objekte sortiert sind wird ersichtlich, dass kurz vor dem Ausbruch und dem Anlegen der „`RyukReadMe`"-Files an zwei ausführbaren EXE-Dateien Änderungen durchgeführt wurden[1]. Dies ist zum einen die Datei „`internetsecurity_plugin_v08.15_signed.exe`" im `Downloads`-Verzeichnis des Benutzers und zum anderen die „`Rlwjy.exe`" im `Public User`-Ordner.



Full path	Name	Type	Size	Created	Modified	Record changed
	.. = (Root directory)		26,1 GB	14.07.2009 04:38:56,5 +2	10.06.2019 16:53:32,4 +2	10.06.2019 16:53:32,4 +2
\Users	. = Users		1,2 GB	14.07.2009 05:20:08,8 +2	28.05.2019 20:27:52,6 +2	28.05.2019 20:27:52,6 +2
\Users\Günther Kastenfrosch\AppData\Roamin...	Todos.lnk	lnk	0,5 KB	10.06.2019 16:42:22,1 +2	22.06.2019 12:57:22,0 +2	22.06.2019 12:57:22,0 +2
\Users\Günther Kastenfrosch\AppData\Roamin...	1561201027584.67fb40b0-467e-4f60-bdf7-f3...	jsonlz4	12,3 KB	22.06.2019 12:57:07,6 +2	22.06.2019 12:57:07,6 +2	22.06.2019 12:57:07,6 +2
\Users\Günther Kastenfrosch\AppData\Roamin...	67fb40b0-467e-4f60-bdf7-f3bc37ce0912	json	33,5 KB	22.06.2019 12:57:07,6 +2	22.06.2019 12:57:07,6 +2	22.06.2019 12:57:07,6 +2
\Users\Günther Kastenfrosch\AppData\Local\...	index.dat	indexdat	32,0 KB	22.06.2019 12:57:22,0 +2	28.05.2019 21:20:56,6 +2	22.06.2019 12:57:22,0 +2
\Users\Günther Kastenfrosch\AppData\Roamin...	index.dat	indexdat	256 KB	28.05.2019 20:28:25,1 +2	22.06.2019 12:47:24,1 +2	22.06.2019 12:56:08,7 +2
\Users\Public\Rlwjy.exe	Rlwjy.exe	exe	171 KB	22.06.2019 12:56:15,4 +2	22.06.2019 12:56:15,4 +2	22.06.2019 12:56:15,4 +2
\Users\Günther Kastenfrosch\Downloads\inter...	internetsecurity_plugin_v08.15_signed.exe	exe	384 KB	22.06.2019 12:55:51,6 +2	22.06.2019 12:56:08,7 +2	22.06.2019 12:56:08,7 +2
\Users\Günther Kastenfrosch\AppData\Roamin...	6824f4a902c78fbd.automaticDestinations-ms	automa...	3,5 KB	10.06.2019 16:41:27,3 +2	22.06.2019 12:57:56,6 +2	22.06.2019 12:57:56,6 +2
\Users\Public\Recorded TV\Sample Media\Ryu...	RyukReadMe.txt	ascii	0,8 KB	22.06.2019 12:57:01,7 +2	22.06.2019 12:57:01,7 +2	22.06.2019 12:57:01,7 +2
\Users\Public\Recorded TV\RyukReadMe.txt	RyukReadMe.txt	ascii	0,8 KB	22.06.2019 12:57:01,7 +2	22.06.2019 12:57:01,7 +2	22.06.2019 12:57:01,7 +2
\Users\Günther Kastenfrosch\AppData\Local\T...	RyukReadMe.txt	ascii	0,8 KB	22.06.2019 12:57:01,4 +2	22.06.2019 12:57:01,4 +2	22.06.2019 12:57:01,4 +2
\Users\Günther Kastenfrosch\AppData\Local\T...	RyukReadMe.txt	ascii	0,8 KB	22.06.2019 12:57:01,4 +2	22.06.2019 12:57:01,4 +2	22.06.2019 12:57:01,4 +2
\Users\Günther Kastenfrosch\AppData\Local\T...	RyukReadMe.txt	ascii	0,8 KB	22.06.2019 12:57:01,4 +2	22.06.2019 12:57:01,4 +2	22.06.2019 12:57:01,4 +2
\Users\Günther Kastenfrosch\AppData\Local\T...	RyukReadMe.txt	ascii	0,8 KB	22.06.2019 12:57:01,4 +2	22.06.2019 12:57:01,4 +2	22.06.2019 12:57:01,4 +2
\Users\Günther Kastenfrosch\AppData\Local\T...	RyukReadMe.txt	ascii	0,8 KB	22.06.2019 12:57:01,4 +2	22.06.2019 12:57:01,4 +2	22.06.2019 12:57:01,4 +2
\Users\Günther Kastenfrosch\AppData\Local\T...	RyukReadMe.txt	ascii	0,8 KB	22.06.2019 12:57:01,4 +2	22.06.2019 12:57:01,4 +2	22.06.2019 12:57:01,4 +2

Abbildung 23: Verdächtige EXE-Dateien

Bei der Datei „`internetsecurity_plugin_v08.15_signed.exe`", die offensichtlich in das `Downloads`-Verzeichnis aus dem Internet heruntergeladen wurde, lassen sich weitere Metadaten extrahieren. Dies funktioniert entweder über das Einblenden der entsprechenden Spalte oder über einen Rechtsklick mit der Funktion „`Edit Metadaten`". Hier kann die URL, über die das File geladen wurde, extrahiert werden. Die Web-Adresse lautet:

„*webcheckemailandinternetsecurity-centercomslash.de/internetsecurity_plugin_v08.15_signed.exe*".

[1] Anmerkung: Die Erstellung einer Datei ist auch eine Änderung

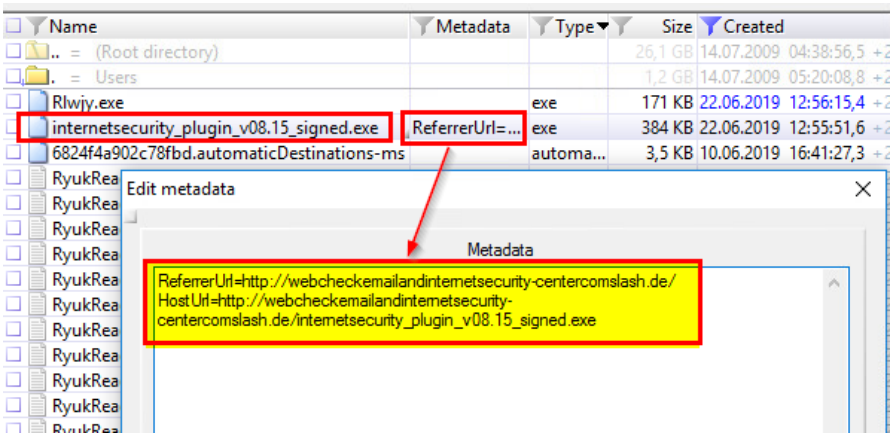


Abbildung 24: Metadaten

Damit ist bekannt, welche Datei die Kontamination ausgelöst hat und aus welcher Quelle sie stammt.

