Introduction

Digital forensic procedures are closely complemented by incident response investigations. Incident response may be defined as an organized approach to addressing and managing the aftermath of a security breach or cyberattack – also known as an IT incident, a computer incident, or a security incident. The objective is to handle the situation in a way that limits damage and reduces recovery time and costs. Although sometimes organized and named differently according to different sources, there are typically six primary steps of an effective incident response initiative.

1. **Preparation:** An incident response is not a calm and leisurely affair. Without good preparation, an incident response is going to be disorganized and has the potential to make the incident worse. A formal incident response plan is a crucial first step in preparation. Once an approved plan is in place with the appropriate staffing, ensure that the people assigned incident response duties are properly trained on the processes and procedures necessary for investigating an incident. Additionally, tools such as forensic hardware and software should be acquired and incorporated into the process.

2. **Detection:** This is often a complex endeavor. The detection phase is the part of the incident response process where the organization first becomes aware of a set of events that possibly indicate malicious activity or constitute a threat to confidentiality, integrity, or availability. Detection can come from internal or external sources, or both.

3. **Analysis:** In this step, personnel begin collecting evidence from systems, such as running memory, log files, network connections, and running software processes. Depending on the type of incident, this collection can take as little as a few hours to several days. The goal of the analysis step is to determine the root cause of the incident and to reconstruct the actions of the threat actor from initial compromise to detection.

4. **Containment:** With an understanding of what the incident is and what systems are involved, the next step is the containment phase. This is when the incident response team takes measures to limit the ability of a threat actor to continue compromising network resources, communicating with command-and-control infrastructures, or exfiltrating confidential data. Containment strategies range from locking down ports and IP address on a firewall to simply removing the network cable from the back of an infected machine.

   Depending on who you ask, Containment is sometimes considered the first step in the incident response process. While this may be true in terms of overall priorities (an incident should be contained as quickly as possible), in practice, Detection, Analysis, and Containment often overlap and fold back into one another.

5. **Eradication and Recovery:** This step is when the threat actor is removed from the impacted

network. In the case of a malware infection, the incident response team may run an enhanced anti-malware solution. Other times, infected machines may be wiped and reimaged. Other activities include removing or changing compromised user accounts. If the team has identified a vulnerability that was exploited, vendor patches are applied, or software updates are made. Recovery activities are very closely aligned with those that may be found in an organization's business continuity or disaster recovery plans.

6. **Post-incident activity:** Post-incident activity includes a complete review of all the actions taken during the incident. The team should discuss what worked and, more importantly, what did not work. It is during this phase of the process that a written report is completed. For forensic investigators, this type of documentation is critical should the incident ever wind up in court. The documentation should be detailed and show a clear chain of events with a focus on the root cause if it was determined.

In this lab, you will imitate the Analysis step of the incident response process. You will analyze a PCAP file and disk image for evidence, then prepare your findings in an incident response report. You will then continue your investigation and update your report as more evidence comes to light.

Lab Overview

SECTION 1 of this lab has three parts, which should be completed in the order specified.

1. In the first part of the lab, you will analyze a PCAP file taken during a recent incident.

2. In the second part of the lab, you will use E3 to identify forensic evidence related to the incident.

3. In the third part of the lab, you will prepare an incident response report.

SECTION 2 of this lab allows you to apply what you learned in **SECTION 1** with less guidance and different deliverables, as well as some expanded tasks and alternative methods. You will analyze additional evidence and update the incident response report accordingly.

Finally, you will explore the virtual environment on your own in **SECTION 3** of this lab to answer a set of questions and challenges that allow you to use the skills you learned in the lab to conduct independent, unguided work – similar to what you will encounter in a real-world situation.

Learning Objectives

Upon completing this lab, you will be able to:

1. Perform forensic analysis as part of an incident response investigation.
2. Perform forensic analysis on a PCAP file using NetWitness Investigator.
3. Perform forensic analysis on a disk image using Paraben's E3.
4. Correlate evidence from multiple sources to develop your case.
5. Create an incident response report to document your findings.

Topology

This lab contains the following virtual machines. Please refer to the network topology diagram below.

- vWorkstation (Windows: Server 2019)

Tools and Software

The following software and/or utilities are required to complete this lab. Students are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- NetWitness Investigator
- Paraben's E3

Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

SECTION 1

1. Lab Report file including, screen captures of the following:

- Time Graph
- Details of the 2021-Jul-13 15:33:00 session
- Email containing FTP credentials and the associated timestamps

2. Any additional information as directed by the lab:

- Completed Incident Report

SECTION 2

1. Lab Report file including, screen captures of the following:

- Email from Dr. Evil demanding Marvin install a keylogger
- Email from Dr. Evil reminding Marvin to update the firewall and scheduler
- Registry key value associated with the keylogger and the localSPM service

2. Any additional information as directed by the lab:

- Document the Author and Date values associated with the scheduled keylogger task.
- Document the port used for inbound connections to the keylogger and the name and location of the keylogger executable.
- Record the first time and last time the keylogger was started.
- Record whether Marvin interacted with or simply opened the keylogger.
- Updated Incident Report

SECTION 3

1. Lab Report file including, screen captures of the following:

- Exfiltrated files in Marvin's Outlook database
- Email with instructions for installing additional spyware

2. Any additional information as directed by the lab:

- None

Section 1: Hands-On Demonstration

Note: In this section of the lab, you will follow a step-by-step walk-through of the objectives for this lab to produce the expected deliverables.

1. **Review** the **Tutorial**.

   Frequently performed tasks, such as making screen captures and downloading your Lab Report, are explained in the Cloud Lab Tutorial. The Cloud Lab Tutorial is available from the User menu in the upper-right corner of the Student Dashboard. You should review these tasks before starting the lab.

2. **Proceed** with **Part 1**.

Part 1: Analyze a PCAP File for Forensic Evidence

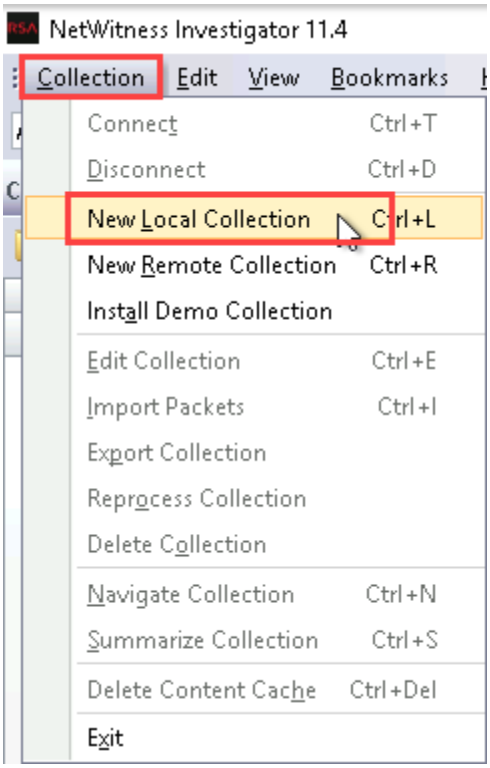
Note: The setting for this lab is a recent security incident at the game development studio Giggly Goofo. The security incident was discovered on July 31, 2021 at 10:30 AM Eastern time and reported 10 minutes later. Based on preliminary findings, the security team suspects that a data breach occurred, involving both internal and external actors, wherein copies of confidential files were exfiltrated from the corporate network. As a digital forensics specialist assigned to the incident response team, you have been tasked with performing the Analysis step of the incident response process. As possible sources of evidence, you have been provided with a PCAP file containing network traffic at the time of the breach and a copy of a drive image from an employee who is suspected to be involved with the incident.
In this part of the lab, you will analyze the contents of the PCAP file using NetWitness Investigator. Developed by RSA, NetWitness Investigator is an enterprise-level threat analysis platform designed to contextualize network activity and efficiently identify malicious activity. In this lab, you will be using the free version of NetWitness Investigator. While it only contains a small portion of the enterprise version's functionality, it is nonetheless a powerful tool for conducting forensic analysis.

In the next steps, you will open the NetWitness Investigator application and import the PCAP file provided by your colleagues on the incident response team.

1. On the vWorkstation desktop, **double-click** the **NetWitness Investigator icon** to open the NetWitness application. If you receive a **File Download - Security Warning** dialog box for an http_500_webOC file, please select **Cancel**.

