IBM Security QRadar Incident Forensics
Version 7.2.6

User Guide

IBM

Product information

This document applies to IBM QRadar Security Intelligence Platform V7.2.6 and subsequent releases unless superseded by an updated version of this document.

Contents

Introduction to using IBM Security QRadar Incident Forensics

This guide contains information about investigating security incidents by using IBM® Security QRadar® Incident Forensics.

Intended audience

Investigators extract information from the network traffic and the documents in the forensics repository. This information is used in the investigation of security incidents.

Technical documentation

To find IBM Security QRadar product documentation on the web, including all translated documentation, access the IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

For information about how to access more technical documentation in the QRadar products library, see Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacting customer support

For information about contacting customer support, see the Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Note:

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. IBM Security QRadar may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM Security QRadar.

Note

IBM Security QRadar Incident Forensics is designed to help companies improve their security environment and data. More specifically, IBM Security QRadar Incident Forensics is designed to help companies investigate and better understand what happened in network security incidents. The tool allows companies to index and search captured network packet data (PCAPs) and includes a feature that can reconstruct such data back into its original form. This reconstruction feature can reconstruct data and files, including email messages, file and picture attachments, VoIP phone calls and websites. Additional information regarding the Program's features and functions and how they may be configured are contained within the manuals and other documentation accompanying the Program. Use of this Program may implicate various laws or regulations. including those related to privacy, data protection, employment, and electronic communications and storage. IBM Security QRadar Incident Forensics may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM Security QRadar Incident Forensics.

Chapter 1. What's new for users in QRadar Incident Forensics V7.2.6

IBM Security QRadar Incident Forensics V7.2.6 introduces new investigative tools to help you analyze files and images for suspicious content or behavior. You can also analyze links that show the relationships or connections between web pages and collaborators.

Artifact analysis for suspicious or malicious content

You can use artifact analysis to investigate incidents such as how systems became infected and whether other assets are similarly compromised.

For example, you can use file analysis capabilities on recovered packet data to see a list of all of the files and whether they contain embedded files or scripts.

You can look at image files that are flagged as having suspect content and embedded scripts.

The file entropy score and distribution can help you distinguish file anomalies and provide evidence that this file contains malware that slipped by undetected and was responsible for infecting systems.

To determine what other systems might be affected, you can use link analysis to quickly visualize all of the websites that were viewed and the subset of accesses to the infected web host.

Learn more...

Chapter 2. Security investigations

With IBM Security QRadar Incident Forensics, you can detect emerging threats, determine the root cause and prevent recurrences. By using forensics tools, you can quickly focus your analysis on who initiated the threat, how they did it and what was compromised.

As a forensics investigator, you can retrace the step-by-step actions of cyber criminals and reconstruct the raw network data that is related to a security incident.

When your organization first becomes aware of a threat or a potential security risk or compliance breach, you set objectives to assess the scope, identify the entities that are involved, and understand the motivations.

You can use the tools in IBM Security QRadar Incident Forensics in specific scenarios in the different types of investigations, such as network security, insider analysis, fraud and abuse, and evidence-gathering.

1. Recover and reconstruct network sessions to and from an IP address.
2. From the incidents that are created, you can query categories of attributes to gather evidence.

   When you create a recovery, an incident is created.
3. Use search filters to retrieve only the information that you are interested in.
4. Depending on the type of investigation, choose the forensics tool that provides you with the evidence that you need.

Suspicious content

You can use search to look for any contextual element or identifier that you know about the attacker or incident. If you use the keyword in the search, suspicious content is returned. Some of the suspicious content might relevant to the investigation.

Data pivoting

Data pivoting is achieved by making the content that is returned by a search result appear as a hotlink. For example, if you search for "Tom", the results might include emails that Tom wrote, Tom's chats, and more contextual information. When you click an email to view, every asset or entity, such as attachments or computer IDs that Tom used, appear as links. An investigator can use these links to investigate quickly.

Digital Impression

Use Digital Impression to look through the data and to map the relationship between entities, such as IP addresses, names, and MAC addresses) based on frequency. You can select one or more results to view the frequency and direction of the relationship.

Surveyor

Use Surveyor to see a timeline of activities so that you can retrace an attack. Surveyor reconstructs the session and sorts the documents in time order.

Content filtering

Use content filtering to look at a subset of content categories, such as WebMail, Pornography, to help you remove the noise or irrelevant when you search.

Network security investigations

You can use QRadar Incident Forensics to detect and investigate malicious activities that target critical assets. You can use the built-in forensics tools to help you remediate a network security breach and prevent it from happening again.

Use QRadar Incident Forensics investigative tools to help you find out how the event occurred, minimize its impact, and do everything that you can to prevent another breach.

Patient zero: Identify the source of an attack

In this scenario, an organization is alerted to a suspected breach. It seeks to find the initial point of an attack to isolate the source. The organization must quarantine the compromised entities to prevent the spread of the attack to other parts of the organization.

Objectives

To solve the problem in these investigations, the organization has these objectives:
- Determine the type of attack.
- Identify the initial entry point of the threat.
- Get details about the malicious payload.
- Understand how the malicious payload was disseminated beyond the point of entry.

Investigation

Use the tools on the **Forensics** tab to help you investigate.
1. Use free-form search to search for symptomatic attributes that are associated with malicious payload.
2. Use content categories to filter out content that isn't relevant to the investigation.
3. Examine suspect content that is flagged by the product.
4. Use Digital Impressions and visualizations to explore extended relationships of the malicious payload, perpetrator, or target.
5. Use data pivoting and follow data linkages to identify patient zero.
6. Use Surveyor to see a timeline of activities so that you can retrace an attack.

Compromised systems

In this scenario, an organization is alerted that one or more of their systems was compromised by an advanced cyber attack technique such as a watering hole, phishing, brute force, or an SQL injection.

Objectives

To solve the problem in these investigations, the organization has these objectives:
- Determine the extent of the compromise within the organization.
- Understand the type of operational risk of the compromise on each system.
- Uncover any peripheral actions that the initial attack did to circumvent cleanup activities and detection.

Investigation

Use the tools on the **Forensics** tab to help you investigate.
1. Use free-from search to search for malicious payload or a compromised asset.
2. Examine suspect content that is flagged by the product.
3. Use Digital Impressions and Visualizations to explore entity relationships that result from compromised systems.
4. Use Surveyor to see a timeline of activities so that you can retrace an attack.
5. Discover inconsistencies or suspicious interactions across data categories by using free-form search, data pivoting, and suspect content.

Data leaked to unauthorized entities

In this scenario, an organization is alerted that sensitive data was leaked to unauthorized entities within the organization or to external parties.

Objective

To solve the problem in these investigations, the organization has these objectives:
- Determine the nature and the amount of leaked data.
- Understand the techniques that were employed.
- Uncover the perpetrators.
- Identify the source of the leak.

Investigation

Use the tools on the **Forensics** tab to help you investigate.
1. Use free-form search to search for identifiers of data that was leaked.
2. Examine suspect content that is flagged by the product.
3. Review the full extent of leaked or leaking data by reviewing data reconstruction.
4. Use Digital Impression and visualizations to explore all involved entity relationships.
5. Use Surveyor to see a timeline of activities so that you can retrace an attack.
6. Use free-form search to discover the motivations for the data leak.
7. Use data-pivoting to find linkages to other data that was possibly leaked.

Insider analysis investigations

Use QRadar Incident Forensics to detect collusion, sabotage, and misuse of access. Identify the perpetrator, identify collaborators, identify compromised systems, and document data losses.

Misuse of access

In this scenario, an organization is alerted that one or more of their employees are misusing credentials or are used as a proxy to access sensitive systems and data for unauthorized activities.

Objective

To solve the problem in these investigations, the organization has these objectives:
- Determine the user's identity.
- Resolve who or what is employing the identity for unauthorized activities.
- Understand the objective of the misuse of access.
- Assess whether the entity has more identities that might also be misused.