5.3 Untersuchung der Malware (auf öffentlichen Quellen)

Um sicher zu gehen, dass die gefundenen Dateien tatsächlich der Ursprung der Kontamination sind, wird der Online-Dienst `VirusTotal.com` verwendet. Eine Möglichkeit ist es, die Datei aus dem Image zu extrahieren und auf die Webseite zur weiteren Prüfung hochzuladen. Dabei wird die ausführbare Datei jedoch auch bei VirusTotal abgelegt. Eine andere Möglichkeit ist, die Datenbank des Webdienstes nach dem von `X-Ways` berechneten Hash (`5ac0f050f93f86e69026faea1fbb4450`) zu durchsuchen, was in diesem Fall einen Treffer ergibt und die Ransomware Ryuk identifiziert.

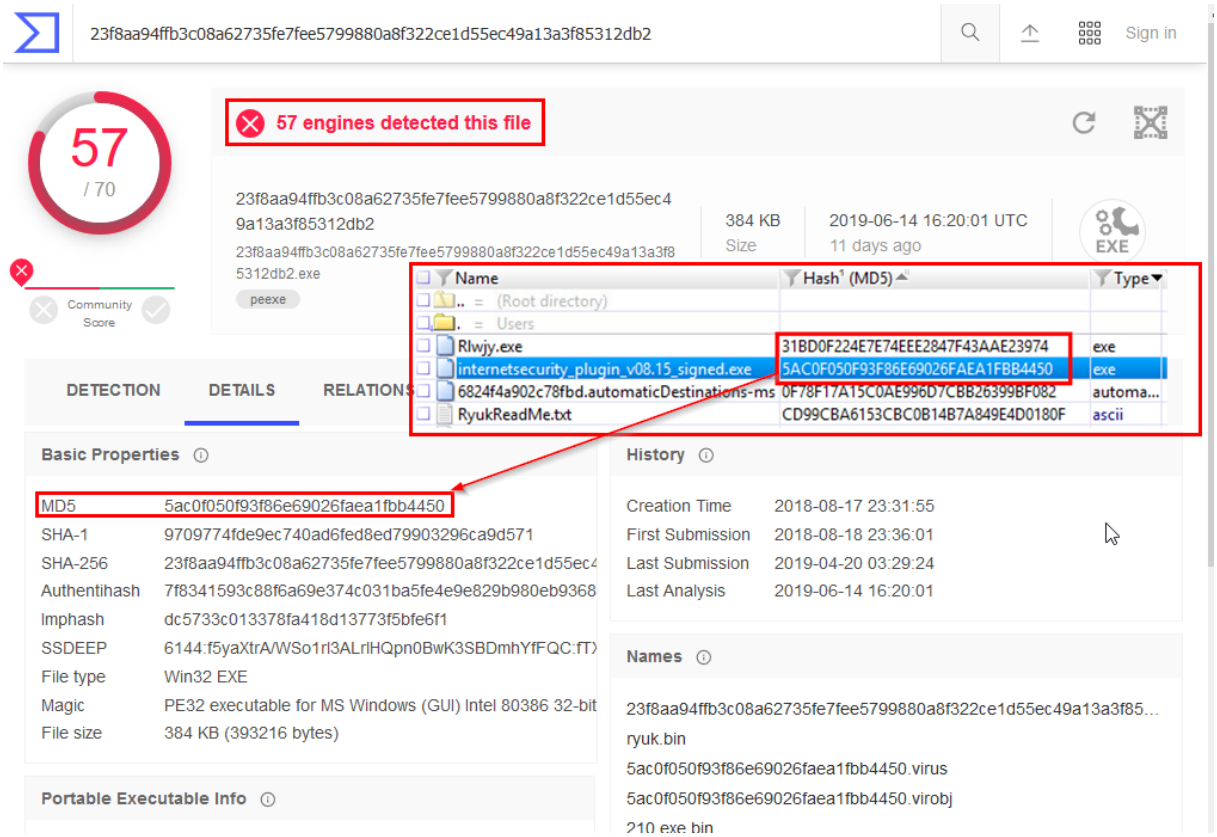


Abbildung 25: Virustotal.com - Hashabgleich - internetsecurity_plugin_v08.15_signed.exe

Sofern ein Virus bereits bekannt ist, können hier auch das typische Verhalten und die Beziehungen der schadhaften Datei nachvollzogen werden. Der Webdienst gibt auch einen guten Anhaltspunkt, wie die Schadsoftware Persistenz erzeugt und welche konkreten Dateien sie dazu liest/schreibt.

Der Abgleich vom Hash der ebenfalls identifizierten Datei „`Rlwjy.exe`“ gibt keinen Treffer zurück. Dies lässt sich darauf zurückführen, das die Datei von der ersten Schadsoftware (Stager) erzeugt wird und für jeden Angriff ein individueller Verschlüsselungskey erzeugt wird. Da dieser Verschlüsselungskey in der zweiten Datei (Payload) enthalten ist, unterscheidet sich der Hash bei jedem Opfer.