NetWitness Investigator icon

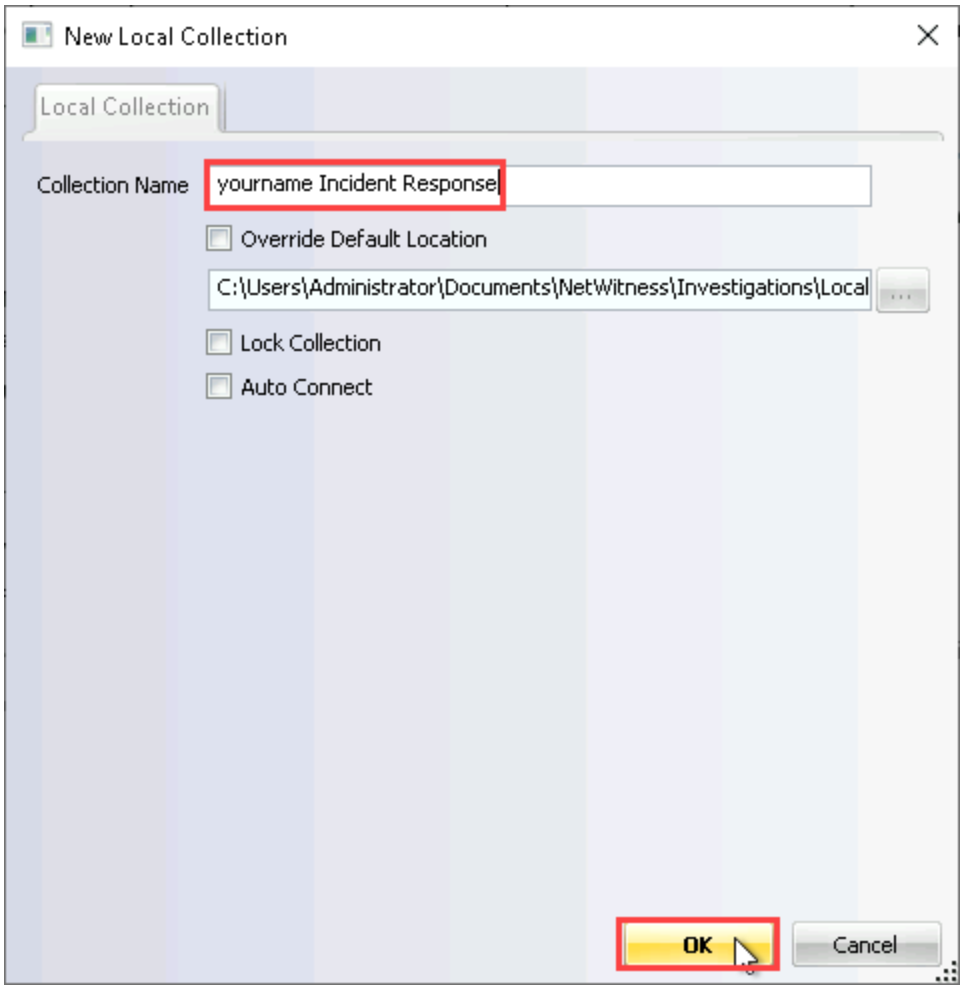
2. From the NetWitness Investigator menu bar, **click Collection** and **select New Local Collection** from the menu to open the New Local Collection dialog box.



Collection > New Local Collection

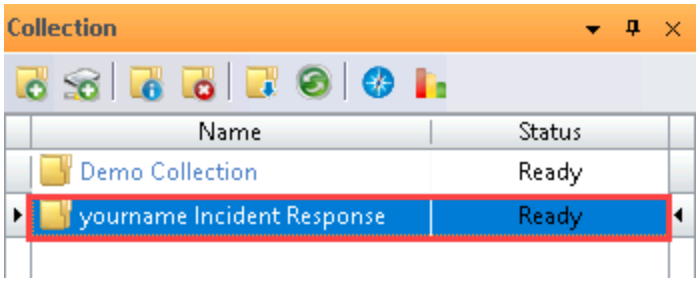
3. In the New Local Collection dialog box, **type** ***yourname*** **Incident Response** in the

Collection Name box, replacing *yourname* with your own name, and **click OK** to name the new collection and close the dialog box.



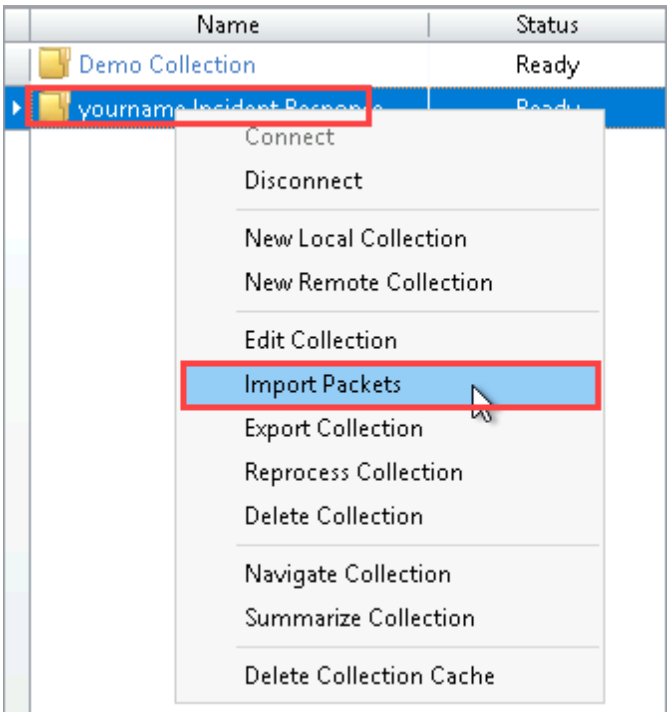
New Local Collection dialog box

4. In the Collection pane, **double-click** the ***yourname* Incident Response collection** to activate it and change the status to Ready.



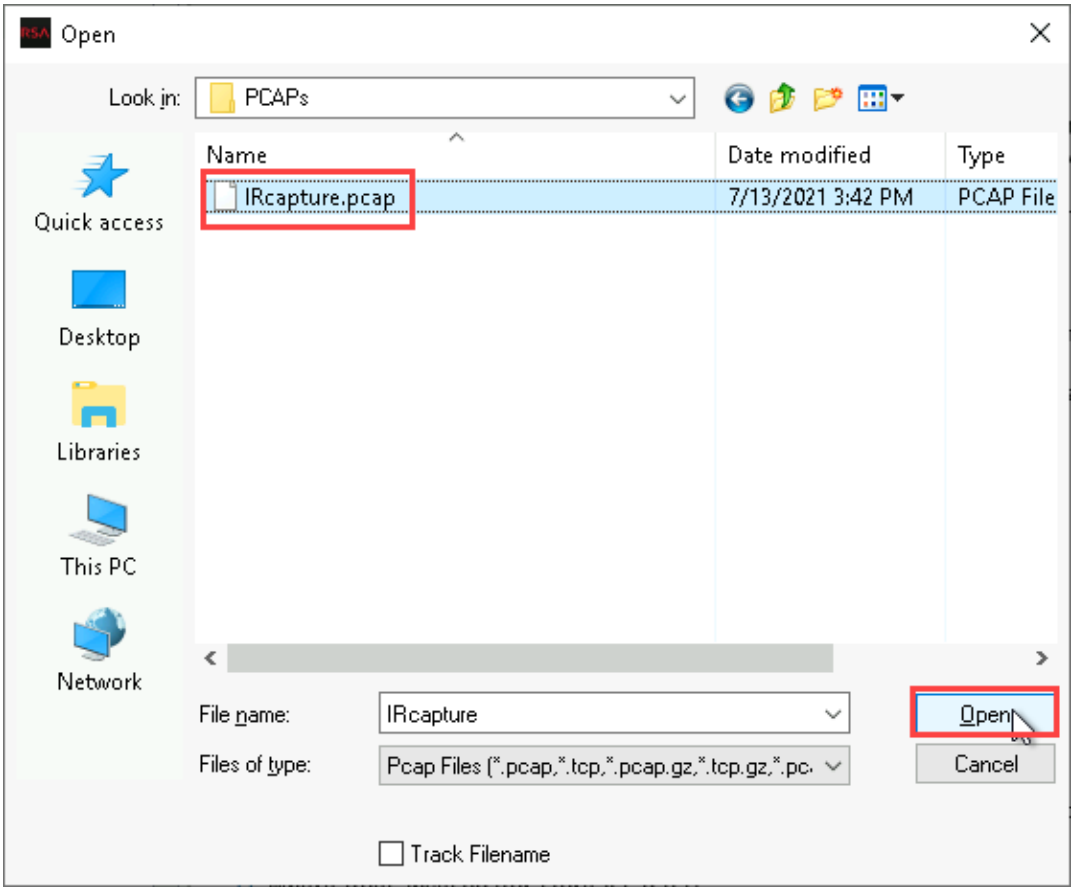
Activate the collection

5. In the Collection pane, **right-click** the ***yourname*** **Incident Response collection** and **select Import Packets** from the context menu to open the Open dialog box.