Investigation

Use the tools on the **Forensics** tab to help you investigate.
1. Use free-form search to search for identities who are accessing sensitive systems or data.
2. Resolve which of those access attempts are suspicious by looking at suspect content, doing free-form searches, data pivoting, and content filtering.
3. View the data reconstruction for the content that is being accessed.
4. Retrace any patterns of access and evaluate frequency in Surveyor.
5. Use Digital Impression to reveal aliases that used by a single entity.

Collusion

In this scenario, an organization is alerted that one or more stakeholders are colluding among themselves or with external parties to engage in activities that are detrimental to the organization.

Objective

To solve the problem in these investigations, the organization has these objectives:
- Determine the colluding entities.
- Understand the nature and patterns of interactions among the collaborators.
- Uncover the content that underlies the scheme.
- Reveal the duration of the scheme to understand risk scope.

Investigation

Use the tools on the **Forensics** tab to help you investigate.
1. Use free-form search to search for identifiers of entities that are involved.
2. Examine suspect content that is flagged by the product.
3. Use Digital Impression, visualizations, and content filtering to identify relationships that might be suspicious.
4. Use Surveyor to trace the activities of involved entities to get the content of the interactions.
5. Discover the motivations for the collusion by reviewing reconstructed documents.
6. Use free-form search and data-pivoting to find the beginning of the colluding activities.

Sabotage

In this scenario, an organization is alerted that one or more stakeholders are attempting to disrupt operations. The stakeholder might be being used as a proxy.

Objective

To solve the problem in these investigations, the organization has these objectives:
- Identify the saboteur.
- Understand the techniques that were employed by the saboteur.
- Assess the impact and scope of the disruption.
- Pinpoint vulnerabilities that were exploited by the saboteur

Investigation

Use the tools on the **Forensics** tab to help you investigate.
1. Use free-form search to search for symptoms of the sabotage.
2. Examine suspect content that is flagged by the product.
3. Use visual navigation, Digital Impression, and content filtering to explore the symptoms and detect identifiers of the saboteur.
4. Use Surveyor to trace the activities of the saboteur.
5. Use data reconstruction to discover saboteur roles and motivations.
6. Use data reconstruction to review the content that the saboteur used.
7. Use free-form search, Surveyor, and suspect content to reveal the compromised systems and procedures that enabled the sabotage.

Fraud and abuse investigations

Use QRadar Incident Forensics to locate unauthorized transactions, unsanctioned allocation of resources, protocol deviations, and evading legal controls.

Unauthorized transactions

In this scenario, an organization is alerted that unauthorized transactions are leading to a negative financial impact on business operations.

Objective

To solve the problem in these investigations, the organization has these objectives:
- Locate the unauthorized transactions.
- Identify the entities that are involved and responsible for the unauthorized transactions.
- Understand the frequency and the trends of the unauthorized transactions.
- Assess the risk scope of the unauthorized transactions.

Investigation

Use the tools on the **Forensics** tab to help you investigate.
1. Use free-form search to search for any inconsistent or suspicious transactions.
2. Use free-form search and data-pivoting to search for repetitions of those transactions.

3. Use data-pivoting and Digital Impression to discover the entities that associated with the suspicious transactions.
4. Uncover the content of the transactions to reveal quantitative value by reviewing reconstructed documents.

Unsanctioned allocation of resources

In this scenario, an organization suspects unsanctioned allocation of resources, which is leading to a negative financial impact on business operations.

Objective

To solve the problem in these investigations, the organization has these objectives:
- Locate the misallocation of resources.
- Identify the entities that are involved and responsible for the misallocation of resources.
- Understand the motivations for the unsanctioned allocation of resources.
- Assess the size and scope of the misallocated resources.

Investigation

Use the tools on the **Forensics** tab to help you investigate.
1. Use free-form search for communications that are associated with allocated resources.
2. Use free-form search, data-pivoting, and Digital Impression to find identifiers of entities that are making unsanctioned allocation of resources.
3. Process the content of the interactions that are involved to assess motives by reviewing reconstructed documents and by using visualizations.
4. Use Surveyor to retrace allocation activities to understand the quantity of misallocated resources.

Protocol deviations and evading legal controls

In this scenario, an organization is alerted that business, IT protocols, and legal controls were circumvented, which can result in a negative financial impact.

Objective

To solve the problem in these investigations, the organization has these objectives:
- Assess which protocols or legal controls were evaded.
- Pinpoint the entities who engaged in this behavior.
- Understand the motivations of these entities.
- Assess the pervasiveness of this misbehavior.

Investigation

Use the tools on the **Forensics** tab to help you investigate.
1. Use free-form search to search for business processes that are governed by protocols or controls.
2. Use free-form search, data-pivoting, and data reconstruction to cross-reference with documentation that outlines the protocols and legal controls.
3. Use content filtering, free-form search to discover specific instances where protocols/controls were evaded.

4. Use Digital Impression, visualizations, data-pivoting, and content filtering to find the associated entity identifiers.
5. Use Surveyor to retrace entity activities to explore possible motivations.

Evidence collection investigations

Use QRadar Incident Forensics to assess the risk of vulnerabilities in the organization, quantify the confidence in identifying threats or perpetrators, and refine security practices.

Confidence in identifying threats

In this scenario, an organization is alerted about a certain threat, exploit, or vulnerability. To justify remediation efforts that might otherwise preempt normal business operations, they want to quantify a confidence interval for any associated risk.

Objective

To solve the problem in these investigations, the organization has these objectives:
* Validate the susceptibility to the security risk.
* Determine whether there is evidence of the security risk.
* Assess the breadth and monetary impact of the security risk.
* Understand the nature of the security risk

Investigation

Use the tools on the **Forensics** tab to help you investigate.
1. Use free-form search, suspect content, and data-pivoting to search for the threat, exploit, or vulnerability by using potentially targeted entities as a starting point.
2. Use free-form search and data-pivoting to compile occurrences.
3. Use free-form search to cross-reference documents that might provide reference to the impact.
4. Use Digital Impression and visualizations to identify the affected entities.
5. Use Surveyor to analyze the activities that are associated with the threat or perpetrator.

Refining security practices

The detection of new and risky behaviors motivates an organization to assess whether existing security practices are sufficient. In this scenario, an organization seeks to qualify the effectiveness of its security rules for the risks that it faces.

Objective

To solve the problem in these investigations, the organization has these objectives:
* Recognize new or risky behaviors.
* Assess the efficacy of existing security rules.
* Understand the security gaps that emerge due to dynamic operations.
* Evaluate the effectiveness of proposed security practices.

Investigation

Use the tools on the **Forensics** tab to help you investigate.

1. Use free-form search to search for new or risky behaviors, such as for mobile users and cloud-based services, by using domain and organizational knowledge.
2. Examine suspect content and use Surveyor to cross-reference these behaviors with existing security rules or practices.
3. Use free-form search, Surveyor, content reconstruction, and visualization to analyze alerts from security rules for frequency of false positives.
4. Use free-form search, Surveyor, content reconstruction, data-pivoting, and visualization to discover false negatives that are undetected by existing security rules or practices.

Risk assessments

In this scenario, a security bulletin that outlines certain vulnerabilities, exploits, or malicious behavior prompts an organization to do a risk assessment. The risk assessment determines whether the organization is susceptible or is already compromised.

Objective

To solve the problem in these investigations, the organization has these objectives:

- Assess the presence of identified vulnerabilities in the organization.
- Detect the malicious presence of external parties.
- Uncover evidence of any compromise.
- Determine whether the organization is a victim of an exploit.
- Determine the user's identity.

Investigation

Use the tools on the **Forensics** tab to help you investigate.

1. Use free-form search to search for traits of vulnerabilities, exploits, or other malicious behavior that is specified in the security bulletin.
2. Use free-form search to cross-reference research or other data to derive indicators.
3. Use Surveyor to investigate interactions that possibly exploited vulnerabilities that were identified.
4. Examine suspect content that is flagged by the product.
5. Review content that underlies potentially risky interactions by using data reconstruction.
6. Use Surveyor to retrace the activities of potentially risky entities.