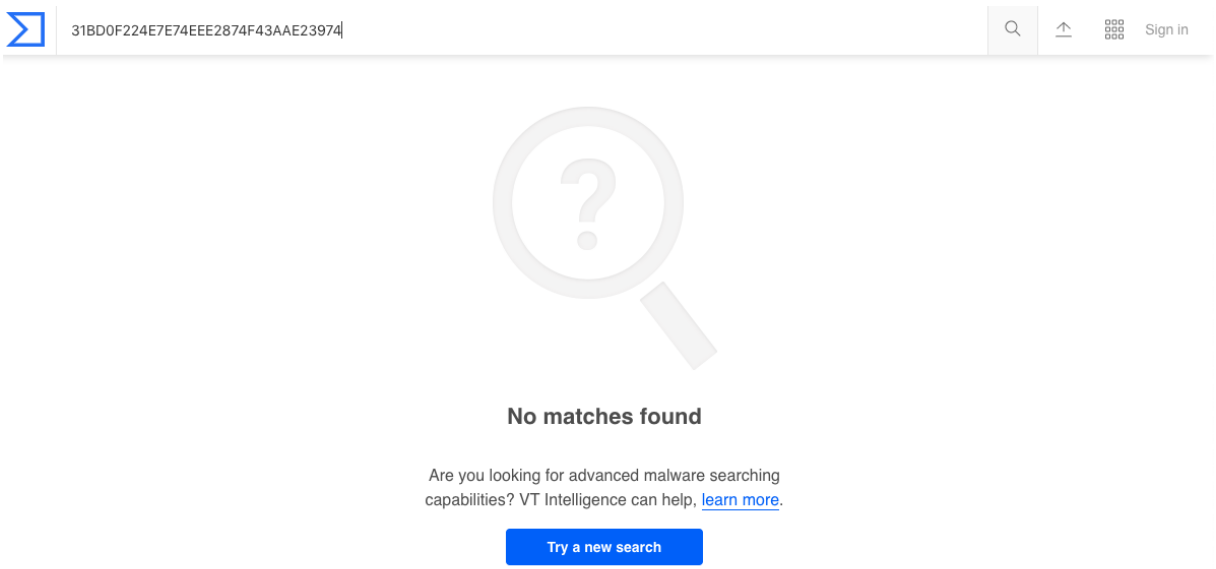


Abbildung 26: Virustotal.com - Hashabgleich - Rlwjy.exe

5.4 Untersuchung des Email-Verkehrs (Windows Live Mail)

Um herauszufinden, wo die Schadsoftware ihren Ursprung hat bzw. warum der Nutzer den Link aufgerufen hat, werden die beiden oben erwähnten Ansätze „E-Mail & Browser“ weiterverfolgt. Im AppData-Ordner des Benutzers konnte unter „`%localappdata%\Local\Microsoft\Windows Live Mail\[redacted]e34\Posteingang\`“ ein Ordner mit drei E-Mails identifiziert werden. Eine davon hat den Betreff „*`Test`*“, zwei weitere „*`DRINGEND: Internet Security Center, Sicherheit Ihres E-Mailzugangs`*“.

Mit `X-Ways` kann beim Anklicken der E-Mail im Bereich „`Preview`“ der Text eingesehen werden. Aus dieser E-Mail geht hervor, dass es sich um eine reine HTML-Mail ohne Anhang handelt. Der Text suggeriert dem Nutzer, dass er „gehacked“ wurde und eine Aktion seinerseits erforderlich ist. Im zweiten Absatz darauf hingewiesen, dass der Nutzer evtl. ein Plugin installieren muss.

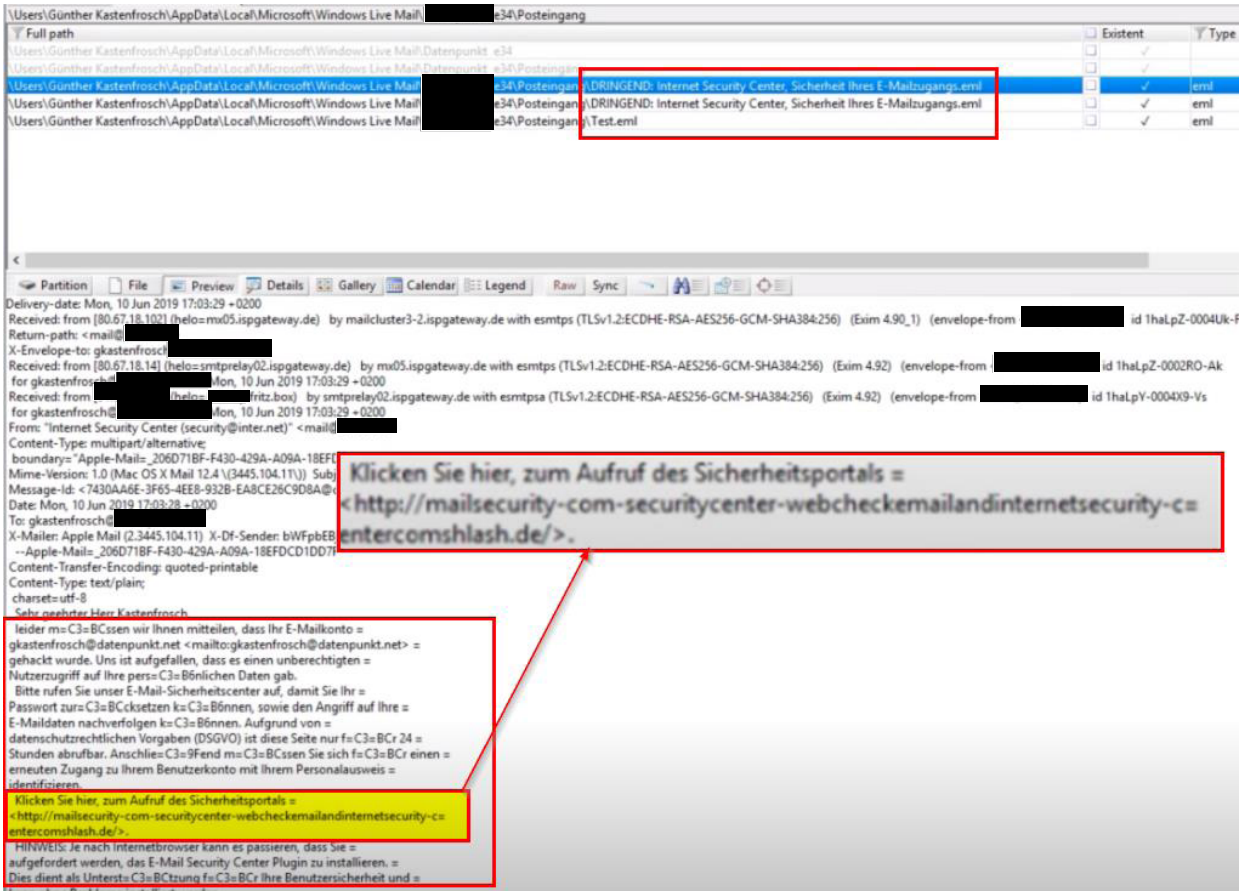


Abbildung 27: Gefundene E-Mail-Elemente

Da es sich um einen Weblink handelt wird die Suche an dieser Stelle ausgesetzt und im Browser, mit dem der Link vermutlich geöffnet wurde, fortgeführt.

5.5 Untersuchung des Webbrowsers (Firefox)

Auf dem Rechner wird im AppData-Ordner ein Profil des Webbrowsers „Mozilla Firefox“ gefunden, was vermutlich der verwendete Browser von Herrn Kastenfrosch ist. Als Startpunkt ist es sinnvoll das Surfverhalten des Nutzers zu betrachten.

5.5.1 Firefox Thumbnails

Eine Untersuchung des Profil-Ordners unter %Localappdata%\Mozilla\Firefox\ führt zum Unterordner „thumbnails“, der kleine Vorschaubilder einiger zuletzt besuchter Webseiten enthält. Eines der kleinen Bilder zeigt eine Webseite, die verdächtig nach dem Downloadlink des suggerierten Plugins in der E-Mail aussieht. Dadurch kann man sicher sein, dass der richtige Browser gefunden wurde und der Angriff über diesen stattfand.