Import Packets

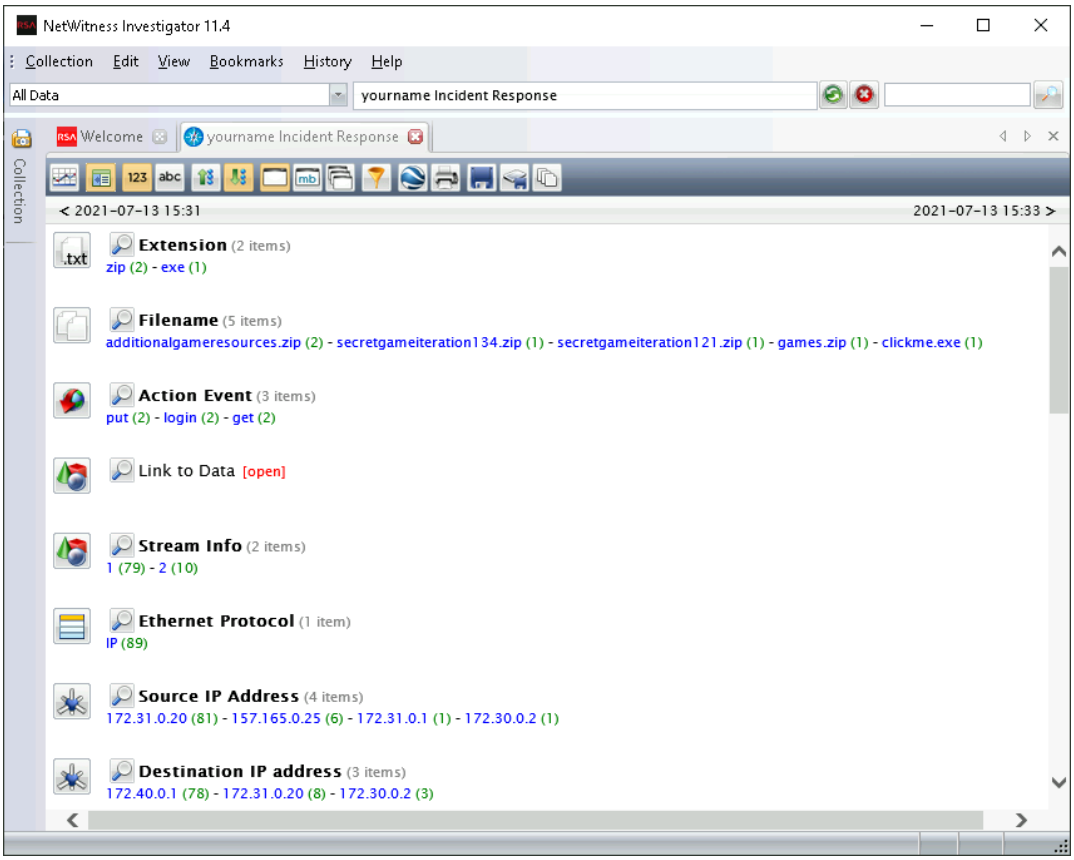
6. In the Open dialog box, **navigate** to **This PC > Local Disk (C:) > Incident Response Evidence > PCAPs** and **select** the **IRcapture.pcap file**, then **click Open** to import the contents of the file into the *yourname* Incident Response Collection.



Open dialog box

Note: While importing, the Status column changes to Importing. When the collection is ready for analysis, the Status column will change to Ready.

7. When the file has finished importing, **double-click** the ***yourname* Incident Response collection** to open it in the Navigation View.

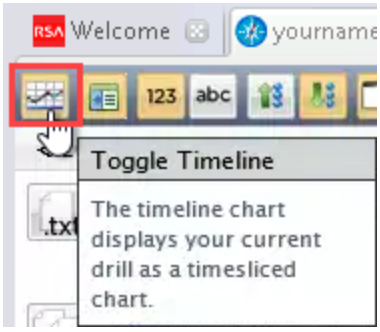


Navigation View

Note: In NetWitness Investigator, collections are explored using the Navigation View. The Navigation View contains multiple reports, which are displayed within the Navigation View as individual headers, such as Alerts, Service Type, Source IP Addresses, and more.

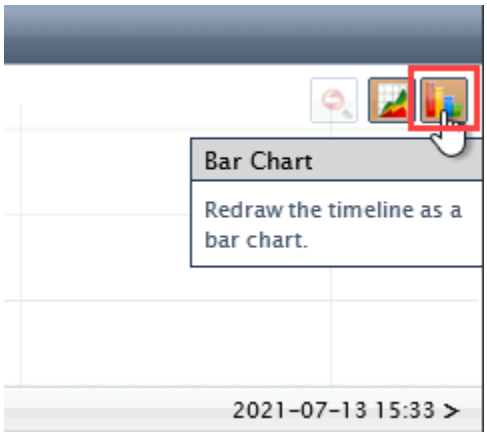
In the top pane, below the Navigation Toolbar, you should see two timestamps. These correspond to the time and date that the packet capture session in the PCAP file began (July 13, 2021, at 3:31 PM) and ended (July 13, 2021, at 3:33 PM).

8. In the Navigation View, **click** the **Toggle Timeline button** to display the Time Graph.



Toggle Timeline

9. In the Time Graph, **click** the **Bar Chart button** to display the time graph as a bar chart.



Bar Chart

Note: The Time Graph provides a breakdown of the sessions contained in the PCAP file. In the Bar Chart display mode, you can hover your cursor over a specific bar to see how many sessions occurred in that interval. In both the Area Chart or Bar Chart display modes, you can drag and drop your cursor within any blue area to zoom in and narrow the focus of NetWitness to sessions that occurred within the selected interval. For example, if you had reason to suspect that malicious network activity occurred at 10:07 AM (perhaps an employee clicked a malicious link in a phishing email), you could use the zoom feature to display only the NetWitness reports related to traffic occurring at that exact moment. To zoom back out at any time, you can click the Zoom Out Timeline button next to the Area Chart and Bar Chart buttons.

10. **Make a screen capture** showing the **Time Graph**.

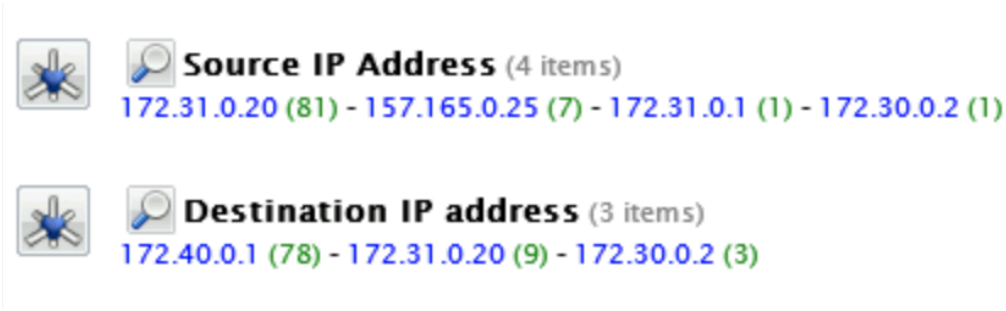
11. **Click** the **Toggle Timeline button** to hide the Time Graph.

12. In the Navigation View, **locate** the **Filename report**.

Filename report

Note: The Filename report lists any files that were detected during the capture session. Knowing that your employer is a game developer and the security incident involved exfiltration of confidential company data, it appears that the four .zip files listed here might contain the stolen data. The fifth file, clickme.exe, does not appear to be related to game development, but could be a malicious executable.