Chapter 3. Getting started with forensics investigations

To get started with forensics investigations in IBM Security QRadar Incident Forensics, use the **Quick Start** menu to navigate and filter data that is in the forensics repository. This launchpad contains pre-defined summary queries that you can use to start a search or get relationships for an entity.

To get started, follow these guidelines:

1. Start a forensics recovery or search from an offense on the **Offenses** tab.
   - If you right-click an offense or any IP address and run a forensics recovery, forensics retrieves the raw capture data for the specified time ranges from the capture device, extracts and rebuilds documents, and then adds the results to the forensics repository.
   - If you right-click an offense or any IP address and run a forensics search, the forensics repository is filtered and searched for that IP address. Results are then shown in the main grid on the **Foresnics** tab. You can refine your search by building queries.

   When QRadar Incident Forensics receives a search request, it processes the packet capture data and puts it back into the format that was sent to the intended recipient. Microsoft Word documents, for example, are recovered as Word files. Voice-over-IP phone calls are recovered as audio files. The recovered files are then indexed by using both metadata and file contents to make them searchable.

2. On the **Forensics** tab, click **Quick Start**.

   After you run a recovery or a search, instead of doing free-form searches and building your own queries, you can quickly start your investigation by using the pre-defined queries from the **Quick Start** menu on the **Forensics** tab. For example, you can look at the **Suspect Content** category and run one of the queries such as **entity alert**. *Suspect content* is a based on a defined set of rules on content that signify suspicious activity. An *entity alert* flags a possible malicious entity that is involved in breaching a security policy.

   The content categorization and filtering capabilities help to reduce the volume of data returned

3. From the **Grid**, select documents to look at.

   QRadar Incident Forensics returns prioritized search results. Similar to the way that search engine optimization prioritizes sites in an Internet search, the most frequent occurrences appear at the top of the list.

   You can start to pivot the data by clicking links and searching the metadata that is associated with the document. The data pivot capabilities provide various search views and data summaries.

4. To investigate relationships between all actions and the security incident, in the document view, select a link and right-click **Get relations for**.

   After you investigate attributes, filter the information that you gather by connecting entities.

5. Click **Digital Impressions** to follow the identity trail and get a compiled set of associations.

   A digital impression is an index of metadata that can help identify suspected attackers or rogue insiders by following malicious user trails. In building these relationships, QRadar Incident Forensics uses data from network sources such

as IP addresses, MAC addresses, and TCP ports and protocols. It can find information such as chat IDs, and it can read information such as author identification from word processing or spreadsheet applications. A digital impression can help uncover associations by linking the entity's identity to identifying information for other users or entities.

QRadar Incident Forensicssearches and bookmarks

Investigators use IBM Security QRadar Incident Forensics to extract relevant data from network traffic and documents.

Searching and bookmarking records

To enable intuitive forensics activityQRadar Incident Forensics retrieves packet data and ingests other content. This technology provides search-driven data exploration, session reconstruction, and forensics intelligence to help security incident investigations.

Investigators focus their investigation through course-grained actions and then proceed to fine-tune those findings into a relevant final result set. A simple, high-level approach is to search and bookmark many records at first. Then, focus on the bookmarked records to identify a final set of records. Determine which material is relevant and tweak queries to include and or exclude items. Use that material to prove a hypothesis.

As you develop new leads, you can follow up on them by using other methods. You can use visualization and analysis tools to manually and automatically assess the results for relevance. You can also use varied queries to get a different aspect of the same issue.

Processing bookmarked results

When you find results that are significant to your investigation, you can bookmark the results for deeper inspection and final determination. Bookmark more than you think you need. If in question, bookmark it. You want to eliminate the irrelevant material and focus on what you think is relevant.

After you bookmark a set of results that you think are relevant, you can fine-tune your inspection.

1. Inspect each bookmarked document through the visualization and analysis tools.
2. Attach case notes to the documents and make final decisions on each document about its relevance to the case.
3. If a record is not relevant, remove the bookmark.

   In the investigation process, you identified the relevant material in the repository and you now have a set of relevant bookmarked records.
4. Print, export or process the relevant records.

Document search and investigation

Investigators search for documents that are relevant to a lead or a hypothesis about how a security incident took place.

Searches

Instead of manually sifting through masses of documents, most of which are not related to the case, investigators use the forensic repository to extract documents that satisfy characteristics of interest. For example, a document that occurred within a certain time period, pertains to a topic of interest, or a document that is sent or received by a suspected attacker.

Searches can be specific. For example, "find the exact character string "Mission Alpha"" is specific. Alternatively, searches can be general. For example, "find all social security numbers wherever they exist in the repository" is more general.

Searches can be simple and based only on one criterion. Complex search results must satisfy multiple conditions. For example, finding all email between two suspected attackers about a topic and exclude emails that contains attachments, is a complex search. The purpose of a search is to quickly and accurately reduce the records to a manageable working set. With a smaller set of documents for the investigator to inspect, the documents have a higher likelihood to be relevant to the case.

Running a recovery on an IP address or port

You can run a recovery on one or more IP addresses or ports. If you don't enter an IP address or port, all TCP and UDP traffic is recovered. If you enter multiple IP addresses or ports, you must use a comma to separate them.

Restriction: As a rule, you can enter about 7 IPv4 addresses and 7 ports or a maximum of about 255 characters at one time. The **IP Address** and **Port** fields are combined with other phrases to create a filter string. The filter string can't be more than 255 characters

Forensic cases

Cases are logical containers for your collection of imported document and packet capture files.

Cases are either created by administrators or investigators that have privileges to create cases. Administrators create and assign cases to investigators. Investigators might create a new case when they retrieve packet capture data from an IP address in IBM Security QRadar.

Related tasks:

"Uploading pcap files and documents from external systems to forensics cases" on page 14
You can upload external data into specific cases.

Collections

Use collections to group related data from a specific source, such as a packet capture (pcap) data file, PDF, or network stream.

Collections are used to identify and manage groups of related data. You can quickly delete the group data in the collection when your investigation is complete.

Collections are either created by administrators or investigators. Administrators create collections to manually load data to IBM Security QRadar Incident Forensics. Administrators also add collections to cases. Investigators might create a new collection when they initiate the retrieval of packet capture data from an IP address in IBM Security QRadar.

Consider the following rules for collections and collection names:
- Collection names must be unique.
- Cases include one or more collections.
- Collections can be added to multiple cases.
- Search results return duplicate data when an investigator owns two cases with the same collection.
- If a collection name is not unique when a new pcap is uploaded, the original collection is deleted before the new pcap is uploaded.

Uploading pcap files and documents from external systems to forensics cases

You can upload external data into specific cases.

Before you begin

An administrator must enable secure FTP permissions for the user who wants to upload external files.

About this task

IBM Security QRadar Incident Forensics can import data from any accessible directory that is on the network. The data can be in a number of formats, including but not limited to the following formats:
- Standard PCAP format files from external sources
- Documents such as text files, PDF files, spreadsheets, and presentations
- Image files
- Streaming data from applications
- Streaming data from external PCAP sources

You can upload multiple files to a case.

Restriction: The case name must be unique. You cannot create a case that has the same name as an existing case.

Procedure

1. In the FTP client, do the following steps:
   a. Ensure that Transport Layer Security (TLS) is selected as the protocol.
   b. Add the IP address of the QRadar Incident Forensics host.
   c. Create a logon that uses the QRadar Incident Forensics user name and password that was created.
2. Connect to the QRadar Incident Forensics server and create a new directory.
3. To FTP and store pcap files, under the directory that you created for the case, create a directory that is named `singles` and drag the pcap files to that directory.

4. To FTP and store other files types that are not pcap files, under the directory that you created for the case, create a directory that is named `import` and drag the files to that directory.