Abbildung 28: Thumbnail-Vorschau einer Webseite

5.5.2 Firefox Bookmarks, History und Chronik (places.sqlite)

Ein guter Ansatzpunkt für die Auswertung von Firefox bietet sich im `Profil`-Ordner mit der Datei „`places.sqlite`“ an. Diese speichert Lesezeichen, Downloads sowie die Chronik des Benutzers und liegt im Ordner „`%APPDATA%\Mozilla\Firefox\Profiles\`“. Über `Rechtsklick > „Recover/Copy“` kann die Datei aus dem Image extrahiert und weiterverarbeitet werden – dies wird an dieser Stelle getan.

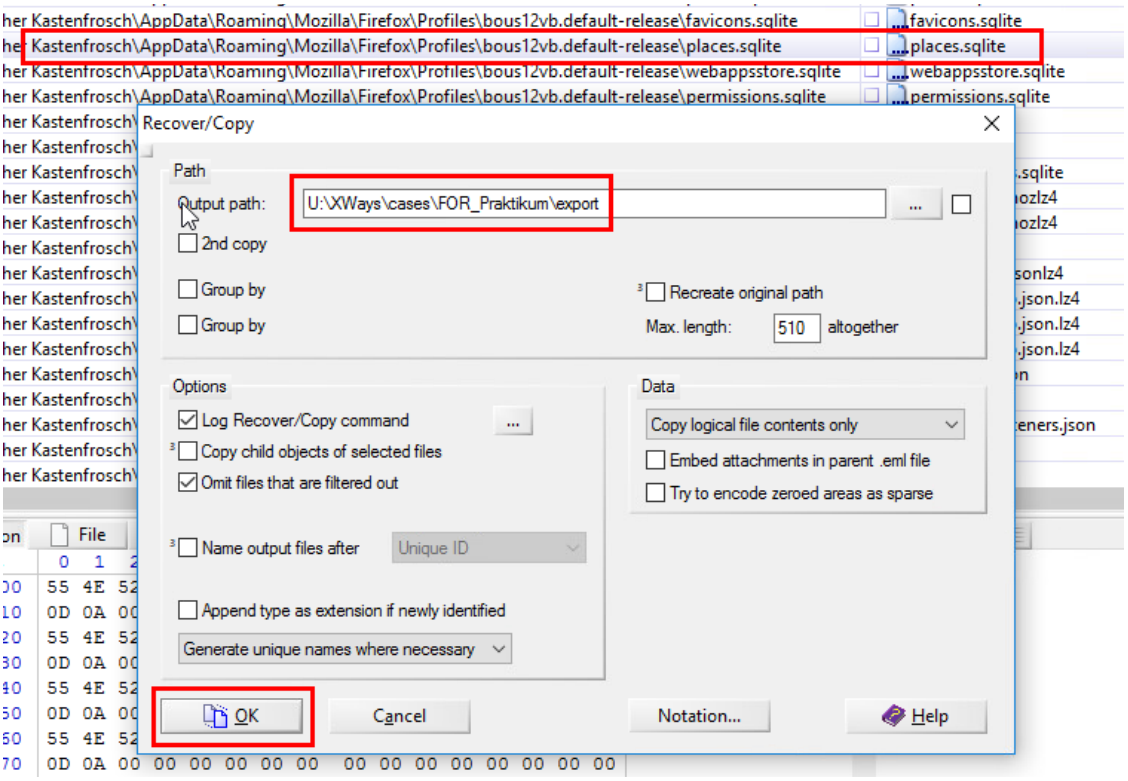


Abbildung 29: Export der Firefox-Datenbank places.sqlite

Die exportierte Datei `places.sqlite` kann anschließend mit einem beliebigen Tool geöffnet werden, das SQLite-Datenbanken unterstützt. In diesem Fall wird das Programm `SQLite Forensic`

Explorer vom Hersteller Acquire Forensics in der Version 2.0 verwendet. Das Schema der Datenbank kann bei Mozilla[2] eingesehen werden.

In der Tabelle moz_origins können die besuchten Hosts samt verwendetem Protokoll ausgelesen werden. Als eine der letzten besuchten Seiten fällt die Webseite auf, die in *Untersuchung der Ursache* bereits als Quelle für die heruntergeladene Schadsoftware identifiziert wurde.

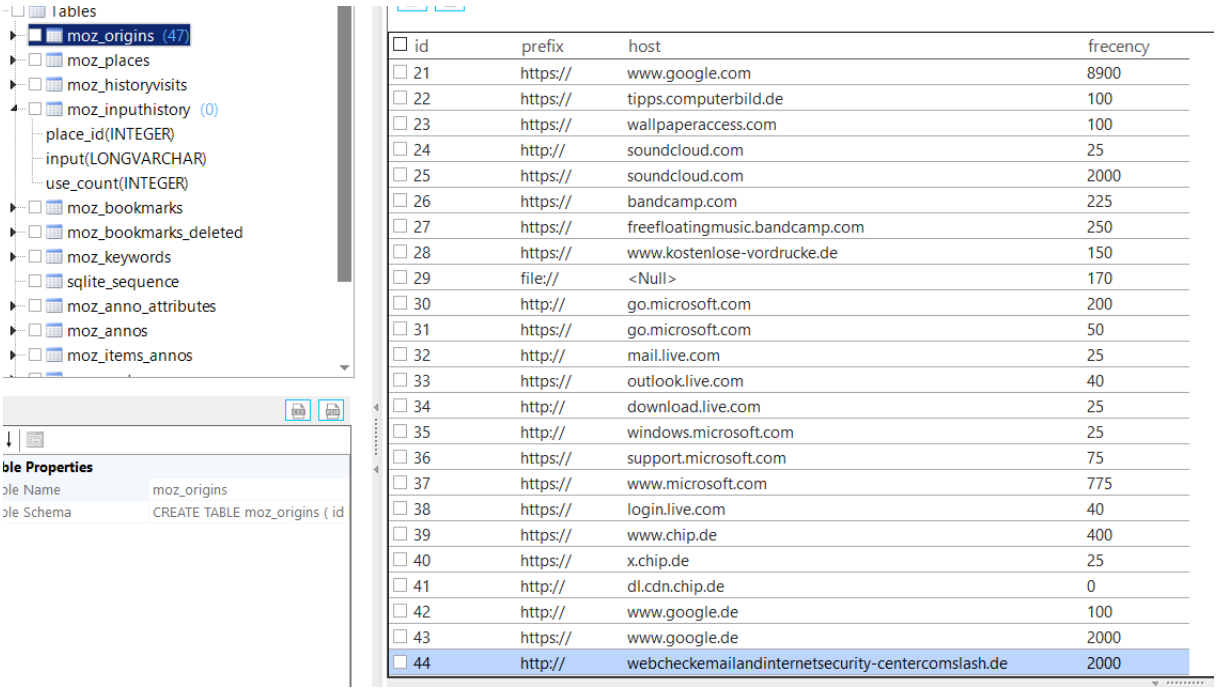


Abbildung 30: Firefox places.sqlite - moz_origins

Die Tabelle moz_places listet hingegen die konkret aufgerufenen Webseiten auf; auch hier taucht die identifizierte Seite sowie der konkrete Downloadlink der schadhaften Software in der Liste auf.