13. In the Navigation View, **locate** the **Source IP address** and **Destination IP address reports**.



IP Address reports

Note: The Source IP Address report contains IP addresses from which connections were established in the PCAP file. Similarly, the Destination IP Address report contains IP Addresses to which connections were established. You should see four entries under Source IP Address and three entries under Destination IP Address. Altogether, you should see four unique IP addresses, three of which share portions of the same network address (172.x.x.x). As an IT employee at Giggly Goofo, you know that all internal IP addresses on the internal company network begin with 172. Therefore, your attention should immediately be drawn to 157.165.0.25. Knowing that this PCAP was taken within the Giggly Goofo LAN, this IP address appears to be an external device connecting to the LAN, which makes it a strong candidate for further investigation.

14. Under the Source IP Address report, **click** the **(7)** next to **157.165.0.25** to open the Session List View for this source IP address.

Note: As you drill down into specific reports, NetWitness will keep track of your current location in the Drill Path at the top. If you need to return to the Navigation View for the yourname Incident Response collection at any time, click the yourname Incident Response link within the Drill Path.

15. In the Session List View for 157.165.0.25, **locate** the **session** that started on **2021-Jul-13 15:33:00**.

    This is the earliest session of the series, with the largest number of events.

Note: In the detailed session information on the right, you should see the names of two of the files that you previously identified as potential exfiltrated data. According to the session details, an FTP transfer occurred between 157.165.0.25 and 172.31.0.20 using the username GigglyGoofoDev and password Il0veC0d!nG. This appears to be at least one source of the data breach and provides valuable information for continuing your investigation, including IP addresses, credentials, timestamps, and filenames. Naturally, you will need to document all of these details for later use in your incident response report.

16. **Make a screen capture** showing the **details of the 2021-Jul-13 15:33:00 session**.

17. **Close** the **NetWitness Investigator window**.

Part 2: Analyze a Disk Image for Forensic Evidence

Note: In this part of the lab, you will turn your attention to the disk image provided by the security team. According to the security team, the disk image was taken from the laptop of a Giggly Goofo employee named Marvin Jonson, whom they have reason to suspect may be involved in the data exfiltration incident.

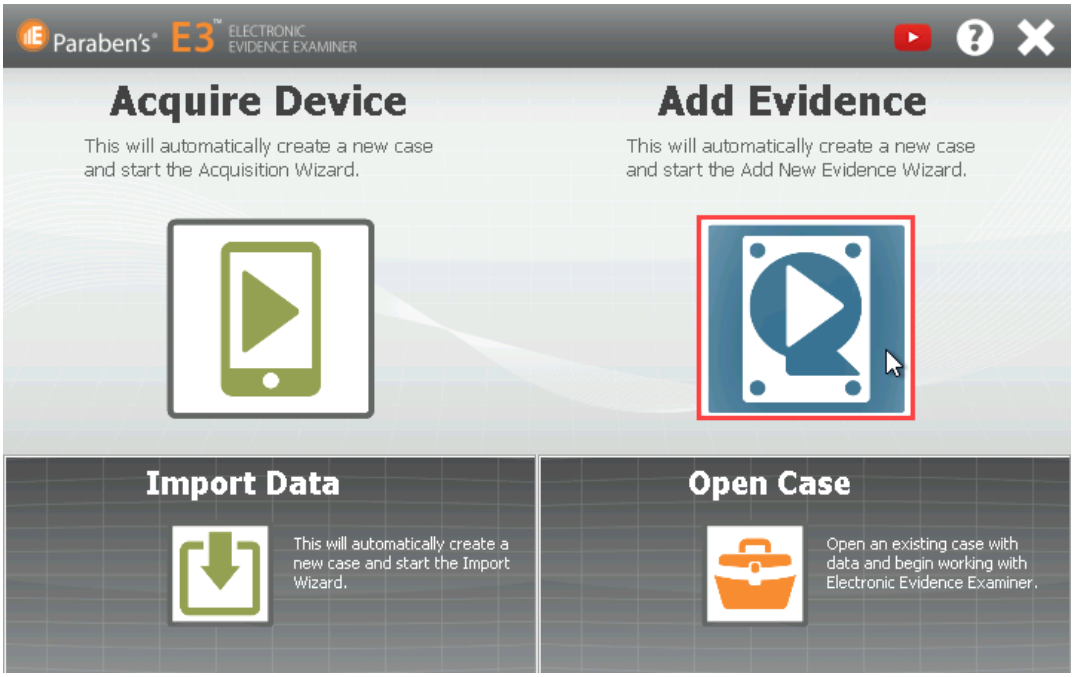
In the next steps, you will use Paraben's E3 forensic analysis software to import and examine Marvin's drive image for evidence of his involvement in the security breach.

1. On the vWorkstation desktop, **double-click** the **Electronic Evidence Examiner icon** to open the E3 application

E3 icon

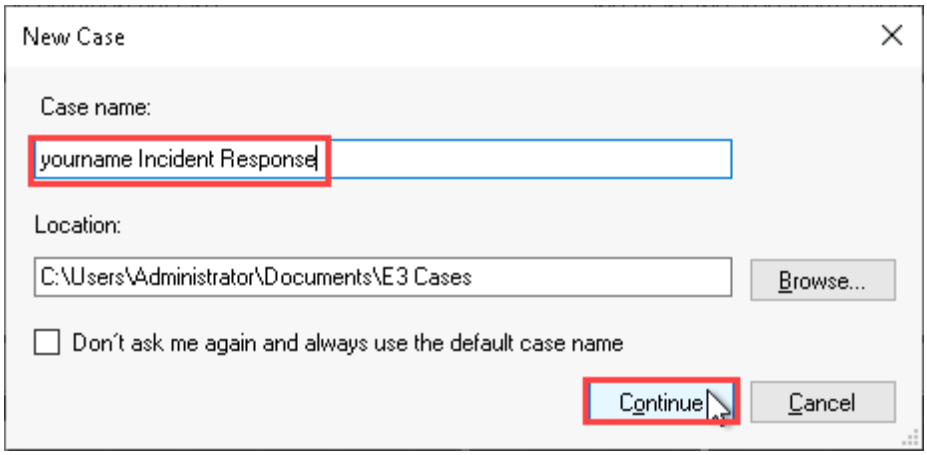
Note: E3 may take several minutes to load. The E3 welcome screen opens with shortcuts to the most common activities that forensic investigators will perform within the tool.

2. On the Welcome screen, **click** the **Add Evidence button** to open the New Case dialog box.



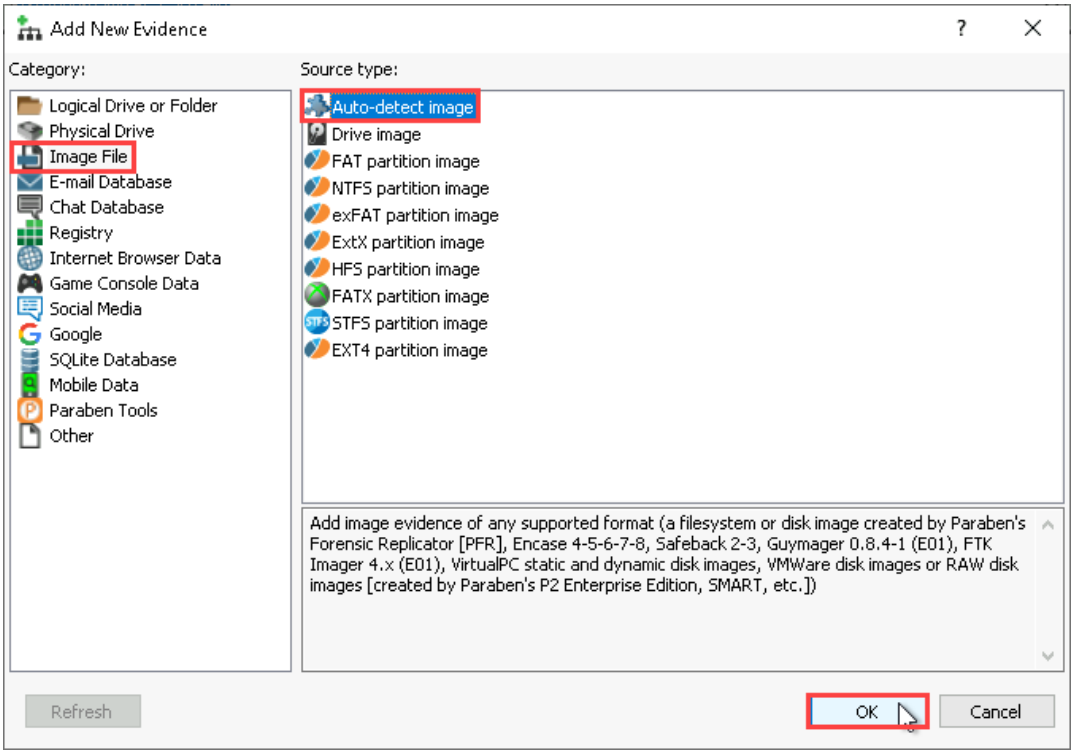
Welcome page - Add Evidence

3. In the New Case dialog box, **type *yourname* Incident Response** in the Case name field, replacing *yourname* with your own name, then **click Continue** to create your new case file and open the Add New Evidence dialog box.