5. To restart the FTP server, type the following command:

   `etc/init.d/vsftpd restart`

6. To restart the server that moves the files from the upload area to the QRadar Incident Forensics directory, type the following command:

Results

You can see your case in one of the tools on the **Forensics** tab.

Forensics repository queries

Investigators specify the characteristics of the documents they are interested in retrieving from the forensics database. Multiple queries are used to find a set of documents for an investigation.

Multiple queries and manual inspection of a small set of documents is superior to sifting through the entire repository. Ideas for subsequent queries and refined queries are often hatched during the inspection of an irrelevant document.

Increased quantity and specificity of query terms result in higher relevance results sets. Your goal is to define as much as is known about the results that you want and to be highly specific when possible. Any number of query terms can be entered into the search criteria. You separate terms with a space or with a Boolean operator. Terms that are separated only with a space imply a Boolean logical OR operator. An OR operator means that finding any of the terms is equally desirable. Results that satisfy the most search terms are placed at the top of the list to indicate the strength of the match to the query terms.

A single search criterion is also referred to as a query term. Searches typically involve more than one query term. The set of query terms for a single search is also referred to as a Query String. Becoming adept at formulating queries takes practice, but it is not hard. It involves only a few query terms and learning how to create and negate the terms in combinations that give you what you want. Since query strings are saved in QRadar Incident Forensics, you can continuously fine-tune your searches as you learn the data better.

Related tasks:

"Visualizing relations and associations" on page 26
Use the Visualize window to look at relations among attributes in recovered documents. For example, you can inspect the email addresses that communicated with a specific email address.

Free-form query terms

Investigators search for exact character string matches by entering the query terms directly in the search criteria field on the **Forensics** tab. You can use single or multiple word queries.

The following table describes the type of search queries that can be used.

Table 1. Types of free-form queries

Type of search query	Description	Example
Single word query	Searches for one term in the documents.	puppies
Single query with wildcard	Searches for a match for one or more characters in the middle or end of a query term. **Restriction:** Wildcard characters cannot be used as the first character in a search.	te?t test* te*t
Multiple word query	Specifies that search results are returned in query term relevancy order. The documents that contain both query terms are listed first, followed by documents that contain only one of the query terms. Documents containing only one query term are ranked according to the number of occurrences of the individual query term.	free puppies
Multiple word query with double quotation marks	Matches the exact string. Documents that contain both words, but not in this order and in this proximity are not returned as results. Effectively, the double quotation marks turn these two words into a single string or query term. To the search engine, they are not seen as two separate words anymore.	"free puppies"
Multiple word query that uses the AND operator	Specifies that both query terms must be present in the document to result in a match. The query terms can be in any order and it is not necessary for them to be in close proximity to each other.	free AND puppies

Metadata tags

Common entities are tagged to allow investigators to quickly retrieve exact result sets from relevant documents.

Many metadata fields might be used in the Incident Forensic index, depending on the type of session, document, or protocol.

When you specify a metadata tag name, it must be exact and exist in the forensic repository.

The following table lists types of metadata tag searches.

Table 2. Metadata tag searches

Type of metadata tag search	Format	Example
Standard	`MetadataTag:<value>`	`ApplicationProtocol:http`
Wildcard	`MetadataTag:*`	`CreditCardNumber:*`
Range	`MetadataTag:[<start value> TO <end value>`	`Duration:[30 TO 56]`

Related concepts:

Investigators bookmark documents and add notes to documents to track ideas and rationale about documents in their case.

Boolean combinations

Multiple query terms can be strung together by using simple Boolean operators to create highly targeted query strings. Properly formed, these query strings can return results that exactly match what an investigator is looking for.

The basic Boolean operators are AND, OR, NOT, and (). The AND operator specifies that both query terms must match in the document. The OR operator specifies that either query term can be found in a document. The NOT operator negates, or removes results, that match the query terms that are negated. The () operator groups query terms and values to apply functions to a set, apply multiple values to a single function, or for clarity of syntax.

Boolean operators must be uppercase.

The following table lists the Boolean operators and an example of a query string.

Table 3. Boolean operators for query strings

Boolean operator	Example query string	Example explanation
AND	`TcpPort:80 AND Protocol:http`	Two query terms are used to find all standard web traffic. If web testing occurs on Port 8080, then it would not be a match since both query terms would not be true.
OR	`Collection:yahoo* OR` `Collection:cnn* OR Collection:msn*`	Three query terms are used to limit the results to results from the Yahoo, CNN, and MSN document collections in the forensics repository.
NOT	`ApplicationProtocol:http AND NOT` `ServerTcpPort:(80 OR 8080 OR 81)`	Searches for traffic with non-standard port usage. The first query term looks for standard HTTP traffic and the second query term eliminates all traffic that is using accepted HTTP ports.

()	`(ApplicationProtocol:http AND NOT`
	`ServerTcpPort:(80 OR 8080)) OR`
	`(ApplicationProtocol:pop* AND NOT`
	`ServerTcpPort:110)`
	
	`NOT (Collection:yahoo* OR`
	`Collection:cnn* OR Collection:msn*)`
		These queries use parentheses effectively to achieve complex goals. Without parentheses, these queries are longer and more complex to formulate and debug.

Query builder tool

Use the query builder tool to create searches or manage saved searches.

The query builder tool graphically walks investigators through the process of creating powerful searches that use categorized lists of query terms with examples.

Table 4. Parameters for the query builder tool

Parameter	Description
Select Category	Filters the list of metadata tags available in the **Select Field** list.
Select Field	The metadata tags used to tag the information in the forensics repository.
Query Example	Runs the query that is in the **Query Input** field and reports the number of results.
New	Replaces an existing query with the new query when you click **Insert Query**.
AND	Combines a new query with the existing query when you click **Insert Query**. the documents must match both query terms.
OR	Combines the new query with the existing query when you click **Insert Query**. Documents must match either term.

Investigators can save and organize searches in folders on the file system, which allows sharing between investigators. Investigators use descriptions or names for saved queries for reference, management, and understanding purposes.

The **Use Query** function on the **Query** tab is used to send a saved query to the **Search Criteria Input** filed for execution.

Investigators use the previous query list to find previously run queries and re-execute them by selecting the query that they want to run and clicking **Insert Query**.

Query filter tool

The query filter tool uses the active data to provide visual cues for building persistent filters.

The query filter is a persistent background filter that reduces the active document set that is being interrogated by the query string. By using a filter, you reduce the available document set without overloading the query string with static query terms. As a result, you have more control over the query string.

The query filter is a good place to start an investigation because of the case-dependent filter type lists, dynamic updating, and real-time result summary. The filter type lists are populated with all the values that are found in the cases that are available to you. You can quickly see what data is contained within the cases that you own. Selecting or clearing filter type list items automatically updates the result summary. You can quickly see the effectiveness of the filter and how large of a document set remains when you use the filter.

Tuning the default query filter is not advised for queries that you want to reuse. For queries that you want to keep, create a new query filter. If you modified the default query filter, reset it when you are finished to prevent mistaken exclusion of documents from future search queries.

Results for active filters

Investigators view results from active filters in the result summary section on the query filter tool.

As the filter is changed the summary updates to display the total document count and available document count. Total document count is the number of documents available to the investigator before the filter is applied. Available document count is the number of documents available after the filter is applied. Investigators use these counts to judge the effectiveness of their filter and adjust appropriately as they are building it.

Search filters for the query filter tool

Investigators filter the data for their assigned cases. The data is separated into groups by filter type, for example, IP address or MAC Address.

Using the logic action toggle, the investigator can either include or exclude items that are selected from the list.

Each search filters group has a logic action toggle that can be set to either include or exclude the items that are selected in the list. When set to include, the items in the list are joined with a logical AND, meaning each available document contains all of the items selected. When set to exclude, a logical OR is used, meaning each available document does not contain any of the items selected.

Investigators can use the **UserQuery** group to formulate their own query strings to be added to the filter.