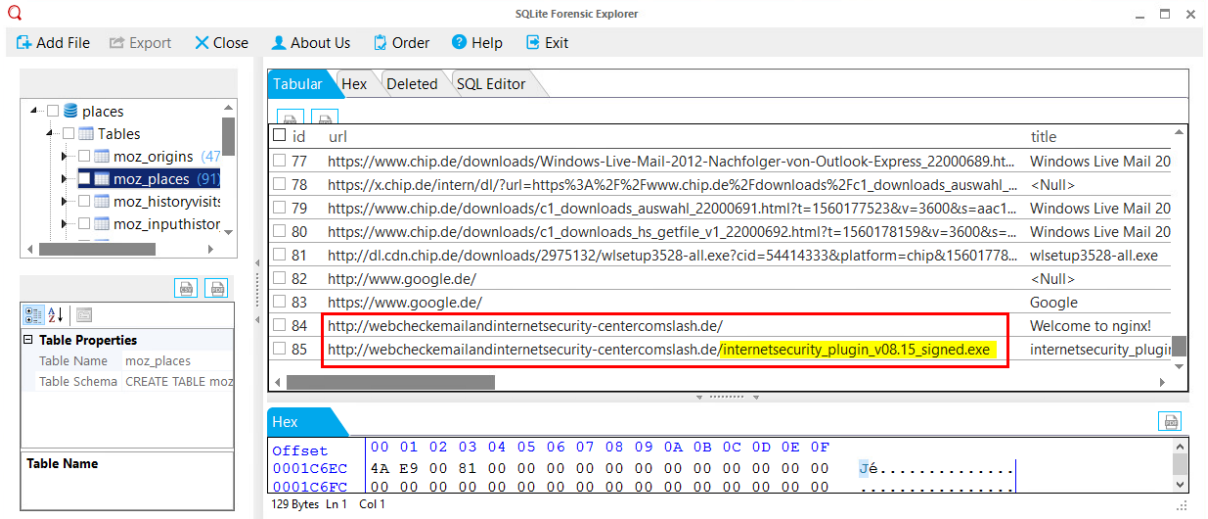


Abbildung 31: Firefox places.sqlite - moz_places

[2] https://developer.mozilla.org/en-US/docs/Mozilla/Tech/Places/Database

Ein weiterer interessanter Aspekt in den `moz_places` sind aufgerufene URLs. Insbesondere die Einträge, die bei der Suche über Google angefallen sind. Anhand des Datenbankauszugs ist ersichtlich, dass der Benutzer unter anderem nach den beiden Suchbegriffen *„anti virus macht den computer langsam“* und *„windows defender ausschalten“* über den Dienst Google recherchiert hat. Es ist daher davon auszugehen, dass er seinen `Windows Defender` deaktiviert hat, um den PC mutmaßlich schneller zu machen.

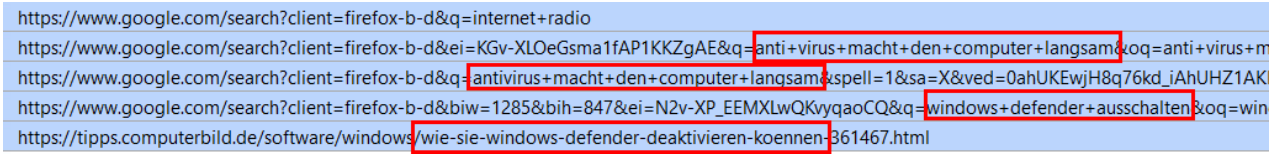


Abbildung 32: Firefox places.sqlite - moz_places - Sucheingaben

5.6 Untersuchung der Email

Die E-Mail wurde am 22. Juni 2019 um 12:36:40 (MESZ) vom Host `mailcluster3-2.ispgateway.de` verschlüsselt über das Mailprotokoll SMTP mit der IP-Adresse `80.67.18.23` abgerufen. Dieser Host antwortet mit dem Hostnamen `mx14.ispgateway.de`. Eine Whois-Abfrage dieser IP-Adresse deutet daraufhin, dass die IP-Adresse zum Internet Service Provider „Domainfactory“ gehört.

Der Host `mx14.ispgateway.de` hat die E-Mail wiederum vom Host mit der IP `80.67.31.29` (Hostname `smtprelay02.ispgateway.de`), ebenfalls per verschlüsselter SMTP-Verbindung erhalten.

`smtprelay02.ispgateway.de` hat die E-Mail wiederum von einem Host mit der IP 91.[redacted].[redacted].15 (Hostname [redacted]`.fritz.box`) erhalten. Der Anzeigename der E-Mail war „`Internet Security Center (security@inter.net)`“, tatsächlich (also technisch) hatte die E-Mail jedoch den Absender `mail@`[redacted]`.de`. Außerdem lässt sich aus den Metadaten identifizieren, dass die ursprüngliche E-Mail über das E-Mail-Programm `Apple Mail` verschickt wurde.

Der Hostname des Absenders ([redacted]`.fritz.box`) deutet darauf hin, dass die E-Mail aus einem eher kleineren Netzwerk versendet wurde, da der Suffix des Hostnames `fritz.box` auf die Verwendung eines Home/Small Business Routers der Firma AVM hinweist. Die IP-Whois-Abfrage auf die dazugehörige IP-Adresse 91.[redacted].[redacted].15 gibt zurück, dass diese IP-Adresse zum Netzbereich von Vodafone Kabel Deutschland gehört.

Da die E-Mail nach dem Versand nicht mehr den E-Mail-Anbieter gewechselt hat (alle IPs, außer dem ursprünglichen Absender gehören zu Domainfactory), ist davon auszugehen, dass auch die Postfächer

der Domain „[redacted].net“ und damit auch das Postfach des Geschädigten bei diesem Provider liegt.