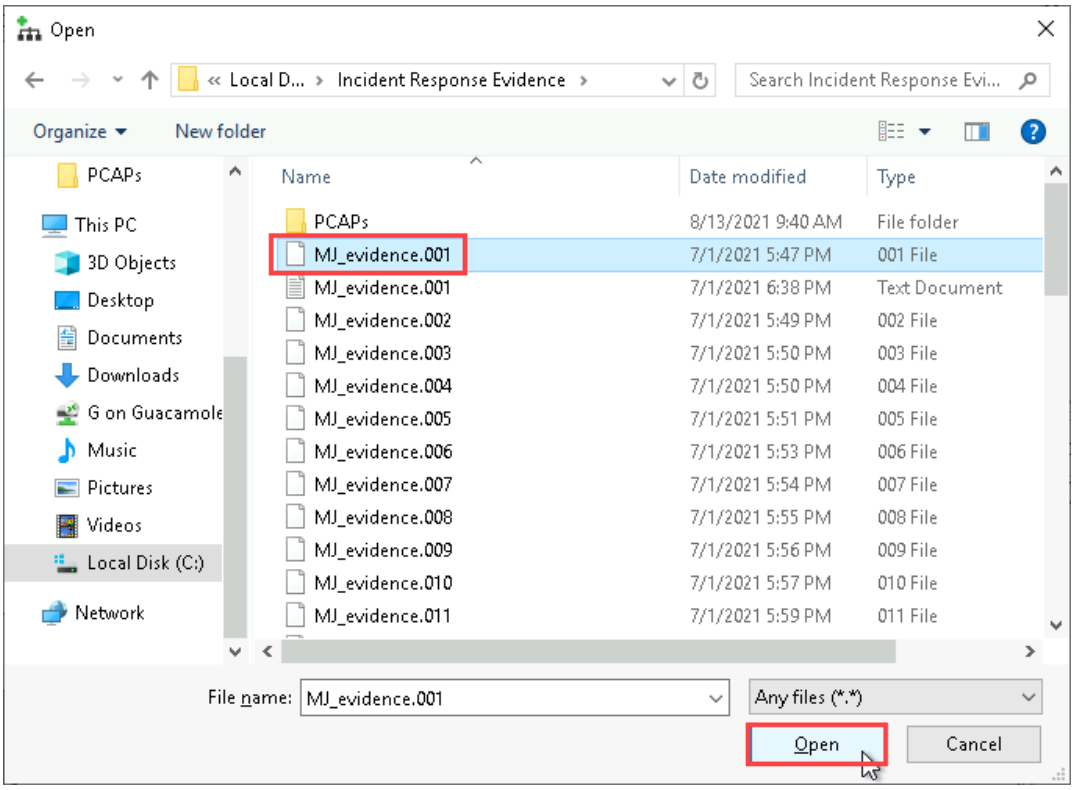
New Case dialog box

4. In the Add New Evidence dialog box, **click** the **Image File category**, then **select** the **Auto-detect image Source type** and **click OK** to continue.



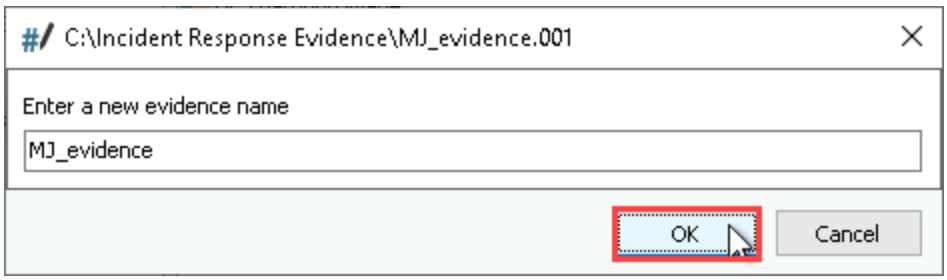
Add New Evidence - Auto-detect image

5. In the Open dialog box, **navigate** to **This PC > Local Disk (C:) > Incident Response Evidence** and **select** the first **MJ_evidence.001 file**, then **click Open** to import the digital drive image for this lab.



Open dialog box

6. When prompted, **click OK** to accept the default name for the drive image and add the data from the drive image to your case file.

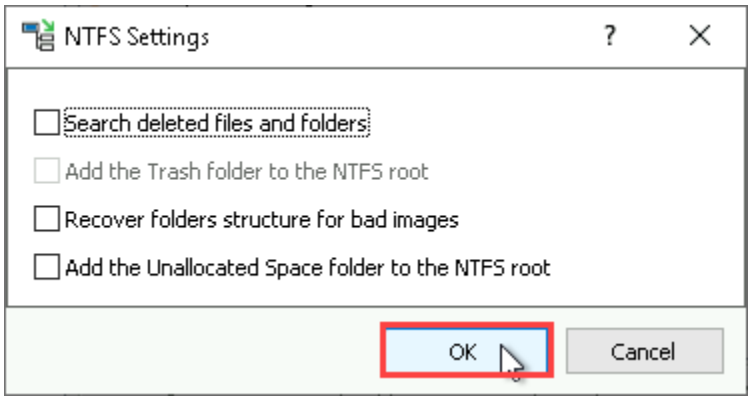


Evidence name

Note: The *yourname* Incident Response case will appear in the Case Content pane. The Case Content pane is the primary display and navigation area for all evidence in the open case file. Within the Case Content pane's tree-view structure, you can access case nodes, evidence nodes, evidence type nodes, folder nodes, and data grids/streams. Technically, the Case Content pane does not store the actual evidence, but provides a series of links to elements within the physical evidence.

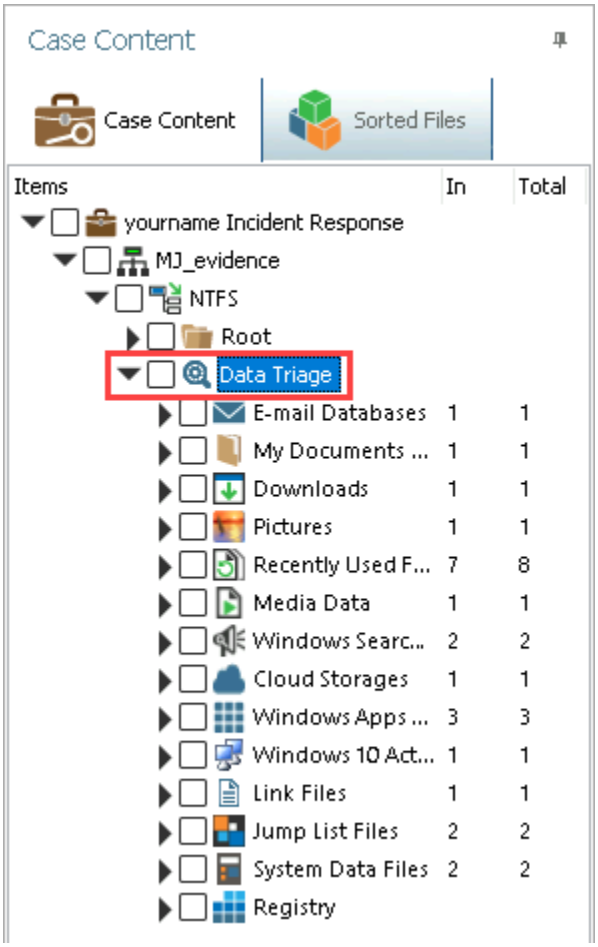
When you select a specific node or grid within the Case Content pane, the contents of the enclosing folder or database will be displayed in the Data Viewer in the center pane. Within the Data Viewer, you can select individual files, folders, and records. Additional information about the currently selected node, grid, file, folder, or record will be displayed in the Viewers pane on the right, which provides multiple ways to view your current selection.