Limiting the number of returned documents in a search

You can add filters to your IBM Security QRadar Incident Forensics queries to limit the number or type of documents that you see in the search results page.

Procedure

1. On the **Forensics** tab, click the **Query Filters** icon.

   The data is separated into groups by filter type.

2. In the Search Filters window, for each filter type, choose whether to include the documents in the search results by clicking **Include** or **Exclude**.

3. To find an item in a filter group, follow these steps:

   a. In the **Filter Type** column, expand a filter group.

   b. In the Search window, select the criteria and click **Find**.

      When you search for a record in the **Webcategory** filter group, all matching category fields are displayed. For example, when you search for **Webcategory equal chat**, **Chat**, and related categories, such as **Instant Messaging**, **Webmail/Unified Messaging**, **Search Engines/Web catalogs/Portals**, and **Cloud** are displayed.

Document annotations

Investigators bookmark documents and add notes to documents to track ideas and rationale about documents in their case.

Documents can be bookmarked on the main results screen, and in the surveyor tool on the chronological grid that displays the sequence of documents that are exchanged during an interaction. Since queries and investigations might be complex, investigators bookmark all records, including documents with small interest. Using a bookmark eliminates the need to re-create the complex queries and lines of investigation. Annotations can be created after a record is bookmarked.

During an investigation, there are times in which you want to follow two or more paths. Use the browser function to duplicate the current tab that you are on. Duplicating the tab helps you avoid having to remember to go back and follow the additional paths or to remember how to get to the branching point. You can duplicate the current tab any number of times as required. Follow each different path in a different tab and bookmark relevant documents along the way. You can add a note that designates the path that led to each bookmarked document.

Notes are a way of recording thoughts while you investigate. Notes can be removed only by an administrator. Notes are tagged with the user ID of the investigator and the time stamp when it was entered. When documents are exported, notes are output with the reconstructed document and its attributes.

Related concepts:

"Metadata tags" on page 16
Common entities are tagged to allow investigators to quickly retrieve exact result sets from relevant documents.

Chapter 4. Investigation tools

Investigators use the Surveyor, Digital Impressions, Export, and Visualize tools to manage data in different ways.

The search results page is the default page on the **Forensics** tab. Search results are available on the **Grid** tab. Investigators use the search results on the grid to quickly search for and access documents. On the **Grid** tab, use the Surveyor, Digital Impressions, Export, and Visualize tools to further the investigation.

Row indicator

The row indicator provides a unique identifier for each document that is returned in a result set. Use the row indicator to send a document and all required related documents to the Reconstructed View visualization tool.

Row sort

You can sort the rows that are displayed in the grid. Because the total number of results might be larger than the number of results that are displayed on the grid, the entire result set cannot be sorted.

Documents viewed indicator

The documents viewed indicator is a small circle that alternates between red and green to indicate whether an investigator viewed a document.

Document selection

Investigators use the displayed documents selector to choose the number of documents that display in the results grid. You can use SELECT ALL to send documents to a subsequent function and you can send many documents for processing or visualization. When you select documents by using the displayed documents selector, you are selecting all documents and not just the documents present in the grid.

Network and document visualization

Investigators use the visualization tool to detect patterns, understand where the most network traffic and document congestion is during a specified time period, and view suspect content. For example, investigators can visualize network traffic patterns, such as servers that are accessed after company hours.

The VGrid tool is divided into time blocks. Suspect content, such as network traffic or documents, is depicted by a red rectangle on the grid. A green rectangle depicts regular content. A brightly colored block indicates more traffic. The higher the saturation of the color, the greater the amount of traffic. The brightness of a time block is relative to the current data displayed in the VGrid tool. For example, a brightly colored time block becomes darker as different time blocks are loaded with more data.

Investigators can view the types of network traffic and the number of documents for each time block that contains content.

Inspecting network traffic and documents in a time block

Investigators might want to inspect individual documents, browsed websites, or sent emails within a specific time block.

Procedure
1. On the **Forensics** tab, select the **VGrid** tab.
2. Use one of the following options to inspect content in a time block:
   - To view the types of network traffic and number of documents, hover over the time block.
   - To search content in the time block, select one or more time blocks. Right-click and select **Search selected time blocks**.
   - To view the sequence of events, select the time block and then select **Surveyor**.
   - To visualize the content, select a time block and then select **Visualize**.

Surveyor tool

Use the surveyor tool to visualize a sequence of events in a security incident as they occurred.

This tool is used by investigators to see what suspected attackers viewed and their actions. The surveyor tool depicts the chronological sequence of activities in a security incident in a movie-like visualizer. Because Surveyor is time-oriented, the selection of a single document from the results screen does not show much. If too few documents were selected, expand the time radius around the selected documents in the **Attributes** tab. Expand the time by clicking the **Show Context** link.

Investigators can filter their queries by case time, protocol, and IP address.

You can view the **List** tab to see a chronological list of documents that were sent and received. The step-by-step recreation of the interaction is depicted in the Surveyor tool.

Green document ID numbers indicate that a document was reviewed by an investigator, while documents with red ID numbers were not reviewed.

Reconstructed document view

The **View** tab shows a reconstructed view of the document that is selected on the left side of the screen in the List view.

This powerful combination of sequencing on the left and reconstruction on the right makes it possible to see what suspected attackers saw and did on the network. In addition to the visible documents that traversed the network, Surveyor also shows the behind-the-scenes computer-to-computer handshakes and certificate exchanges that took place.

Related tasks:

Chapter 5, "Investigating network traffic for an IP address," on page 33
To get visibility of the relevant content in the conversations that occurred during a security incident, you can recover and reconstruct network traffic that is associated with an IP address. You can also search through existing cases that are related to an IP address.

Extracted document content

The **Text** tab shows content that is extracted from the document. The document content is unformatted.

This text is from the search engine indexer.

Document export in QRadar Incident Forensics

In IBM Security QRadar Incident Forensics, all exported documents, except exported pcap documents, include the reconstructed document, the raw text of the document, attributes, and notes that are attached to the document.

When pcap documents are exported, no reconstruction is done. For example, when you export a web page, anything that the browser downloaded during the main connection is downloaded. Usually, most of the text content is downloaded during main connection. However, most modern browsers use multiple connections to download more items, such as style sheets and images, which are not part of the export. When you export, the pcap content is not first reconstructed.

Another example is complex protocols, such as FTP and VOIP, where there is a main command and control connection and a separate data connection. If you export the pcap files for a VOIP call or an FTP download, the data is not reconstructed and you might get results that you don't expect.

Exporting documents as pcap files

You can export documents as pcap files from multiple IBM Security QRadar Incident Forensics and IBM Security QRadar Packet Capture appliances.

Restriction: The content that you export to pcap format is not reconstructed.

Procedure

1. To export data from selected documents, in the recovery grid on the **Forensics** tab, select the check boxes next to the documents, and then click **Export**.

   You can select a maximum of 25 documents to export to pcap format.
2. From the **Select Export Type** list, click **PCAP**.
3. After all of the documents for a QRadar Incident Forensics host are exported, you can click **Download**.
4. If the export of a document fails, export the document again by clicking the **FAIL** message.

Results

If you export a single pcap file, the pcap file is downloaded. If you export more than one pcap file, then the pcap files are assembled into a compressed file (.zip) and the compressed file is downloaded.

Each document stores the IP address of the QRadar Incident Forensics host and the IP address of the QRadar Packet Capture device that the document originally came from. If you remove a QRadar Incident Forensics host or move a QRadar Packet Capture, you might not be able to do an export.

Digital Impression

A *digital impression* is a compiled set of associations and relationships that identify an identity trail. Digital Impression reconstruct network relationships to help reveal the identity of an attacking entity, how it communicates, and what it communicates with.

Use the Digital impression tool to quickly answer these important questions:
- What is known about this suspected attacker, computer, or IP address?
- Who has this suspected attacker talked to?
- Who is in their network of contacts?
- Is the suspected attacker trying to disguise their identity?