Von Domainfactory wurde die E-Mail trotz des mutmaßlichen Phishing-Charakters als legitim gespeichert. Das lässt sich auf die Verwendung von „ESMPTSA“ zurückführen. Bei diesem Protokoll authentifiziert sich der Nutzer vor der Benutzung des E-Mail-Dienstes. Das bedeutet in unserem Fall, dass die E-Mail tatsächlich von einem Nutzer versendet wurde, der Zugriff auf das E-Mail-Postfach „mail@[redacted].de“ hat.

```
1.  Delivery-date: Sat, 22 Jun 2019 12:36:40 +0200
2.  Received: from [80.67.18.23] (helo=mx14.ispgateway.de)
3.      by mailcluster3-2.ispgateway.de with esmtps (TLSv1.2:ECDHE-RSA-AES256-GCM-
    SHA384:256)
4.      (Exim 4.92)
5.      (envelope-from <mail@[redacted].de>)
6.      id 1hedNw-0004JD-M1; Sat, 22 Jun 2019 12:36:40 +0200
7.  Return-path: <mail@[redacted].de>
8.  X-Envelope-to: gkastenfrosch@[redacted].net
9.  Received: from [80.67.31.29] (helo=smtprelay02.ispgateway.de)
10.     by mx14.ispgateway.de with esmtps (TLSv1.2:ECDHE-RSA-AES256-GCM-SHA384:256)
11.     (Exim 4.92)
12.     (envelope-from <mail@[redacted].de>)
13.     id 1hedNv-0002lh-M2
14.     for gkastenfrosch@[redacted].net; Sat, 22 Jun 2019 12:36:40 +0200
15. Received: from [91.[redacted].15] (helo=[redacted].fritz.box)
16.     by smtprelay02.ispgateway.de with esmtpsa (TLSv1.2:ECDHE-RSA-AES256-GCM-
    SHA384:256)
17.     (Exim 4.92)
18.     (envelope-from <mail[redacted].de>)
19.     id 1hedNv-00062j-9I
20.     for gkastenfrosch@d[redacted].net; Sat, 22 Jun 2019 12:36:39 +0200
21. From: Internet Security Center (security@inter.net) <mail@[redacted].de>
22. Content-Type: multipart/alternative;
23.     boundary="Apple-Mail=_41D33340-3B48-4599-8849-B9B15B8E304E"
24. Mime-Version: 1.0 (Mac OS X Mail 12.4 \(3445.104.11\))
25. Subject: DRINGEND: Internet Security Center, Sicherheit Ihres E-Mailzugangs
26. Message-Id: <96CAC41A-E9EE-47A1-9076-3CEB12778325@[redacted].de>
27. Date: Sat, 22 Jun 2019 12:36:39 +0200
28. To: gkastenfrosch@[redacted]
29. X-Mailer: Apple Mail (2.3445.104.11)
30. X-Df-Sender: bWFpbEBjaGxvYi5kZQ==
31. X-Received-
    SPF: none ( mx14.ispgateway.de: domain of [redacted].de does not provide an SPF record
    )
32. X-Spam-Checker-Version: SpamAssassin 3.4.0 (2014-02-07) on
33.     spamfilter02.ispgateway.de
34. X-Spam-Level:
35. X-Spam-Status: No, hits=-1.9 required=9999.0 tests=BAYES 20 autolearn=disabled
36.     version=3.4.0
37. X-Spam-CMAETAG: v=2.2 cv=T8/8d7CQ c=1 sm=1 tr=0
38.     a=JeGsAAKMHZmXDY1U4ywBTA==:17 a=dq6fvYVFJ5YA:10 a=nPzoH-kDAAAA:8
39.     a=MmSED-M6AAAA:8 a=r4k769tl49q4qrEZSFsA:9 a=QEXdDO2ut3YA:10
40.     a=bsk5O1Vtv3cA:10 a=NhIVlvsutasDiaCjegQA:9 a=CK11688CYmKptqMs:21
41.     a=_W_S_7VecoQA:10 a=jpRh-jkEdKE4ZNWW_jGS:22 a=_rsA_YMgoWxAtRYYE-oX:22
42. X-Spam-CMAECATEGORY:
43. X-Spam-CMAESUBCATEGORY:
44. X-Spam-CMAESCORE:
```

5.7 Systeminformationen aus der Registry

Zur weiteren Analyse werden der User-Hive (Datei `NTUSER.DAT` (`C:\Users\<Benutzername>`) aus dem Benutzerordner) sowie die systemweiten Registry-Hives aus dem Laufwerkspfad `C:\Windows\System32\config` exportiert und auf dem lokalen Rechner zur weiteren Verarbeitung gespeichert.

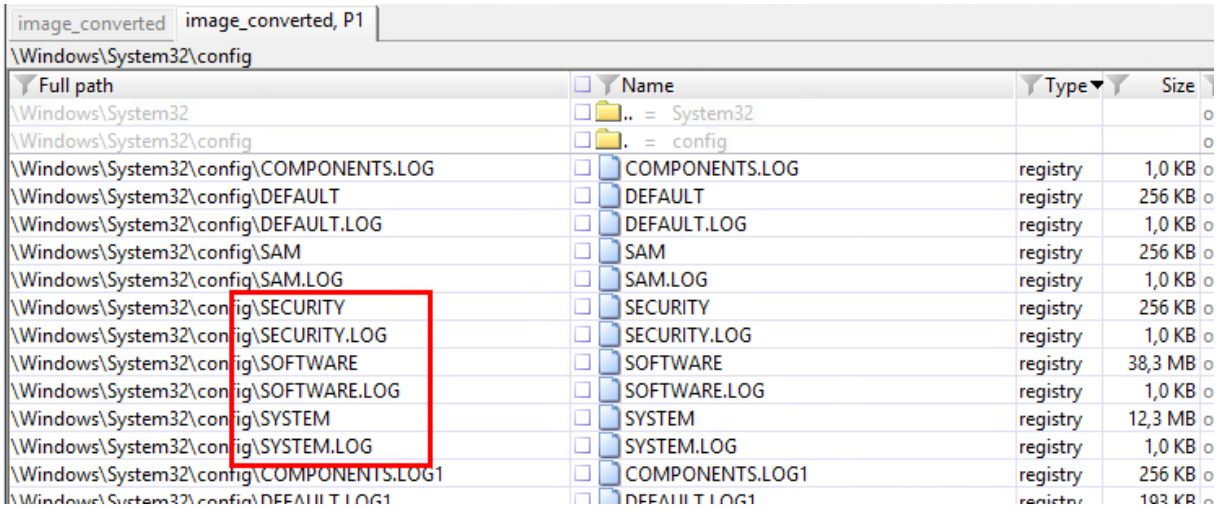


Abbildung 33: Export der Windows Registry

Zum Analysieren der exportierten Dateien kommt das Tool `RegRipper`[3] zum Einsatz, welches sowohl eine GUI besitzt, als auch über die Konsole gestartet werden kann. Im Hintergrund besteht es aus mehreren hundert Perl-Skripten zum Aufbereiten verschiedenster Informationen aus der Registry.