7. When prompted, **click OK** to close the NTFS Settings dialog box without making any changes.



NTFS Settings dialog box

8. In the Case Content pane, **navigate** to ***yourname* Incident Response / MJ_evidence / NTFS**, then **expand** the **Data Triage node** to display the Data Triage categories.

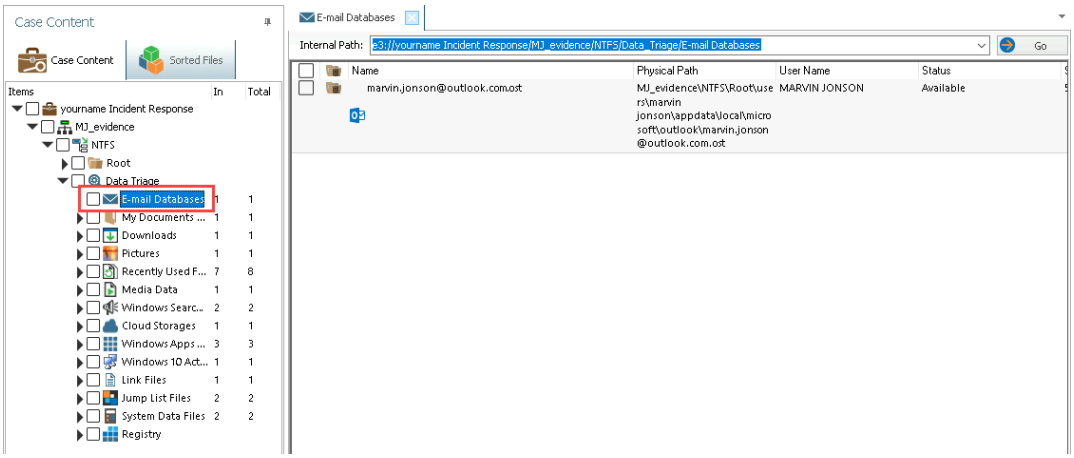


Data Triage

Note: The Data Triage function in E3 allows you to quickly view potentially high-value evidence, such as email databases, recently used files, and parsed registry data.

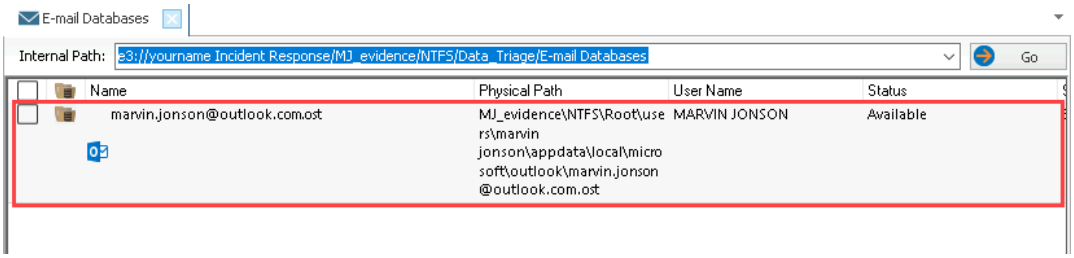
In the next steps, you will use E3's Advanced Search functionality to search for evidence in Marvin's email records.

9. In the Case Content pane, **select** the **E-mail Databases category** to display all email databases detected on the drive image in the Data Viewer.



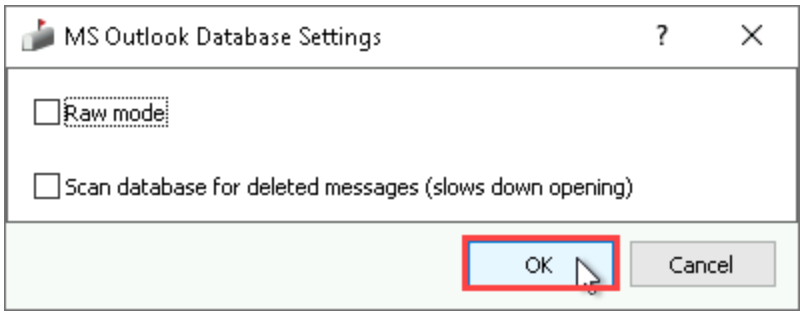
E-mail Databases category

10. In the Data Viewer, **double-click** the **marvin.jonson@outlook.com.ost database** to open it.



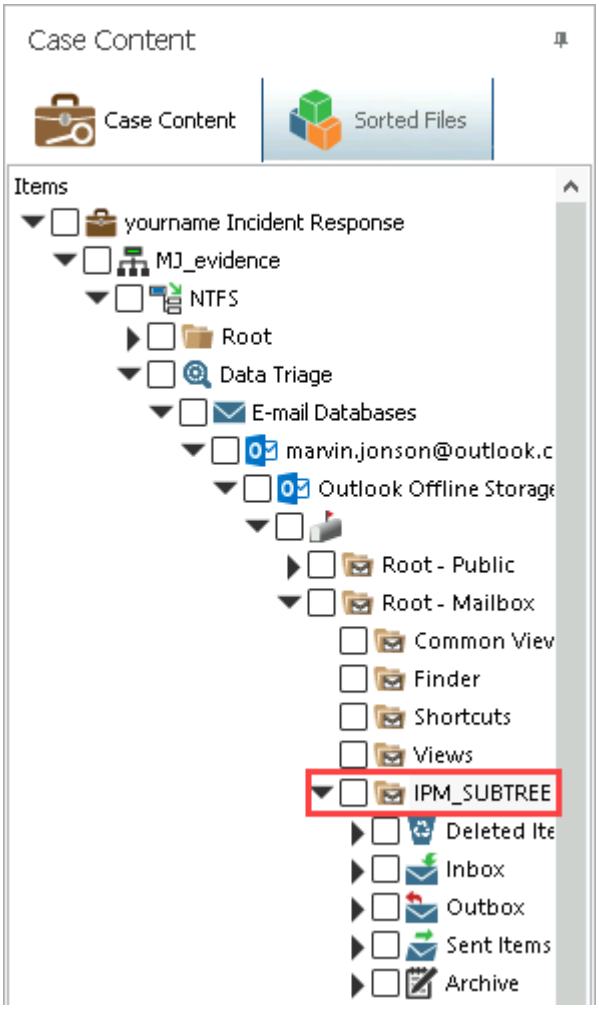
Marvin.jonson@outlook.com.ost database

11. When prompted, **click OK** to close the MS Outlook Database Settings dialog box without making any changes.



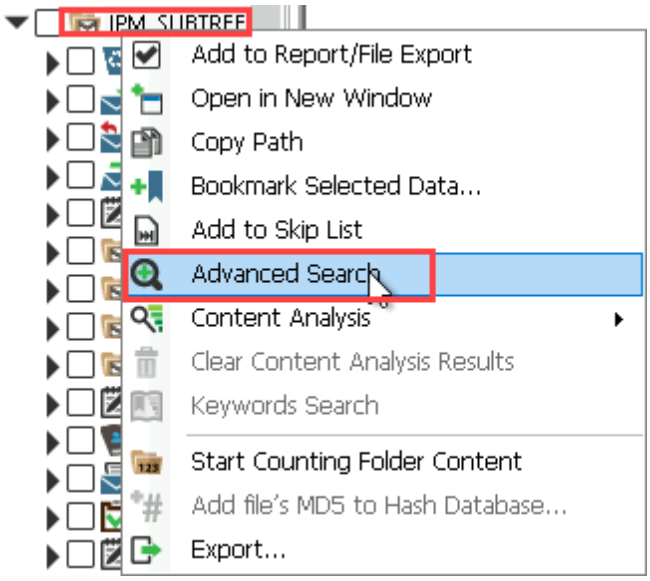
MS Outlook Database Settings dialog box

12. In the Case Content pane, **navigate** to **marvin.jonson@outlook.com.ost\Outlook Offline Storage\Root - Mailbox**, then **expand** the **IPM_SUBTREE folder node** to display the structure of the email database.