Online identifiers

Online identifiers, such as email addresses, Skype addresses, MAC addresses, chat IDs, social media IDs, or Twitter IDs are used to identify entities or people. Known entities or persons that are found in the network traffic and documents are automatically tagged.

IBM Security QRadar Incident Forensics correlates tagged identifiers that interacted with each other to produce a digital impression.

The collection relationships in digital impression reports represent a continuously collected electronic presence that is associated with an attacker, or a network-related entity, or any digital impression metadata term. Investigators can click any tagged digital impression identifier that is associated with a document. The resulting digital impression report is listed in tabular format and is organized by identifier type.

Getting relationship information

A digital impression report shows the interactions between a *centering identifier* and all other identifiers. A *centering identifier* is the online identifier that is source of interest in a security incident.

The top-most identifier in many categories is usually the identity of the centering identifier in that identifier type or category. For example, if the identifier is a MAC address, the email address that has the most interactions likely belongs to the suspected attacker who owns the computer. However, if IP addresses are assigned dynamically, you must also investigate the IP addresses that are assigned over a time range.

The correlations between other categories and the centering identifier are typically less strong. Before you decide to act based on the digital impression, validate the data with independent sources. Use the Digital Impression tool to expand the radius of an investigation to more suspected attackers and entities.

Investigating relationships to track identity trails

Digital Impression reconstructs network relationships to help you identify an attacking entity and other entities that it communicates with.

The Digital Impressions tool shows the frequency distribution of correlated events. The tool shows relationships between entities and counts the relations. The higher

the count, the stronger the relationship. For example, if you view the relationships between an email address and other entities, you can see who is communicating with whom. You can view the IP addresses that are associated with the email address, the IP addresses that the suspect visited, and the other names that are associated with the email address.

In distributed deployments, you can choose to see relationships for one node in your organization.

Procedure

1. Select a result from the list of documents in the recovery grid and click the **Digital Impression** tab.

2. From the list, select an item that you want to explore.

   By default, the digital impression report is listed in tabular format, which is organized by identifier type. All identifiers that interacted with the centering identifier are displayed. The interacting identifiers are organized by identifier type and are sorted by frequency of interaction.

3. If you see an identifier of interest, select it.

   Identifiers are hyperlinks and you can use them as the centering identifier of another report. Another tab is created and the new centering identifier is displayed. You can see who a given suspected attacker interacts with and then who the suspect's interactions interact with. You can expand the radius of an investigation to more suspected attackers and entities with whom they interact.

4. To look at another host, select the IP address from the **Select Remote Host** list.

   In distributed installations, you can choose the QRadar Incident Forensics host and then view the digital impression. The default view is the primary host, but you can select any secondary host that is associated with the QRadar Incident Forensics host.

5. To see a visualization of the associations and relationships of the interactions of the centering identifier to other identifiers, click the **Visualize Data** tab.

Visualize tool

You can explore associations and relationships visually across multiple attributes and data categories.

Use the Visualize window to look at a metadata relational map of one, two, or a large selection of documents. When large selections of documents are used, the investigator gets a comprehensive view of metadata relationships and relative frequency. Investigators can then follow these paths to further their investigation of a security incident.

The visualization of the selected documents can easily be rebuilt with a different relation by changing one or both relations.

The visualization shows every relation that is contained within the selected documents and shows the frequency of relation. Each node represents a distinct piece of metadata that is being related from the selected documents. The size conveys the relative frequency when compared to other nodes. Links show the connections that are found between the distinct pieces of metadata and convey frequency through size. Investigators can use the nodes to identify possible avenues for further investigation.

Visualizing relations and associations

Use the Visualize window to look at relations among attributes in recovered documents. For example, you can inspect the email addresses that communicated with a specific email address.

Procedure

1. In the recovery grid, click the check boxes for the documents that you want to investigate and click **Visualize**.
2. Select the layout, number of documents to display, and the relations among attributes that you want to see and click refresh.
3. Use the zoom controls to see more or less detail of the image.
4. To perform a new search or modify the active filter, right-click a node.

   From the context-sensitive menu, you can bring that piece of metadata back to perform a new search. You can also modify the active filter to either include or exclude the metadata.

   Restriction: You can view up to 9999 documents at a time in one Visualize window.

Artifact analysis for suspicious or malicious content

As a security analyst, you can look for threats that evaded detection by analyzing reconstructed artifacts, such as files and images. To understand connections between collaborators and artifacts, you can also investigate the links to and from these files and images.

Example - Using artifact analysis to find the source of an attack (patient zero)

John is a security analyst at Replay Industries. Several systems are infected despite all of security measures that are in place. After he identifies and quarantines these systems, John needs to find out how these systems became infected and whether other assets are similarly compromised.

Packet recovery from an IP address

Starting with the IP addresses and the approximate time frame that is involved, John is able to use QRadar Incident Forensics to recover the relevant packet data.
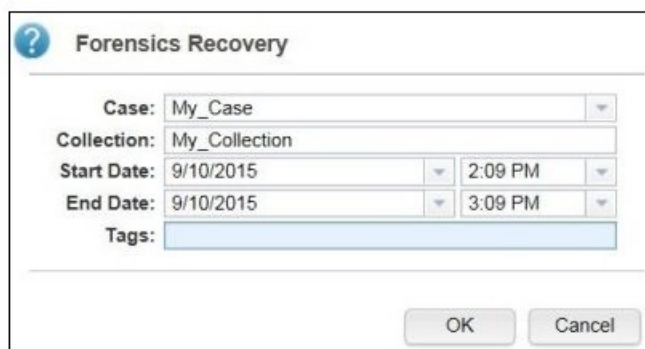

Figure 1. Recovery from an IP address

File analysis

Looking for executable content, John starts by using the file analysis capabilities included within QRadar Incident Forensics. Now he can see a list of all of the files, how often they were sent, whether they contained embedded files or scripts, and their entropy scores. John quickly sees an image file which QRadar Incident Forensics flagged as both suspect content and as having an embedded script.

Doc #	File Name	Extension	Description	Protocol	Frequency	Suspect Content	Embedded Script	Embedded Files	File Size (Bytes)	File Hash (SHA-256)	Entropy
1	index.php	php	CSS File	http	1	No Suspect Content	No Embedded Script	0	1916	70c6e673cd0150b1ffa89e	4.93731
2	index.php	php	CSS File	http	1	No Suspect Content	No Embedded Script	0	163060	dbbb35dcf2e494f068b9d1	5.74523
3	index.php	php	JavaScript	http	1	No Suspect Content	No Embedded Script	0	164112	909a0b9fa48182b58dd85	5.38451

Figure 2. File analysis attributes

The *file entropy score*, which measure the randomness of data and is used to find encrypted malware, and the entropy distribution also clearly show that a portion of the file is not what it should be. Further analysis proves that this file contains a new form of malware that slipped by existing security measures undetected and was responsible for the infected systems.

In the following diagram, entropy is used as an indicator of the variability of bits per byte. Because each character in a data unit consists of 1 byte, the entropy value indicates the variation of the characters and the compressibility of the data unit. Variations in the entropy values in the file might indicate that suspect content is hidden in files. For example, the high entropy values might be an indication that the data is stored encrypted and compressed and the lower values might indicate that at runtime the payload is decrypted and stored in different sections.
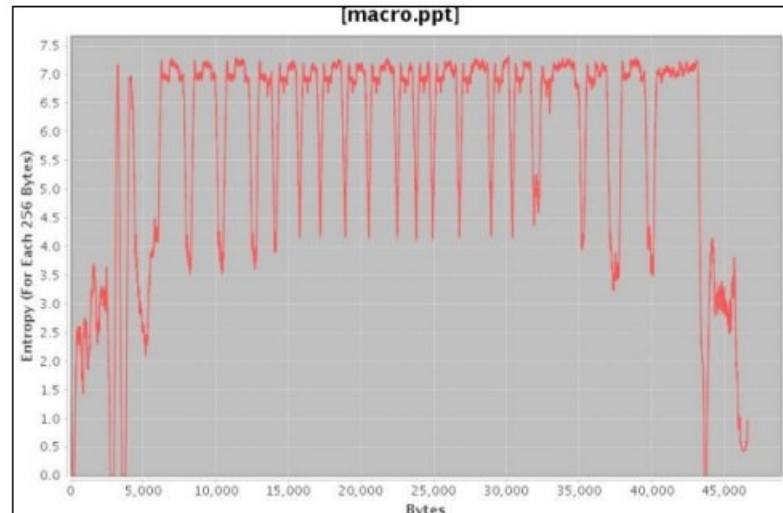

Figure 3. Example of file entropy graph that shows embedded scripts

John now needs to understand where this file came from and who else might have it. John uses QRadar Incident Forensics to quickly find the web server that supplied the infected image file. The web page in question is popular for broadcasting the most current news for everyone's favorite NFL team and is compromised. Even though the website contained many images, it was only the one image that John found earlier by using file analysis that contained the embedded malware.