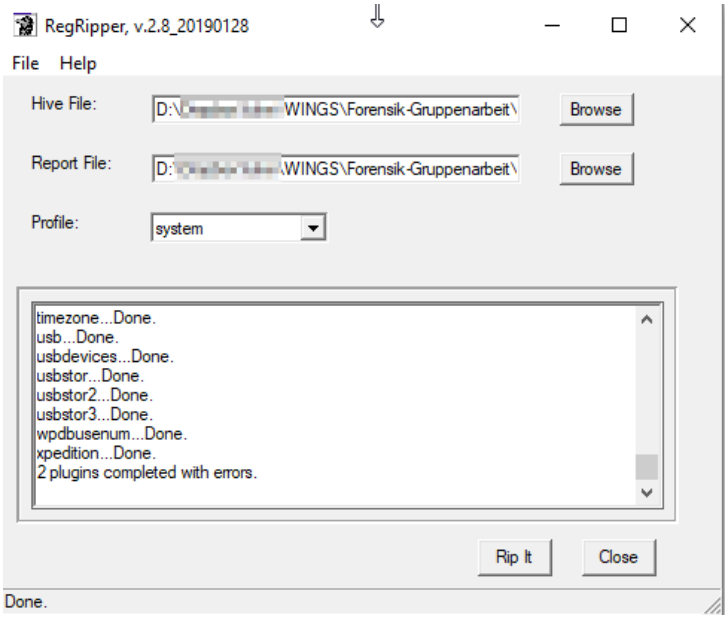


Abbildung 34: RegRipper 2.8

[3] https://github.com/keydet89/RegRipper2.8

Nachdem die exportierten Hive-Dateien durch den RegRipper aufbereitet wurden, können aus den Report-Files die gewünschten Informationen extrahiert werden. Aus der Datei NTUSER.DAT kann der Autostart-Eintrag im Public User-Folder extrahiert werden, der einen Verweis auf die identifizierte Schadsoftware „Rlwjy.exe“ anzeigt. Somit wurde für alle Nutzer auf dem System das Programm gestartet.

```
1.  user_run v.20140115
2.  (NTUSER.DAT) [Autostart] Get autostart key contents from NTUSER.DAT hive
3.
4.  Software\Microsoft\Windows\CurrentVersion\Run
5.  LastWrite Time Sat Jun 22 10:56:20 2019 (UTC)
6.    svchos: C:\users\Public\Rlwjy.exe
```

Über das Skript compname erhält man Information zum Computer- bzw. Hostnamen des Systems, was für die Identifikation des Systems von Bedeutung ist.

```
1.  compname v.20090727
2.  (System) Gets ComputerName and Hostname values from System hive
3.
4.  ComputerName    = WIN-BS9RVGO8L4V
5.  TCP/IP Hostname = WIN-BS9RVGO8L4V
```

Im Bereich des Skripts nic_mst2 erhält man einen Einblick in die Netzwerk- und DHCP-Konfiguration des Systems. Das Skript dnschanger zeigt hingegen Informationen zum DNS des Clients und würde eventuelle Manipulationen am DNS-Eintrag erkennen.

```
1.  nic_mst2 v.20080324
2.  (System) Gets NICs from System hive; looks for MediaType = 2
3.
4.  Network key
5.  ControlSet001\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}
6.
7.  ControlSet001\Services\Tcpip\Parameters\Interfaces
8.  LastWrite time Sat Jun 22 10:44:47 2019 (UTC)
9.
10. Interface {43965CA1-D709-4080-8652-6294433BFDD8}
11. Name: LAN-Verbindung
12. Control\Network key LastWrite time Tue May 28 18:28:35 2019 (UTC)
13. Services\Tcpip key LastWrite time Sat Jun 22 11:06:51 2019 (UTC)
14.     DhcpDomain     = localdomain
15.     DhcpIPAddress  = 192.168.2.129
16.     DhcpSubnetMask = 255.255.255.0
17.     DhcpNameServer = 192.168.2.1
18.     DhcpServer     = 192.168.2.254
19. ----------------------------------------
20. dnschanger v.20120203
21. (System) Check for indication of DNSChanger infection.
22.
23. Adapter: {43965CA1-D709-4080-8652-6294433BFDD8}
24. LastWrite Time: Sat Jun 22 11:06:51 2019 Z
25.   NameServer                  192.168.2.128
26.   DhcpNameServer              192.168.2.1
27.
28. Adapter: {E71F6BE3-1E56-4EF8-8B06-A0E4246CD463}
29. LastWrite Time: Tue May 28 18:26:53 2019 Z
30.   NameServer
```

Zur Korrelation der Daten mit anderen Systemen ist es notwendig, die Zeitzone des Clients zu extrahieren. Hier hilft das Skript `timezone` und liefert entsprechende Informationen zurück.

```
timezone v.20160318
(System) Get TimeZoneInformation key contents

TimeZoneInformation key
ControlSet001\Control\TimeZoneInformation
LastWrite Time Tue May 28 18:27:40 2019 (UTC)
  DaylightName   -> @tzres.dll,-321
  StandardName   -> @tzres.dll,-322
  Bias           -> -60 (-1 hours)
  ActiveTimeBias -> -120 (-2 hours)
  TimeZoneKeyName-> W. Europe Standard Time
```

Über das Skript `appcompatcache_tln` lässt sich der Application Compatibility Cache des Windows-Systems extrahieren. Dieser zeigt ausgeführte Software an, die von Windows „geshimmt“ wurde. Dies passiert bei allen Programmen auf einem Windows-System und ist eigentlich als Kompatibilitätsmodus gedacht. Das Shimming wird sowohl beim Ausführen, als auch bei Änderung oder Kopieren von Programmen, durchgeführt. Hier erkennt man, dass die zwei bereits identifizierten exe-Dateien sowie das Programm `vssadmin.exe` geshimmt wurden. Da die Datei seit der Installation nicht angepasst wurde, liegt es nahe, dass das Angriffsskript über das Programm `vssadmin.exe` versuchte die Volume Shadow Copies und damit die möglicherweise bestehenden Backups von Dateien zu löschen.

```
appcompatcache_tln v.20190112
(System) Parse files from System hive AppCompatCache

ControlSet001\Control\Session Manager\AppCompatCache
LastWrite Time: Sat Jun 22 11:07:12 2019 Z
Signature: 0xbadc0fee
Win2K8R2/Win7, 64-bit

1561200975|REG|||M... [Program Execution] AppCompatCache - C:\users\Public\Rlwjy.exe
 [Executed]
1561200968|REG|||M... [Program Execution] AppCompatCache - C:\Users\Günther Kastenfr
osch\Downloads\internetsecurity_plugin_v08.15_signed.exe [Executed]
1247535589|REG|||M... AppCompatCache - C:\Windows\system32\vssadmin.exe
```

Aus der Analyse mit `RegRipper` können also folgende Aspekte mitgenommen werden: Einerseits die Identifikation des Systems (siehe auch Kapitel 5.1), andererseits die Tatsache, dass die Schadsoftware mittels eines Run-Key-Eintrags in der Registry für Persistenz gesorgt hat. Zudem lässt sich ein weiterer Hinweis auf den modus operandi der Schadsoftware (Nutzung von `vssadmin.exe`) finden. Daraus können auch Detektions- bzw. Erkennungsregeln entwickelt werden.