IPM_SUBTREE

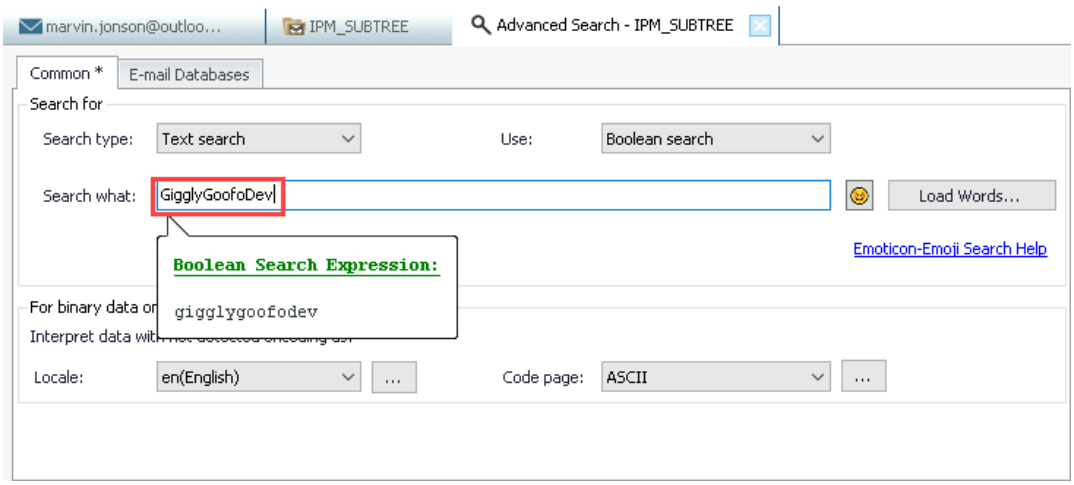
13. In the Case Content pane, **right-click** the **IPM_SUBTREE folder node** and **select Advanced Search** from the context menu to open the Advanced Search pane in the center console.



Advanced Search

Note: From your work in Part 1, you know that data was exfiltrated directly from the Giggly Goofo FTP server using compromised credentials. If Marvin was knowingly involved in the security breach, it seems likely that he may have shared the FTP credentials via email. For that reason, running a search for the FTP username seems like a good start.

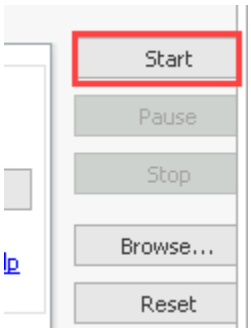
14. In the Advanced Search pane, **type** `GigglyGoofoDev` in the Search what field.



Search what field

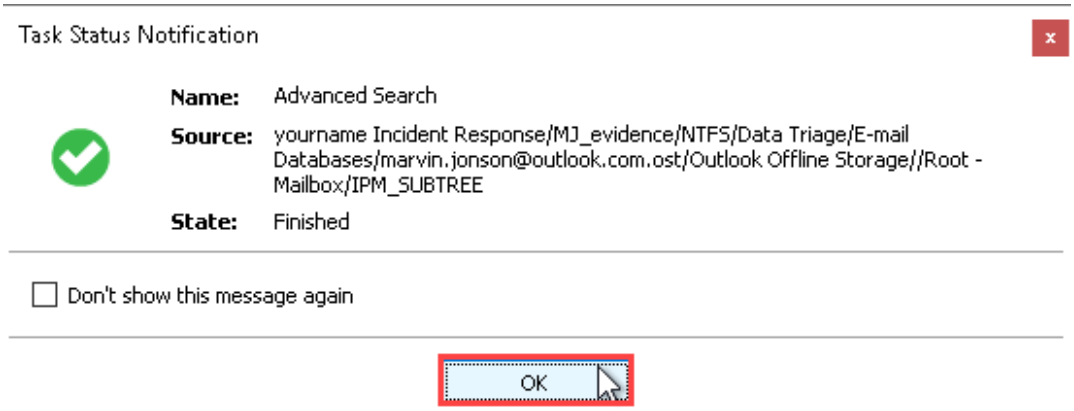
15. **Click** the **Start button** to run the search.

    You may need to scroll to the right to see the Start button. The search will take about 1 minute to complete.



Start button

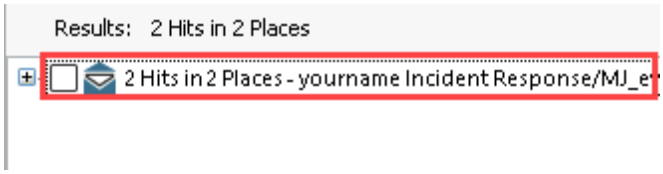
16. When prompted, **click OK** to close the Task Status Notification dialog box.



Task Status Notification dialog box

17. In the Results pane, **double-click** the **search results** to display the email in the E-mail Data pane and open the enclosing folder in a new Data Viewer tab.

    You may need to extend the E-mail Data pane to see the full email.



Results

Note: And there it is! Your search should return an email where Marvin appears to send the FTP server's publically-facing IP address and valid credentials to one Dr. Evil. While the nature of the relationship these two men arguably raises more questions than answers, at this point you have actionable proof that Marvin is involved in the data theft incident.

18. **Make a screen capture** showing the **email containing FTP credentials and the associated timestamps**.

19. **Close** the **E3 window**.

Part 3: Prepare an Incident Response Report

Note: In this part of the lab, you will document the findings of your investigation in an incident response report. For this purpose, you will reference a sample Incident Reporting Template developed by Carnegie Mellon University for the United States Computer Emergency Readiness Team (US-CERT).

1. **Navigate** to the Incident Management guide at https://us-

cert.cisa.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-IM.pdf and **review** the “Example Incident Reporting Template" on page 42.

Note: In the next steps, you will use the information gathered during your investigation to complete an abbreviated version of the sample Incident Reporting Template provided by US-CERT. At this point in your investigation, you should have evidence demonstrating that data was exfiltrated from the corporate network by one Dr. Evil via the company's own FTP server, and that Marvin Jonson provided the FTP credentials to Dr. Evil over email.

2. **Review** the information you gathered in Parts 1 and 2 of this section.

3. **Complete** the following incident response template.

Giggly Goofo Game Studios

Incident Response Team - Incident Reporting Template

Date
Insert current date here.

Name
Insert your name here.

Incident Priority
Define this incident as High, Medium, Low, or Other.

Incident Type
Include all that apply: Compromised System, Compromised User Credentials, Network Attack (e.g., DoS), Malware (e.g. virus, worm, trojan), Reconnaissance (e.g. scanning, sniffing), Lost Equipment/Theft, Physical Break-in, Social Engineering, Law Enforcement Request, Policy Violation, Unknown/Other.

Incident Timeline
Define the following: Date and time when the incident was discovered, Date and time when the incident was reported, and Date and time when the incident occurred, as well as any other relevant timeline details.

Incident Scope
Define the following: Estimated quantity of systems affected, estimated quantity of users affected, third parties involved or affected, as well as any other relevant scoping information.

Systems Affected by the Incident

Define the following: Attack sources (e.g., IP address, port), attack destinations (e.g., IP address, port), IP addresses of the affected systems, primary functions of the affected systems (e.g., web server, domain controller).

Users Affected by the Incident

Define the following: Names and job titles of the affected users.

Note: This concludes Section 1 of the lab.

Section 2: Applied Learning

Note: SECTION 2 of this lab allows you to apply what you learned in **SECTION 1** with less guidance and different deliverables, as well as some expanded tasks and alternative methods. You will analyze additional evidence and update the incident response report accordingly.

Part 1: Identify Additional Email Evidence

Note: After successfully completing an initial incident response report and submitting it to the rest of the incident response team and senior leadership for review, the security team quickly isolated the FTP server and locked all of Marvin Jonson's accounts. While your peers have commended you for your quick response and detailed documentation, you are concerned that your initial findings do not encompass the full scope of the incident, and that additional data may have been exfiltrated through other means. If Marvin was so easily compelled to give up access to the company FTP server, what else might he have done?