Link analysis to visualize website communication

To determine what other systems might be affected, John uses link analysis to quickly visualize all of the websites that were viewed and despite the large amount of traffic across websites for companies that Replay did business with, a small subset of accesses might clearly be seen to the infected web host. John analyzes these links to see what other servers on his network were used to access this web host.

In his investigation, John uses the nodes in the graph, which represent web pages and the arrows between the nodes represent the relationships or transactions between the web pages to quickly assess traffic patterns and to see how documents were traversed. The larger the node, the more links the document has in its path and the larger the link arrow, the more times that link was used.
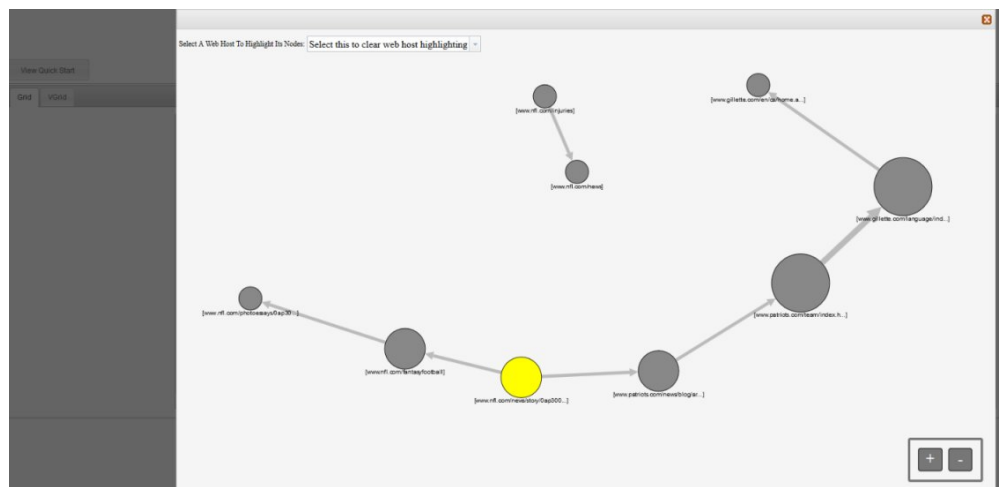
Being a popular NFL news site, it was not surprising to see a number of other servers were in contact with that web host and were potentially affected.

Image analysis

To narrow down which servers downloaded the malicious image file, John switches to image analysis and can quickly see all of the image files that were sent or received.
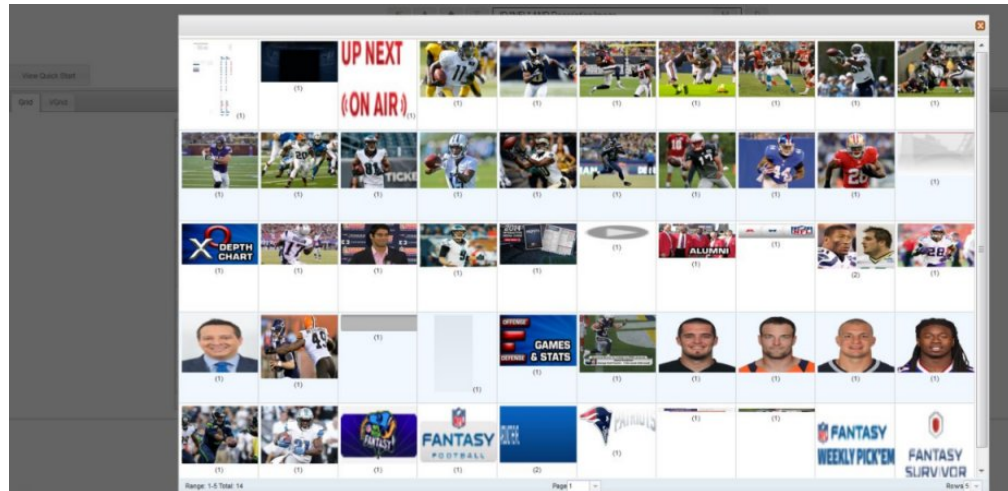
Figure 4. Example of image analysis and image distribution

John quickly confirms that all of his infected servers and 2 servers he was unaware of, had all access the compromised image file.

John also determines that several of the other servers that accessed the same website didn't download the infected file. John now has the information that he needs to quarantine these 2 extra servers, and create a new file hash of the infected file that Replay Industries can upload and shared with others on IBM X-Force® Exchange.

Analyzing files for embedded content and malicious activity

To investigate files for hidden threats, you can look at file entropy values, download embedded files and scripts for further analysis, and view the document and its attributes.

Because intruders can obfuscate the contents of binary files within container files, you can use file analysis in IBM Security QRadar Incident Forensics to examine whether files contain embedded scripts or other binary content.

File entropy measures the randomness of the data in a file and is used to determine whether a file contains hidden data or suspicious scripts. The scale of randomness is from 0, not random, to 8, totally random, such as an encrypted file. The more a unit can be compressed, the lower the entropy value; the less a unit can be compressed, the higher the entropy value.

In the following diagram, entropy is used as an indicator of the variability of bits per byte. Because each character in a data unit consists of 1 byte, the entropy value indicates the variation of the characters and the compressibility of the data unit. Variations in the entropy values in the file might indicate that suspect content is hidden in files. For example, the high entropy values might be an indication that the data is stored encrypted and compressed and the lower values might indicate that at runtime the payload is decrypted and stored in different sections.

Procedure

1. On the **Forensics** tab, select one or more recovered files from the **Grid** view.
2. From the investigative tools menu at the top of the grid, click **File Analysis**.

In the results, each row of the grid contains an analysis data for a document, for example, the file name, description, whether suspect content is detected, and entropy values.

3. To sort files by a specific attribute, such as entropy, click the associated column heading.
4. From the list of files, right-click a file for further investigation
   - To review the document and its attributes, click **Display Document**.
   - To review an entropy graph and check whether an embedded file or script might contain malware, click **Display Entropy**.

     You can use entropy values as an indication of whether the file might contain malicious content. For example, ASCII text files are typically highly compressible and have low entropy values. Encrypted data is typically not compressible, and usually has a high entropy value. Malware is often packed and hidden in both files and images.
   - To download embedded files, click **Extract Embedded Files** and select the files to download.

     This option is available only for documents with embedded files or scripts. Files are downloaded to the download location of your web browser. Be careful not to open potentially harmful scripts in an unprotected environment.

Analyzing images for hidden threats or suspicious activity

Viewed images are sorted by size and relevance with a frequency number in parentheses. This analysis might be useful to you when an employee is using company resources to look at inappropriate, restricted, or prohibited images. For example, the images might be related to airplanes, certain buildings, or locations that are targets for security breaches.

With image analysis, you can view the most relevant images from one or more documents in one or more packet capture files in one display instead of being forced to open each document and viewing the images.

Procedure

1. On the **Forensics** tab, from the **Grid** view, select one or more documents that contain image in the description.
2. From the investigative tools menu at the top of the grid, click **Image Analysis**.