6 Timeline des IT-Systems

Im Folgenden wird beschrieben, welche Vorgänge auf dem vorliegenden IT-System stattgefunden haben. Der Schwerpunkt liegt hier auf Ereignissen, die im sachlichen Zusammenhang mit dem Sicherheitsvorfall stehen können. Die Timeline wurde auf Basis der Zeitstempel aus dem Betriebssystem, sowie einiger Metadaten erzeugt. Hierbei wurden die Daten auch mit dem „Record Changed“ Zeitstempel abgeglichen, um die Manipulation von Zeitstempeln erkennen zu können.

10.06.2019 @ 16:37:10 (MESZ):

Herr Kastenfrosch hat beim Surfen im Internet einen Radio-Stream aktiviert und über den Browser Firefox im Internet gesurft. Dabei hat er bei der Suchmaschine Google nach den Begriffen „*anti virus macht den computer langsam*“ und „*windows defender ausschalten“* gesucht. Es ist davon auszugehen, dass er seinen Windows Defender nach einer bei „computerbild.de“ gefundenen Anleitung deaktiviert hat. Anschließend hat er noch weitere Webseiten aufgerufen und ein „normales“ Surfverhalten gezeigt.

22.06.2019 @ 12:36:40 (MESZ)

Über einen E-Mail-Provider wurde eine Mail mit dem Betreff „*DRINGEND: Internet Security Center, Sicherheit Ihres E-Mailzugangs*“ an die Adresse „gkastenfrosch@[redacted].net“ versendet. Der Absender konnte sich erfolgreich authentifizieren, sodass davon auszugehen ist, dass er Zugang zu der Absender-E-Mail-Adresse „mail@[redacted].de“ hat oder hatte.

22.06.2019 @ 12:48:16 (MESZ)

Kurz darauf hat das Mailprogramm von Herrn Kastenfrosch die zugestellte E-Mail abgerufen und in eine lokale EML-Datei gespeichert. Es ist davon auszugehen, dass das Mailprogramm zu dem Zeitpunkt aktiv war, da nur wenige Minuten später auf die Mail zugegriffen wurde.

22.06.2019 @ 12:55:51 (MESZ)

Herr Kastenfrosch hat über seinen Standard-Browser Mozilla Firefox die Webseite „webcheckemailandinternetsecurity-centercomslash.de/internetsecurity_plugin_v08.15_signed.exe“ aufgerufen und die Schadsoftware auf seine Festplatte heruntergeladen.

22.06.2019 @ 12:56:08 (MESZ)

Kurz nach dem Download hat er die Datei ausgeführt. Die dadurch gestartete Schadsoftware hat die Datei „Rlwjy.exe“ erzeugt und ebenfalls ausgeführt.

22.06.2019 @ 12:57:01 (MESZ)

Die erzeugte Schadsoftware hat die Dateien von Herrn Kastenfrosch verschlüsselt und in jedem Ordner eine Textdatei „RyukReadMe.txt“ hinterlegt, die ihn auf die Verschlüsselung hinweist sowie zur Zahlung eines Lösegelds auffordert.

22.06.2019 @ 13:07:13 (MESZ)

Der Computer wurde per Shutdown korrekt heruntergefahren; dies war die letzte Aktion, die auf dem IT-System festgestellt werden konnte.

7 Fazit und Untersuchungsergebnisse

Nachfolgend werden die Ergebnisse, das Vorgehen sowie die zum Einsatz gekommenen Werkzeuge bewertet.

7.1 Bewertung der Ergebnisse

Die Ergebnisse der Untersuchung eignen sich in unterschiedlicher Hinsicht für weitere Aktivitäten: Zunächst konnte der mutmaßliche Absender der E-Mail identifiziert werden. Hier ergibt sich eine weitere Spur, die man z.B. bei einer Anzeige einbringen könnte. Zwar ist es möglich, dass der Nutzer des Rechners „[redacted].fritz.box“ nicht wusste, dass von seinem Account bösartige E-Mails verschickt wurden, allerdings wäre das in einer weiteren polizeilichen Untersuchung zu analysieren.

Es konnten keine Backups oder Entschlüsselungsmöglichkeiten für die Daten des Nutzers identifiziert werden. Ob der Nutzer über Offline-Backups verfügt ist an dieser Stelle nicht bekannt, daher lässt sich der entstandene Schaden nicht beziffern.

Auch hinsichtlich der Tools, Taktiken und Prozeduren (TTP) des Angreifers konnten einige Erkenntnisse gewonnen werden: Der Angreifer benutzt AutoRun-Keys für die Persistenz, generiert beim Start der Schadsoftware eindeutige Binaries, die vermutlich den Verschlüsselungsschlüssel enthalten und verwendet das Tool „`vssadmin.exe`“ um Volume Shadow Copies zu löschen. Hieraus lassen sich Regeln für die weitere Detektion des Angreifers gewinnen.

7.2 Bewertung des Vorgehens

In einer gerichtlichen Untersuchung hätte das hier gewählte Vorgehen eine wichtige Schwachstelle. Aufgrund der „Übungsrealität“ wurde auf einen physischen Write-Blocker verzichtet. In einem Fall, bei dem es auch auf die gerichtliche Verwertbarkeit der Untersuchung ankommt, wäre dies eine absolute Mindestbedingung. Da in diesem Falle der legitime Nutzer des IT-Systems ein Interesse daran hatte, die Untersuchung durchzuführen, konnte man von ihm außerdem wertvolle Hinweise erhalten, zu welchen Zeitpunkten welche Aktivitäten legitim bzw. auffällig waren. Dadurch konnte der Aufwand für die forensische Untersuchung des Systems reduziert werden. Bei einer „Blackbox-Untersuchung“ hätte man vermutlich wesentlich mehr zeitlichen Aufwand einbringen müssen, um zunächst ein genaues Bild von der „Normalität“ auf dem System zu erhalten. Erst danach wäre die eigentliche Identifikation von Anomalien möglich gewesen.

7.3 Bewertung der genutzten Werkzeuge

Die zum Einsatz gekommenen Werkzeuge haben sich für die hier vorliegende Analyse bewährt. Insbesondere den Tools „X-Ways Forensics“ und „RegRipper“ fiel im vorliegenden Fall eine Schlüsselrolle zu: Nur durch diese beiden (sehr systemnahen) Tools konnten die TTP (Tools, Tactics, Procedures) des Angreifers identifiziert und analysiert werden.

Das Tool „SQLite Forensic Explorer“ hat sich sehr dazu geeignet, zusätzliche Informationen zu beschaffen wie das IT-System des Nutzers geschwächt wurde. Hier konnte die Suchanfrage des Nutzers identifiziert werden, die zur Deaktivierung des Windows Defender geführt hat.

Abbildungsverzeichnis