In the next steps, you will continue your investigation of Marvin's email archives to learn more about what led up to his sharing the FTP credentials.

1. From the vWorkstation desktop, **launch** the **E3 application**.

2. From the Welcome screen, **open** the ***yourname*** **Incident Response case file** that you created in Section 1.

3. In the Case Content pane, **expand** the **Data Triage node**, then **select** the **E-mail Databases category** to display the contents in the center pane.

4. In the center pane, **double-click** the **marvin.jonson@outlook.com.ost database** to open it.

5. In the Case Content pane, **navigate** to **marvin.jonson@outlook.com.ost\Outlook Offline Storage\Root - Mailbox**, then **expand** the **IPM_SUBTREE folder.**

6. In the Case Content pane, **right-click** the **IPM_SUBTREE folder** and **select Advanced Search** to open an Advanced Search pane in the center console.

7. In the Advanced Search pane, **click** the **Email Databases tab**, then **click** the

Sender(From) checkbox and **type** `evildr683@yahoo.com`.

You may need to scroll to the right to see the *Filter sender and recipient* section.

8. **Click Start** to run the search for emails from Dr. Evil.

   You may need to scroll to the right to see the Start button.

9. When the search is complete, **review** the results.

Note: As you review the email exchange between Marvin and Dr. Evil, you wonder how exactly Marvin met this strange man and what leverage Dr. Evil has over him, but those details are well outside the scope of your immediate investigation. Within the results, you should see evidence that Dr. Evil instructed Marvin to install a keylogger, and then to make changes to both the firewall and scheduled tasks. Both of these demands should be cause for concern and will require further investigation.

10. **Make a screen capture** showing the **email from Dr. Evil demanding Marvin install a keylogger**.

11. **Make a screen capture** showing the **email from Dr. Evil reminding Marvin to update the firewall and scheduler**.

Part 2: Identify Evidence of Spyware

Note: You now have reason to believe that Marvin may have installed a keylogger on his company workstation and made unauthorized changes to the firewall and scheduled tasks. When conducting a forensic investigation on a Windows drive image like this one and attempting to identify evidence of application installations or changes to system functions, one of your first stops should be the Windows Registry. The Windows Registry is a database that stores a wide range of settings for the operating system and applications installed on it.

In the next steps, you will open the Registry category in the Data Triage view and run a search for registry settings related to keylogging software.

1. In the Case Content pane, **navigate** to **Data Triage / Registry / Windows 10 Enterprise**, then **expand** the **Incident Response node**.

Note: Similar to the Data Triage function, the Incident Response node is an E3 function that automatically aggregates some of the most high-value sources of evidence in the Windows Registry, which allows investigators to quickly surface relevant evidence.

2. In the Incident Response node, **right-click** the **Scheduled Tasks category** and **select Advanced Search** to open a Advanced Search pane in the center console.

3. Use the Advanced Search function to **run a search** for the term **`keylogger.`**

4. When the search is complete, **review** the results.

5. **Document** the Author and Date values associated with the scheduled keylogger task.

6. **Repeat steps 2-4** on the FirewallPolicy category.

7. **Document** the port used for inbound connections to the keylogger and the name and location of the keylogger executable.

8. **Repeat steps 2-4** on the Services category, this time running a search for the name of the keylogger executable.

9. **Make a screen capture** showing the **registry key value associated with the keylogger and the localSPM service**.

Note: Now that you have concrete proof that Marvin installed a keylogger on his workstation, you will need to learn more about how he used it. To accomplish this, you will explore the SQLite database associated with the Windows 10 Activity Timeline. The Activity Timeline is a feature that was added to Windows 10 in 2018 with the stated intention of helping users remember what they did on a particular day. For forensic investigators, the Timeline is a veritable goldmine of information, as it effectively provides a granular chronological record of every activity that a user performed. In the next steps, you will drill down into Marvin's timeline and search for activity related to the keylogger.

10. In the Case Content pane, **navigate** to **Data Triage / Windows 10 Activity Timeline, right-click ActivitiesCache.db in the center pane, click Go to Source, and then navigate to /**

$DATA / SQLite Database / Tables / Activity.

11. **Repeat steps 2-4** on the Activity 1-194 table, running a search for the name of the keylogger executable.

12. In the results, **identify** the first and last start times for the keylogger.

Note: When you double-click each search result, the database record will be displayed within its enclosing table in a new Data Viewer pane, while the contents of the record will be displayed in the Properties pane. Within the Properties pane, you should see values identified as AppId, StartTime, and ExpirationTime. If you hover over the AppId value, you should see the full filepath for the application associated with the record, including the name of the keylogger executable. The StartTime and ExpirationTime should identify exactly when the application started and ended. However, they are both recorded as Unix timestamps, which are not particularly legible to humans. In the next steps, you will use a Unix timestamp converter to translate these dates into conventional, human-legible timestamps.

13. From the vWorkstation taskbar, **launch Chrome** and **navigate** to the converter at https://www.epochconverter.com/.

14. **Copy and paste** the **first start time and last start time** for the keylogger into the hex converter.

15. **Record** the first time and last time the keylogger was started.

Note: Within the Properties pane, you should also see a value titled ActivityType. Activity Type will contain either a 5 or a 6, where 5 means that the user opened the application and 6 means that they interacted with the application. Using this information, you should be able to identify whether Marvin interacted with the keylogger or simply opened it.

16. In the results, **review** the values in the **ActivityType column**.

17. **Record** whether Marvin interacted with or simply opened the keylogger.

Part 3: Update an Incident Response Report

Note: You now have email evidence demonstrating that Marvin was compelled by Dr. Evil to install a keylogger and make other unauthorized changes to his workstation, as well as concrete evidence from the Windows Registry that he followed through on those demands. In light of your new revelations, you will need to complete a second Incident Report documenting these new discoveries. As noted within the template, if the information or assessment for a specific header has not changed since your first report, you can simply respond with Unchanged. The objective of this second report is to describe the delta between your first report and your fuller understanding of what occurred.

1. **Review** the information you gathered in Parts 1 and 2 of this section.

2. **Complete** the following incident response template.

   You do not need to repeat any details from Section 1. You just the new information that you discovered in Section 2.

Giggly Goofo Game Studios

Incident Response Team - Incident Reporting Template

Date
Insert current date here.

Name
Insert your name here.

Incident Priority
Has the incident priority changed? If so, define the new priority. Otherwise, state that it is unchanged.

Incident Type
Has the incident type changed? If so, define any new incident type categories that apply. Otherwise, state that it is unchanged.

Incident Timeline
Has the incident timeline changed? If so, define any new events or revisions in the timeline. Otherwise, state that it is unchanged.

Incident Scope
Has the incident scope changed? If so, define any new scoping information. Otherwise, state that it is unchanged.

Systems Affected by the Incident

Has the list of systems affected changed? If so, define any new systems or new information. Otherwise, state that it is unchanged.

Users Affected by the Incident

Has the list of users affected changed? If so, define any new users or new information. Otherwise, state that it is unchanged.

Note: This concludes Section 2 of the lab.

Section 3: Challenge and Analysis

Note: The following exercises are provided to allow independent, unguided work using the skills you learned earlier in this lab - similar to what you would encounter in a real-world situation.

Part 1: Identify Additional Evidence of Data Exfiltration

You have now conducted two thorough investigations into the incident, but you can't shake the feeling that you may have missed something. You suspect it is possible that Marvin may have also used email to send smaller files directly to Dr. Evil. To put your mind at ease, you decide to take one last look at Marvin's drive image, this time beginning your search with the attachments stored within Marvin's Outlook account.

Review Martin's Sent folder, inspecting any attachments using the Attachments view in the E-mail Data pane. Look for any files that appear to contain Giggly Goofo intellectual property.

Make a screen capture showing an **exfiltrated file in Marvin's Outlook database**.

Part 2: Identify Additional Evidence of Spyware

After resuming your investigation, you suddenly recall seeing another suspicious email in Marvin's Inbox - one that was allegedly from the Security team and made reference to monitoring software. As a Giggly Goofo employee, you do not recall receiving a similar request from your colleagues on the Security team, and as a trained professional, you are quite certain that the Security team would not make such a request via email (they would just install it quietly during a monthly software update).

Make a screen capture showing the **email with instructions for installing additional spyware**.

Note: This concludes Section 3 of the lab.