   In the results, thumbnail versions of all the images that are contained within the documents are displayed in order of relevance. The number in parentheses next to the image indicates the number of instances of the image in the document. If you place the cursor over a thumbnail image, the image becomes larger.
3. Right-click an image for further investigation
   - To review the image and its attributes, click **Display Document**.
   - To review an entropy graph and check whether the image might contain malware, click **Display Entropy**.

     You can use entropy values as an indication of whether the file might contain malicious content. For example, bitmap image files and ASCII text files are typically highly compressible and have low entropy values. Encrypted data is typically not compressible, and usually has a high entropy value. Malware is often packed and hidden in both files and images.

Analyzing links for connections and relationships

In link analysis, the links show the commonality between websites that were viewed. During security incident investigations, you can quickly see where there is overlap and how people are communicating.

For example, if you think that group of perpetrators are collaborating but aren't sure how, you can look at a set of documents from a number of users, and use link analysis to show common web pages. You can then investigate specific websites.

Procedure

1. On the **Forensics** tab, select one or more web pages from the **Grid** view.
2. From the investigative tools menu at the top of the grid, click **Link Analysis**.

   If there is a relationship between websites, a cytoscape chart shows the web pages as circles (nodes) and links to and from the web pages as arrows. The larger the node, the more links the document has in its path and the larger the link arrow, the more times that link was used. Selected nodes are yellow.
3. To investigate communication from a specific web host, from the **Select Web Host** list, select the web host.

   The nodes that represent the web pages from the selected web host are highlighted as dark gray circles.
4. To enlarge or decrease the size of the circles (nodes) and arrows, use the zoom in (+) or zoom out (-) controls.

   You can also scroll up or down on the mouse wheel to increase or decrease the size of the nodes and arrows.
5. To move one or more nodes, click and drag the nodes.

   You can move the entire graph by clicking anywhere in the background and then holding and dragging.

Running a recovery from a document's Attributes page

When you view the **Attributes** tab for a document, you can run a recovery for an IP address or port.

Procedure

1. From the Search page on the **Forensics** tab, do a search.
2. From the list of returned documents, click one to open it.
3. Click the **Attributes** tab.
4. Click an IP address or a port.
5. From the menu, click **Run Recovery for**.

Chapter 5. Investigating network traffic for an IP address

To get visibility of the relevant content in the conversations that occurred during a security incident, you can recover and reconstruct network traffic that is associated with an IP address. You can also search through existing cases that are related to an IP address.

When network traffic is reconstructed from an IP address, an incident is created. Investigators can visualize a sequence of events from the security incident or view the documents in the incident.

IBM Security QRadar Incident Forensics indexes all available network data, file data, metadata, and textual characters that are in each recovered file.

In distributed deployments, multiple capture devices and QRadar Incident Forensics hosts capture and process data. You can view aggregated incident recovery results or results by host and capture device.

Procedure

1. To create a case and get data from the packet capture devices, in QRadar, right-click an IP address and then select **Run Forensics Recovery**.

   a. The following table provides guidance for the data recovery parameters:

   Table 5. Parameters for data recovery

Parameter	Description
Case	The case that is used for the investigation. **Restriction:** The case name must be unique.
Collection	Recovered data is grouped into a collection and associated to the case. **Restriction:** The collection name must be unique. If the collection name exists in the case, then the original collection is deleted.
Start date	The start date and time for the data packet capture.
End date	The end date and time for the data packet capture.
Tags	Metadata tags that are used to quickly retrieve exact result sets from relevant documents. **Restriction:** The # symbol is not permitted. You can use other special characters, such as $, %,*.

   b. Click **OK**, and then click the **Forensics** tab.

      Troubleshoot: If you see a message that you do not have permission to recover data, ensure that your security profile has access to the IP address. In some instances, if you used a # character in the **Tags** field, you might see the message.

   c. Click the triangle icon to view your incidents.

   d. To visualize a sequence of events for the incident, click **Jump to surveyor page results**.

   e. To view the documents in the incident, click **Jump to search page results**.

2. To search existing cases for the IP address, in QRadar, right-click an IP address and click **Run Forensics Search**.

   a. On the **Forensics** tab, click the incidents (triangle) icon.

    b. To investigate an aggregate of the activities that are associated with an incident, highlight a case by hovering over it, and then click the search icon.

    c. To investigate activities by QRadar Incident Forensics host and capture device in distributed deployments, expand the **Case** entry and then expand the **Collection** entry.

    d. To view a chronological list of interactions in an incident, highlight the collection by hovering over it, and then click the surveyor icon.

Related concepts:

"Reconstructed document view" on page 22
The **View** tab shows a reconstructed view of the document that is selected on the left side of the screen in the List view.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Glossary

This glossary provides terms and definitions for the IBM Security QRadar Incident Forensics software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

anomaly
: A deviation from the expected behavior of the network.

attack
: Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
: A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

B

Boolean operator
: A built-in function that specifies a logical operation of AND, OR or NOT when sets of operations are evaluated. The Boolean operators are &&, || and !.

breadcrumb
: A web interface element that displays the user's position within a site. It is usually a series of hyperlinks appearing across the top or bottom of the page. These links indicate pages that have been viewed and enable the user to navigate back to the starting location.

C

capture device
: See packet capture appliance.

case
: The information that is contained within a database that pertains to a particular investigation.

category
: A set of items that are grouped according to a specific description or classification. Categories can be different levels of information within a dimension.

centering identifier
: The category item with which all other identifiers have interacted. The centering identifier is the central item in an investigation.

collection
: A distinct named set of data that is associated with a case. For example, an ordered set of captured network packets.

continuously collected electronic presence
: An attacker's online identity as a collection of digital impressions that are linked.

conversation
: A forensically reconstructed flow of data between two or more network endpoints. For example, a social network conversation.

D

decapping
: The process by which the packet capture data is decompiled so that all of the ingested data is produced as a results report.

digital impression
: A report consisting of tagged identifiers that are related to each other within an individual case.

digital impression relationship
A relationship between tagged identifiers related to a case.

domain inspector
A specialized inspector that is designed to deconstruct and extract forensics data from specific domain websites such as Facebook or Gmail.

E

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

F

flow record
A record of the conversation between two hosts.

forensic investigator
The user who extracts relevant data from network traffic and documents in the forensic repository.

H

hypothesis
A proposed explanation for an incident that is based on the available evidence collected in a case. A hypothesis must be testable and falsifiable.

I

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

incident
See security incident.

ingested network traffic
Captured network traffic that has been processed by the forensics decapping process.

M

metadata
Data that describes the characteristics of data; descriptive data.

metadata relational map
A map that displays related metadata from case documents.

O

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

P

packet capture appliance
A stand-alone appliance that intercepts and logs traffic data.

packet capture information
The traffic data information that is collected by a capture device.

protocol inspector
A specialized inspector that is designed to extract forensic data from network protocols such as HTTP or FTP.

R

recovery job
A process that recovers queried capture data and forwards it to the decapper device for ingestion.

S

security incident
An event in which the normal network operations are violated, compromised, or attacked.

superflow
A single flow that is comprised of multiple flows with similar properties in order to increase processing capacity by reducing storage constraints.

surveyor tool
A tool that displays the chronological sequence of activities in a security incident in a visualizer.

T

traffic In data communication, the quantity of data transmitted past a particular point in a path.

trail Digital impressions that connect individuals involved in a case to individuals outside of the case.

V

vulnerability

A security exposure in an operating system, system software, or application software component.

Index

A
annotations   19

D
digital impression
   overview   24

F
files
   uploading by using FTP   14

G
glossary   39

I
IP address investigation   33

M
metadata tag   16

N
new features,   1

P
patterns   21

Q
query   17
query builder   17

S
search criteria   17

T
time blocks   22

V
visualizations   21

W
what's new
   version 7.2.6 users   1

43

IBM ®

Printed in USA